Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

20.05.2012

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

Informations- und Kommunikationsinfrastrukturen haben Wirtschaft, Staat und Gesellschaft grundlegend verändert. Die Nutzung des Cyber-Bereichs (z.B. Internet und mobile Netze) hat viele Vorteile und Chancen gebracht. Allerdings hat die digitale Vernetzung auch dazu geführt, dass Informations- und Kommunikationsinfrastrukturen für kriminelle, nachrichtendienstliche, machtpolitische oder terroristische Zwecke missbraucht oder ihr Funktionieren beeinträchtigt werden können. Störungen, Manipulationen und gezielte Angriffe, die via elektronische Netzwerke ausgeführt werden, sind Risiken, die mit einer Informationsgesellschaft einhergehen. Es ist davon auszugehen, dass Cyber-Angriffe in Zukunft tendenziell zunehmen.

Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat die Strategie zum Schutz der Schweiz vor Cyber-Risiken in Auftrag gegeben. Der Bundesrat verfolgt die folgenden strategischen Ziele:

- die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich
- die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- die wirksame Bekämpfung von Cyber-Risiken, insbesondere Cyber-Kriminalität und Cyber-Spionage

Mit der vorliegenden Strategie wird auch mehreren parlamentarischen Vorstössen, in denen verstärkte Massnahmen gegen Cyber-Risiken gefordert wurden, Rechnung getragen.

Wesentliche Rahmenbedingungen und Voraussetzungen für die Reduktion von Cyber-Risiken sind und bleiben das Handeln in Eigenverantwortung und die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie die Kooperation mit dem Ausland. Mit einem permanenten gegenseitigen Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden. Der Staat soll nur eingreifen, wenn öffentliche Interessen auf dem Spiel stehen und er im Sinne der Subsidiarität handelt.

Die Bewältigung von Cyber-Risiken ist als Teil eines integralen Geschäfts-, Produktions- oder Verwaltungsprozesses zu verstehen, in den alle Akteure von der administrativen, technischen bis hin zur Führungsstufe einzubeziehen sind. In diese Prozesse sind alle Akteure von der administrativen, technischen bis hin zur Führungsstufe einzubeziehen. Ein wirksamer Umgang mit Cyber-Risiken geht vom Grundsatz aus, dass bestehende Aufgaben und Verantwortlichkeiten von Behörden, Wirtschaft und Bevölkerung eine Cyber-Ausprägung haben. Der nationalen Strategie liegt die Überlegung zugrunde, dass jede Organisationseinheit aus Politik, Wirtschaft und Gesellschaft die Verantwortung trägt, diese Cyber-Ausprägung zu erkennen, die damit einhergehenden Risiken in ihren jeweiligen Prozess aufzunehmen und damit zu reduzieren. Die dezentralen Strukturen in Verwaltung und Wirtschaft sollen gestärkt und auf bereits bestehenden Ressourcen aufgebaut werden.

Die fortlaufende Zusammenführung von technischen und nicht technischen Informationen ist notwendig, um Cyber-Risiken umfassend zu analysieren und zu bewerten sowie die Erkenntnisse aus den Untersuchungen zu verbreiten.

Vor diesem Hintergrund schlägt die vorliegende Strategie eine Reihe konkreter Massnahmen entlang von sechs Handlungsfeldern vor:

Handlungsfeld 1	**Massnahmen**	
Forschung und Entwicklung	1	Akademischer Wissensaustausch im Bereich Forschung und Entwicklung
	2	Unterstützung von Forschungsprojekten mit Fachwissen und Ressourcen
Handlungsfeld 2	**Massnahmen**	
Risiko- und Verwundbarkeits-analyse	3	Selbständige Überprüfung der Systeme Risikoanalysen in Zusammenarbeit mit regulierenden Behörden
	4	IKT-Produkte auf organisatorische, systemische und technische Ver-wundbarkeiten untersuchen
Handlungsfeld 3	**Massnahmen**	
Analyse der Bedrohungslage	5	Erstellung Lagebild und Lageentwicklung
	6	Nachbearbeitung von Vorfällen für die Weiterentwicklung von Massnah-men
	7	Fallübersicht und Koordination interkantonaler Fallkomplexe
Handlungsfeld 4	**Massnahmen**	
Sensibilisierung und Ausbildung	8	Vernetzung bestehender und Schaffung von Bildungs- und Informati-onsmassnahmen
	9	Unterstützung von Projekten mit Fachwissen und Ressourcen
	10	Ausbildung aller Akteure von der administrativen, technischen bis hin zur strategisch-politischen Ebene
Handlungsfeld 5	**Massnahmen**	
Internet-Governance und Inter-nationale Policies	11	Aktive Teilnahme der Schweiz im Bereich der Internet-Governance.
	12	Koordination der Akteure bei der Beteiligung an Initiativen und Best-Practices im Bereich Sicherungsprozesse
Handlungsfeld 6	**Massnahmen**	
Kontinuitäts- und Krisenmana-gement	13	Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz) gegen-über Störungen und Ereignissen
	14	Koordination der Aktivitäten in erster Linie mit den direkt betroffenen Akteuren und Unterstützung Entscheidfindungsprozesse mit fachlicher Expertise
	15	Aktive Massnahmen zur Identifikation der Täterschaft und allfälligen Beeinträchtigung deren Infrastruktur bei einer spezifischen Bedrohung
	16	Erarbeitung eines Konzeptes für eine Führungsorganisation in der aus-serordentlichen Lage
Handlungsfeld 7	**Massnahmen**	
Rechtsgrundlagen	17	Überprüfung bestehender Rechtsgrundlagen auf Grund der Massnahmen und Umsetzungskonzepte und Priorisierung von unverzüglichen Anpas-sungen
	18	Prüfung der Grundlagen und Möglichkeiten zur rechtlichen Verpflichtung von Stellen und Organisationen über die Bundesbehörden hinaus

Die verantwortlichen Stellen sollen die Massnahmen im Rahmen ihres Grundauftrags bis Ende 2016 umsetzen. In diesen Umsetzungsprozess gilt es, die Partner aus Behörden, Wirtschaft und Gesellschaft einzubeziehen. Eine Koordinationsstelle überprüft dabei die Umsetzung der Massnahmen und ob bei Bedarf weitere Vorkehrungen zur Risikominimierung notwendig sind. Diese Koordinationsstelle wird in einer Bundesstelle eingerichtet.

1 EINLEITUNG

Die globale digitale Vernetzung hat ungeahnte Möglichkeiten geschaffen, im Guten wie im Schlechten. Staat, Wirtschaft und Gesellschaft machen sich Informations- und Kommunikationsinfrastrukturen und den Zugang zum Cyber-Bereich (Internet, mobile Netze und Anwendungen, E-Business, E-Government, computerbasierte Steuerungsprogramme) zunutze. Das heisst aber auch, dass die Anfälligkeit und Abhängigkeit gegenüber Störungen, Manipulationen und Angriffen zugenommen hat. Die Möglichkeiten, die Informations- und Kommunikationsinfrastrukturen für kriminelle, nachrichtendienstliche, terroristische oder militärische Zwecke zu missbrauchen oder ihr Funktionieren zu beeinträchtigen, sind ebenso wie deren positive Nutzung praktisch unbegrenzt. Es ist davon auszugehen, dass der dahinter liegende Trend, die zunehmende Vernetzung und damit die Komplexität der Informations- und Kommunikationsinfrastrukturen anhalten werden.

Das Funktionieren der Schweiz als Gesamtsystem (Staat, Wirtschaft, Verkehr, Energieversorgung, Kommunikation usw.) hängt von einer steigenden Zahl miteinander vernetzter Informations- und Kommunikationseinrichtungen ab (Rechner und Netzwerke). Diese Infrastruktur ist verwundbar. Angriffe können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit der Schweiz führen. Solche Angriffe können unterschiedliche Täterkreise und Motive haben: Einzeltäter, Aktivisten mit politischen Zielsetzungen, kriminelle Organisationen mit Betrugs- oder Erpressungsabsichten, staatliche Spione oder Terroristen, die Staat und Gesellschaft stören und destabilisieren wollen. Informations- und Kommunikationsinfrastrukturen sind für Angriffe nicht nur deshalb besonders attraktiv, weil sie viele Möglichkeiten für Missbrauch, Manipulation und Schädigung bieten, sondern auch weil sie sich dafür anonym und mit wenig Aufwand nutzen lassen.

Der Schutz[1] der Informations- und Kommunikationsinfrastrukturen vor solchen Angriffen liegt im nationalen Interesse der Schweiz. Zwar wurden in den letzten Jahren Massnahmen getroffen, um die Risiken[2] im Cyber-Bereich zu reduzieren; es hat sich aber gezeigt, dass diese nicht für alle Fälle genügen. Weil mit weiteren Angriffen auf Informations- und Kommunikationsinfrastrukturen (und durch diese auf weitere Einrichtungen) zu rechnen ist, beauftragte der Bundesrat am 10. Dezember 2010 das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), eine nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken auszuarbeiten. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind. Die vorliegende nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken ist das Resultat dieser Arbeiten[3].

---

[1] Darunter sind alle Massnahmen zum Schutz der Informations- und Kommunikationsinfrastrukturen gegen unbefugtes Eindringen und Beeinträchtigung ihrer Funktionen zu verstehen, nicht aber der Kampf gegen die Verbreitung illegaler Inhalte, wie z.B. Kinderpornografie. Es geht um die technischen Aspekte, nicht aber um die inhaltliche Auseinandersetzung mit falschen und irreführenden Informationen und Propaganda.

[2] Risiken definieren sich aus dem erwarteten Schadensausmass und der Eintrittswahrscheinlichkeit von Bedrohungen und Gefahren. Beide werden in der Strategie berücksichtigt.

[3] Die Strategie trägt diversen parlamentarischen Vorstössen Rechnung, in denen verstärkte Massnahmen gegen Cyber-Risiken gefordert wurden: 08.3100 – Motion Burkhalter: Nationale Strategie für die Bekämpfung der Internetkriminalität; 08.3101 – Postulat Frick: Die Schweiz wirksamer gegen Cybercrime schützen; 10.3136 – Postulat Recordon: Analyse der Bedrohung durch Cyberwar;10.3625 – Motion SIK-NR: Massnahmen gegen Cyberwar; 10.3910 – Postulat FDP-Liberale: Leit- und Koordinationsstelle im Bereich der Cyber-Bedrohung; 10.4102 – Postulat Darbellay: Konzept zum Schutz der digitalen Infrastruktur der Schweiz.

Cyber-Risiken sind vielfältig; Wirtschaft, Gesellschaft und der Staat sind ihnen ausgesetzt. Eine wirksame Strategie dagegen muss deshalb einen *umfassenden Ansatz* haben und alle wesentlichen Akteure, staatliche und private, Betreiber kritischer Infrastrukturen (KI), Nutzer und Hersteller einbeziehen. Die vorliegende Strategie zum Schutz der Schweiz vor Cyber-Risiken adressiert in erster Linie die Organe des Bundes und wurde in Zusammenarbeit mit Vertretern aller Departemente, verschiedener KI-Betreibern und der Wirtschaft erarbeitet. Sie beschreibt die Rollen der verschiedenen Akteure und die Ausgestaltung der Zusammenarbeit, die für einen besseren Schutz vor Cyber-Risiken nötig ist und bildet so die Basis der intensiven Zusammenarbeit mit den Kantonen in der Umsetzungsplanung.

Wegen der vielfältigen Dienstleistungen und Präsenz im Internet sowie wegen der Nutzung und Abhängigkeit von kritischen Infrastrukturen[4] ist die Wirtschaft stark und häufig von Cyber-Risiken betroffen, z.B. durch Angriffe mit Betrugs- bzw. Bereicherungsabsichten oder Wirtschaftsspionage. Der Einbezug der Wirtschaft in eine Strategie gegen Cyber-Risiken ist deshalb essenziell.

- Cyber-Angriffe auf kritische Infrastrukturen können besonders gravierende Folgen haben, weil sie lebenswichtige Funktionen beeinträchtigen oder fatale Kettenreaktionen auslösen können. Den (oft privaten) KI-Betreibern kommt deshalb eine besondere Bedeutung zu, als Erbringer von wichtigen Leistungen mit übergeordneter, sicherheitsrelevanter Bedeutung.
- Staatliche Behörden und Verwaltungen aller Ebenen (Bund, Kantone, Gemeinden) können ebenfalls Opfer von Cyber-Angriffen sein. Sie können in ihrer Funktion als Legislative, Exekutive oder Judikative beeinträchtigt werden, aber auch als Betreiber und Nutzer kritischer Infrastrukturen oder von Forschungs- und Entwicklungsinstituten.
- Cyber-Risiken betreffen auch die Bevölkerung mit allen individuellen Nutzern privater und beruflicher Informations- und Kommunikationssysteme sowie kritischer Infrastrukturen. Eine wirksame Strategie gegen Cyber-Risiken muss auch dem individuellen Verhalten und dessen Risiken Rechnung tragen.

In erster Linie sind die einzelnen Akteure selbst für die Aufrechterhaltung und Optimierung von Schutzmassnahmen zur Minimierung von Cyber-Risiken verantwortlich. Dies liegt in der Natur der Sache: Cyber-Risiken sind eine Ausprägung bestehender Aufgaben, Verantwortungen und Prozesse. Es ist somit im Eigeninteresse der Anwender, massgeschneiderte Lösungen für bereichs- oder branchenspezifische Probleme zu erarbeiten und umzusetzen. Dieser Ansatz entspricht auch der für die Schweiz charakteristischen dezentralen Wirtschafts- und Staatsstruktur. Der Staat erbringt subsidiär Leistungen zum Schutz vor Cyber-Risiken, z.B. durch Informationsaustausch, nachrichtendienstliche Erkenntnisse und Strafverfolgung. Wo eigenverantwortliches, bereichsspezifisches Handeln nicht wirksam, effizient oder praktikabel ist, soll der Staat zusätzliche Leistungen für den Schutz vor Cyber-Risiken erbringen und die anderen Akteure unterstützen. Die vorliegende Strategie soll aufzeigen, wo die Schwachstellen beim Umgang mit Cyber-Risiken gegenwärtig liegen. Sie beschreibt, wo der Staat und die anderen Akteure Leistungen erbringen sollen, um das Schutzniveau in der Schweiz zu erhöhen.

Dabei gilt es zu beachten, dass das Bemühen um Schutz mit anderen und ebenso legitimen Interessen kollidieren kann. Eine möglichst vollständige Informationsgrundlage, welche auf

[4] Kritische Infrastrukturen sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat haben. Dazu gehören zum Beispiel Steuerungs- und Schaltanlagen der Energieversorgung oder der Telekommunikation.

technisch-operativen wie auch strategisch-politischen Erkenntnissen beruht, muss geschaffen werden, um entsprechend informierte Entscheide treffen zu können: So können sich *Schutz- und Wirtschaftlichkeitsüberlegungen* dort in die Quere kommen, wo der Aufbau von Redundanzen und Überkapazitäten bei Infrastrukturen zwar dem Schutz zugutekäme, ökonomischen Überlegungen aber zuwiderläuft. Kommt hinzu, dass die wirtschaftliche Liberalisierung diesbezüglich die Ausgangslage insofern verändert hat, als eine zunehmende Zahl KI-Betreiber (z.B. Energie, Telekommunikation) privatisiert oder zumindest teilprivatisiert ist und damit primär marktwirtschaftlicher Logik verpflichtet ist. Ein zweiter Bereich, wo sich Interessenkonflikte ergeben können, sind die *Persönlichkeitsrechte*: Bestrebungen, die Schutzmechanismen im Cyber-Bereich zu verbessern (z.B. durch stärkere Kontrollen oder Überwachung), müssen gegenüber dem Schutz der Privatsphäre abgewogen werden. Es ist auch Aufgabe der vorliegenden Strategie, diesen Güterabwägungen Beachtung zu schenken und aufzuzeigen, wie Massnahmen umsichtig vorgenommen werden können.

Die Strategie zum Schutz der Schweiz vor Cyber-Risiken hat *Schnittstellen zu anderen Projekten*, die sich auf Stufe Bund ebenfalls mit Sicherheitsfragen befassen und thematisch verwandt sind. Diese Arbeiten müssen bei der Umsetzung eng aufeinander abgestimmt sein. Die wichtigsten dieser Projekte sind:

Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz

Die Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz wurde am 9. März 2012 vom Bundesrat verabschiedet. „Sicherheit und Vertrauen“ ist ein Handlungsschwerpunkt des Bundes. Die Ziele, die damit verfolgt werden, sind der Ausbau der Sicherheitskompetenzen, der Schutz vor Internetkriminalität und die Erhöhung der Resilienz der Informations- und Kommunikationstechnologien (IKT) und bei den kritischen Infrastrukturen. Das dazugehörige Konzept, das bereits 2010 vom Bundesrat gutgeheissen wurde, sieht Massnahmen vor, um die Bevölkerung und die kleinen und mittleren Unternehmen für einen sicherheitsbewussten und rechtskonformen Umgang mit den IKT zu sensibilisieren. 2010 hat der Bundesrat ausserdem einen Bericht zur Sicherstellung der Rechtsgrundlagen für die Umsetzung genehmigt. Der Bundesrat erwartet bis Ende 2012 einen Vorentwurf für die erforderlichen Rechtsgrundlagen.

Nationale Strategie zum Schutz Kritischer Infrastrukturen

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. Weiter wird ein Leitfaden zur Verbesserung des umfassenden (integralen) Schutzes der Kritischen Infrastrukturen erarbeitet. Die SKI-Grundstrategie wird derzeit zu einer nationalen SKI-Strategie erweitert und dem Bundesrat gemeinsam mit der vorliegenden Strategie vorgelegt.

Gesetzgebung über die Informationssicherheit im Bund

Der Bundesrat hat das VBS mit Beschluss vom 12. Mai 2010 beauftragt, formell-gesetzliche Grundlagen für den Informationsschutz und die Informationssicherheit zu erarbeiten, um die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten und Informationen zu schützen und zu gewährleisten. Diese neue Gesetzgebung soll in erster Linie die Grundsätze der Informationssicherheit für alle Bundesbehörden festlegen und die Verantwortlichkeiten einheitlich regeln. Damit werden Vorgaben für den Umgang mit schutzwürdigen Daten und Informationen gemacht. Die Vernehmlassung ist für Ende 2012 geplant.

Bericht des Bundesrates in Erfüllung des Postulats Malama (Innere Sicherheit. Klärung der Kompetenzen)

Mit dem Postulat Malama wurde der Bundesrat beauftragt, in einem Bericht die verfassungsrechtliche Kompetenzordnung und die tatsächliche Aufgabenverteilung zwischen Bund und Kantonen im Bereich der inneren Sicherheit zu klären. Dabei wurde geprüft, ob die bestehende Kompetenzaufteilung zweckmässig ist und den heutigen Herausforderungen genügt. Der Bundesrat hat den Bericht am 2. März 2012 verabschiedet.

2 CYBER-RISIKEN

Cyber-Risiken sind real und vielfältig. Auch wenn es keine genauen Angaben, sondern nur grobe Schätzungen darüber gibt, wie gross sie sind, mit welcher Häufigkeit Cyber-Angriffe oder technische Störungen vorkommen, und wie gross der angerichtete Schaden oder das Schadenspotenzial tatsächlich sind, ist die Tendenz der letzten Jahre unbestritten und eindeutig: Vorfälle, bei denen Staaten, Unternehmen und Individuen via Datennetzwerke angegriffen und geschädigt werden, nehmen zu, in Anzahl und Qualität.

Dies ist eine Folge der zunehmenden Vernetzung der Informations- und Kommunikationsinfrastrukturen, von deren gegenseitigen Abhängigkeiten und der Unübersichtlichkeit der dahinter liegenden Prozesse. Mit der Komplexität dieser Systeme steigen auch deren Fehler- und Störanfälligkeit und die potenziellen Angriffsmöglichkeiten. Es muss damit gerechnet werden, dass Cyber-Angriffe professioneller und gefährlicher werden. Neben den bekannten Fällen wird eine grosse Anzahl nicht gemeldeter oder bisher nicht entdeckter Angriffe vermutet, wobei die hohe Dunkelziffer auch mit dem befürchteten Reputationsverlust der angegriffenen Unternehmen zu tun hat.

2.1 Methoden

Cyber-Angriffe werden auf Computer, Netzwerke und Daten geführt. Dabei soll die Integrität der Daten oder die Funktionsweise der Infrastruktur gestört sowie deren Verfügbarkeit eingeschränkt oder unterbrochen werden. Es geht darum, die Vertraulichkeit oder die Authentizität der Informationen zu beeinträchtigen, indem Daten unbefugt gelesen, gelöscht oder verändert, Verbindungen oder Server-Dienstleistungen überlastet oder Informationskanäle ausspioniert werden.

Die Werkzeuge, die dafür von Cyber-Angreifern angewendet werden, sind vielfältig. Es können Schadprogramme gezielt und ohne Wissen des Anwenders auf fremden Computern installiert werden, um die Vertraulichkeit, Integrität und Authentizität von Daten zu beeinträchtigen. Fehlerhafte Funktionen von ungenügend geschützten und gewarteten Betriebssystemen und Applikationen (z.B. Internetbrowser oder Fachanwendungen) dienen den Angreifern, die Kontrolle über die betroffenen Computer zu übernehmen. Damit lassen sich diese Computer über das Internet fernsteuern, und es können zusätzliche Schadprogramme auf den Systemen installiert werden, die wiederum fähig sind, auf die gespeicherten Daten zuzugreifen, diese an die Angreifer zu übermitteln, sie zu verändern oder zu löschen. Es können Daten, wie Tastatureingaben der Benutzer, aufgezeichnet und an die Angreifer übermittelt oder ungewollte Zugriffe auf unsichere Webseiten veranlasst werden. Auf diese Weise können dem Benutzer unter anderem Kreditkartennummern, Zugriffsdaten auf E-Banking-Dienste oder andere vertrauliche Daten entwendet werden. Angreifer nützen aber auch organisatorische Schwächen von Sicherheitskonzepten in Unternehmen aus, um in geschützte Systeme einzudringen. Über Prozesse der Datenverarbeitung und unsicher konzipierte oder mangelhaft gewartete Systeme (z.B. das Belassen des Auslieferungspasswortes) gelingt es den Tätern oft, in die entsprechenden Systeme einzudringen.

Manipulierte Computer werden von Angreifern zudem dazu verwendet, um koordinierte und weit verteilte Massenanfragen auf Serverdienste auszuführen. Damit wird die Verfügbarkeit von Daten gestört: Solche Angriffe werden Distributed-Denial-of-Service-Angriffe genannt.

In vielen Fällen kommen Methoden zur Anwendung, wie sie bei der Spionage verwendet werden, um die Vertraulichkeit von Daten zu verletzen (z.B. Ausnützung menschlicher Schwächen, Diebstahl oder physischer Einbruch). Dabei werden Benutzer von Computersystemen dazu gebracht, Auskünfte über die Sicherheitsmassnahmen zu geben, es werden Datenträger gestohlen oder Infrastrukturen an Ort und Stelle durch Manipulation an der Konfiguration verändert. Es können auch Methoden zur Anwendung kommen, wie sie bei der Sabotage verwendet werden, um gezielt industrielle Steuerungsanlagen[5] anzugreifen, indem eigens dazu entwickelte Schadprogramme eingesetzt werden.

Angreifer geniessen mehrere Vorteile im Cyber-Bereich, um sich und ihre Angriffe vor einer (frühzeitigen) Entdeckung und Strafverfolgung zu bewahren: Anonymität, geografische Distanz, rechtliche Lücken, das Verwischen von Spuren durch Fälschung von technischen Daten und die zunehmend technische Komplexität der Angriffsmethoden. Ausgehend von den festgestellten Angriffsmethoden und Werkzeugen kann in den meisten Fällen nicht eindeutig auf die Angreifer und deren Motive zurückgeschlossen werden. Allen Angreifern stehen dieselben Methoden und Werkzeuge zur Verfügung, wobei diese gleichzeitig unterschiedliche Zwecke erfüllen und anderen Auftraggebern dienen können.

Die häufigsten Cyber-Angriffe können relativ einfach durchgeführt werden, weil die dazu benötigten Mittel und technischen Kenntnisse oft einfach und günstig erwerbbar sind. Beim Grossteil der Angriffe handelt es sich um nicht koordinierte Vandalenakte, Spionage und betrügerische Handlungen im Internet, die in der Regel nur begrenzten Schaden anrichten (z.B. Reputationsschaden) und relativ einfach zu beheben sind. Der Schutz vor solchen Angriffen ist zwar wichtig, die vorliegende Strategie richtet ihr Augenmerk aber besonders auf Angriffe mit grösserem Schadenspotenzial, welche die Handlungsfähigkeit von Wirtschaft, Staat und Gesellschaft direkt oder indirekt stark beeinträchtigen können.

Grössere Schäden können mit spezifisch ausgerichteten Angriffen auf besonders geschützte Ziele angerichtet werden. Solche Angriffe bedürfen eines massiv höheren Aufwandes. Ein absoluter Schutz vor solchen Angriffen ist realistischerweise nicht zu erreichen, weshalb reaktive Fähigkeiten, die sich an einem risikominimierenden Ansatz orientieren und die Schadensbegrenzung und Wiederherstellung der Ausgangslage zum Ziel haben, im Vordergrund stehen.

2.2 Akteure und Motive

Als Täter kommen Einzelpersonen, Gruppen und Staaten in Frage. Sie unterscheiden sich erheblich in ihren Absichten sowie technischen und finanziellen Mitteln.

Staatliche oder staatlich finanzierte Akteure haben in der Regel grössere finanzielle, technische und personelle Mittel und sind besser organisiert, womit ihnen ein relativ hohes Schadenspotenzial zukommt. Sie beabsichtigen mit ihren Angriffen, den Staat, einzelne Behörden, die Armee, die Wirtschaft oder Forschungseinrichtungen auszuspionieren, zu erpressen, zu kompromittieren oder auf andere Weise gegen nationale oder wirtschaftliche Interessen vorzugehen, um machtpolitische und wirtschaftliche Interessen zu verfolgen. Gefährdet sind auch ausländische Unternehmen, Institutionen und Personen in der Schweiz.

[5] International wird von sogenannten SCADA-Systemen gesprochen (*Supervisory Control and Data Acquisition*). Diese IKT-Systeme dienen der Überwachung und Steuerung technischer Prozesse.

Im Oktober 2009 wurde beim Eidgenössischen Departement für auswärtige Angelegenheiten ein Schadprogramm entdeckt, das Spionageaktivitäten ausführte. Es gelangte via E-Mail in das Netzwerk und blieb lange unentdeckt. Auf ähnliche Weise wurden in den Jahren zuvor die Rüstungsunternehmen RUAG und Mowag angegriffen. Im Juni 2010 wurde ein Schadprogramm (Stuxnet) entdeckt, das mutmasslich dazu entwickelt worden war, iranische Urananreicherungsanlagen zu beschädigen, indem ein Softwarefehler in die Steuerungssysteme (SCADA) eingefügt wurde. Wegen der technischen Komplexität wird angenommen, dass nur staatliche Urheber für diesen Angriff in Frage kommen.

Ähnlich bedrohlich werden *Akteure der organisierten Kriminalität* eingeschätzt, weil ihnen meistens auch professionelle Organisationen, grosse Geldmittel und spezifische Fähigkeiten zur Verfügung stehen. Ihre Bereicherungsabsichten können dazu führen, dass bei massenhaften, dauernden und organisierten Cyber-Angriffen auf Wirtschaft (z.B. Finanzwesen) und Individuen erhebliche volkswirtschaftliche Schäden entstehen und die Glaubwürdigkeit des Rechtsstaates in Frage gestellt wird.

Seit Jahren wird unter anderem der Trojaner[6] ZeuS gegen Benutzer von Online-Banking eingesetzt. Das Schadprogramm wird über gefälschte oder manipulierte Webseiten auf die Informatikinfrastrukturen von Privatpersonen eingeschleust. Die Angreifer können anschliessend die Verbindung zu Telebanking-Diensten kapern und damit Geld von Konten abzweigen.

An Bedeutung gewinnen in jüngster Zeit Angriffe auf Webseiten des öffentlichen und privaten Sektors durch sogenannte *„Hacktivisten".* Diese nichtstaatlichen, einzeln oder lose organisierten, unter Umständen aber massenhaft agierenden Akteure verfügen über gute technische Fähigkeiten. Das Schadenspotenzial massenhafter Angriffe aus diesen Kreisen ist mittel bis hoch einzuschätzen. „Hacktivisten" geht es darum, Dienstleistungen zu unterbrechen, finanzielle Schäden zu verursachen und rufschädigend zu wirken, um öffentliche Aufmerksamkeit für ihre Anliegen zu erlangen.

Im Dezember 2010 rief die Hacker-Gruppe „Anonymous" zu einem Angriff auf PostFinance auf. Dadurch wurden die Internet-Dienstleistungen für einen ganzen Tag unterbrochen. Auslöser war die Schliessung des Postcheck-Kontos von Julian Assange, dem Gründer von WikiLeaks. – Russische Aktivisten griffen im Jahr 2007 wegen der Versetzung eines sowjetischen Militärdenkmals in Tallinn estnische Informations- und Kommunikationsinfrastrukturen massiv an. Das E-Government-Angebot und die Internet-Dienste zahlreicher Firmen konnten über mehrere Tage nicht mehr genutzt werden. Zudem wurden Webseiten von Regierungsstellen und Unternehmen mit prorussischen Parolen verunstaltet.

Terroristen nutzen den Cyber-Bereich, um Propaganda zu streuen, Anhänger zu radikalisieren, Mitglieder zu rekrutieren und auszubilden, Geldmittel zu beschaffen, Aktionen zu planen und zu kommunizieren. Bislang steht die Nutzung der Informations- und Kommunikationsinfrastruktur im Vordergrund, nicht aber der Angriff auf diese: Terroristen zielen nach wie vor hauptsächlich darauf ab, auf konventionellen Wegen schwere physische Attacken gegen Leib und Leben sowie Infrastrukturen zu verüben. Terroristisch motivierte Cyber-Angriffe mit hohen Folgeschäden physischer Art erscheinen aus heutiger Sicht wenig wahrscheinlich. Es kann allerdings nicht ausgeschlossen werden, dass Terroristen in Zukunft versuchen könnten, Cyber-Angriffe gegen kritische Infrastrukturen eines Landes zu lancieren. Auch wenn die

[6] Software mit bösartigen Funktionen (auch: *Malware* oder *Malicious Software* genannt).

Schweiz dabei kein direktes Angriffsziel wäre, könnten die grenzüberschreitenden Auswirkungen (z.B. der Ausfall der Stromversorgung oder Störungen des Finanzmarktes) die Schweiz treffen.

Bis heute gibt es kein konkretes Beispiel für Terroranschläge via Cyber-Angriffe. Allerdings werden Internetauftritte von Terrororganisationen bzw. dem Terrorismus nahestehenden Organisationen laufend auf Gewaltaufrufe und Hinweise zu bevorstehenden Anschlägen überwacht (z.B. dschihadistische Webseiten).

Auch unvorhersehbare Ereignisse oder Unfälle wie Systemausfälle durch vorschnelle Abnutzung, Überbeanspruchung, Fehlkonstruktion, mangelhafte Wartung oder Folgen von Naturereignissen können Ausfälle mit ähnlich gravierenden Auswirkungen verursachen.

3 VORHANDENE STRUKTUREN

Nachfolgend wird dargelegt, über welche Strukturen die Schweiz zur Reduktion von Cyber-Risiken verfügt, und welche Rolle den einzelnen Akteuren zukommt.

3.1 Wirtschaft und Betreiber kritischer Infrastrukturen

Betroffenheit[7]

Der Wirtschaftsstandort Schweiz ist von einem starken Dienstleistungssektor geprägt. Handelsbeziehungen und andere Geschäftstätigkeiten basieren über die ganze Wertschöpfungskette auf Informations- und Kommunikationsinfrastrukturen. Daten werden auf firmeninternen und -externen Computern gespeichert und verarbeitet. Die Kommunikation und der Zahlungsverkehr basieren auf Internet-Dienstleistungen (z.B. E-Mail, Internet-Telefonie, E-Banking und Börsenhandel). Verträge werden vermehrt auf elektronischem Weg abgeschlossen (Internet-Handel, Offert-Verfahren etc.). Dies veranschaulicht die Abhängigkeit unserer Wirtschaft vom Funktionieren der von ihr genutzten IKT und weiterer kritischer Infrastrukturen, wie beispielsweise der Stromversorgung. Damit kommt dem Schutz vor Cyber-Risiken für den Wirtschaftsstandort Schweiz nationale Bedeutung zu.

Die kritischen Infrastrukturen stellen die Verfügbarkeit von zentralen Gütern und Dienstleistungen sicher. Grossflächige Störungen oder Ausfälle solcher Infrastrukturen hätten schwerwiegende Auswirkungen auf das Funktionieren von Staat, Wirtschaft und Gesellschaft. Der Schutz kritischer Infrastrukturen – auch gegenüber Cyber-Risiken – ist deshalb wichtig. Die KI-Betreiber dürfen die Risiken nicht nur nach rein ökonomischen Prinzipien handhaben, sondern müssen darüber hinausgehende Anstrengungen zur Minimierung der Risiken unternehmen. Sie sind deshalb bereits heute teilweise besonderen Regeln unterworfen; konkrete und verbindliche Vorgaben bezüglich Schutzstandards im Bereich der eingesetzten IKT fehlen aber in der Regel. In Abhängigkeit von der Kritikalität und der Verletzlichkeit einer Infrastruktur sowie der Bedrohungslage sollten die Vorgaben für Sicherheitsstandards und für weitere risikominimierende Massnahmen umfassender und genauer im Verbund mit den zuständigen behördlichen Stellen geregelt werden.

Hersteller und Lieferanten von IKT-Produkten und -Dienstleistungen tragen eine grosse Verantwortung für die Sicherheit ihrer Produkte und damit auch für die Cyber-Sicherheit ihrer Kunden.

Die Akteure der Wirtschaft handeln grösstenteils in eigener Verantwortung und nach eigenem Ermessen. Um einen Überblick zu erhalten, wurden für die Erarbeitung der Strategie ausgewählte Unternehmen zu ihren derzeitigen Einschätzungen, Massnahmen und Schwierigkeiten sowie Zukunftsperspektiven bezüglich Cyber-Sicherheit befragt.

[7] Das VBS hat Vertreter der Wirtschaft und Betreiber kritischer Infrastrukturen (inkl. Dachorganisationen und Verbände) befragt, welche Massnahmen sie für die Cyber-Sicherheit ergreifen beziehungsweise bereits ergriffen haben, wo die Mängel und Schwierigkeiten liegen und welche Faktoren ihre Schutzvorkehrungen beeinflussen (z.B. finanzielle Überlegungen). Die Befragungen haben insgesamt ein einheitliches Bild ergeben.

Wahrnehmung des Problems

Unbestritten ist, dass Cyber-Risiken für Unternehmen ein Thema sind. Die Einschätzungen der Risiken und die getroffenen Massnahmen unterscheiden sich aber stark voneinander, zwischen den Wirtschaftssektoren, aber auch innerhalb von Sektoren und Branchen sowie innerhalb der Unternehmen. Eine einfache sektorenspezifische Einteilung der Problemwahrnehmung ist deshalb nicht möglich.

Es gibt Unternehmen mit *hoher Problemwahrnehmung.* Dazu zählen mehrheitlich grosse Firmen, die über viel Kapital, Personal, Infrastruktur und spezifisches Knowhow (z.B. Forensik, Risiko- und Krisenmanagement, Computer Emergency Response Teams) verfügen. Diese Unternehmen sind in den meisten Fällen international tätig und gut vernetzt. Auch Unternehmen, die hauptsächlich in Sicherheitsbereichen tätig sind, (z.B. die Rüstungsindustrie), haben ein erhöhtes Schutzbedürfnis und sind mehrheitlich in der Lage, unkoordinierte Cyber-Angriffe, denen die Schweiz täglich ausgesetzt ist, selbstständig abzuwehren.

Zu den Akteuren, bei denen die Problemwahrnehmung ebenfalls hoch ist, gehören die KI-Betreiber. Sie erwarten gemäss Umfrage, dass die Vorgaben für Sicherheitsstandards gemeinsam mit den Aufsichtsbehörden umfassender und genauer festgelegt werden, in Abhängigkeit von der Kritikalität und Verletzlichkeit einer Infrastruktur.

Die grösste Gruppe bilden kleine und mittlere Unternehmen mit einer *durchschnittlichen Problemwahrnehmung*. Diese verwenden meistens kommerziell erhältliche Sicherheitsinfrastrukturen und -konzepte (z.B. Firewalls, Antivirenprogramme). Ihre Fähigkeit zur Verbesserung der Schutzvorkehrungen im Cyber-Bereich ist primär durch die finanziellen Mittel begrenzt.

Eine weitere Gruppe bilden Unternehmen, die eine *tiefe Problemwahrnehmung* haben. Für Schutzmassnahmen gegenüber Cyber-Risiken fehlen die Ressourcen oder das Verständnis für deren Notwendigkeit.

Massnahmen

Die wenigsten der befragten Akteure aus der Wirtschaft können einen gezielten Cyber-Angriff hoher Intensität (in Bezug auf Gleichzeitigkeit, Komplexität, Schadenspotenzial und Dauer) abwehren.

Viele Unternehmen kennen Sicherheitsstandards (z.B. ISO 2700x, NERC) und wenden diese an. Auch sind technische und organisatorische Vorkehrungen vorhanden (z.B. Betrieb von autonomen Systemen, Einsatz von Sicherheitsbeauftragten). Weiter werden Massnahmen zur Verbesserung des Sicherheitsbewusstseins der Mitarbeitenden ergriffen; oft werden dabei aber die Entscheidungsträger vernachlässigt. Die Massnahmen tragen dazu bei, dass betriebsinterne Schwachstellen identifiziert und Schutzmassnahmen kontinuierlich und langfristig verbessert werden. Die grosse Masse der KMU tut aber wenig für ihre Sicherheit. Die Inkaufnahme von Risiken ist oft durch rein ökonomische Überlegungen bestimmt. Cyber-Risiken sind ein integraler Bestandteil von gesamtheitlichen Unternehmensprozessen und können folglich nicht isoliert (voneinander) oder nur auf technischer Ebene angegangen werden. Kommt hinzu, dass die Informationsgrundlagen zur Entscheidfindung häufig lückenhaft sind und cyber-spezifische Angaben marginal / am Rande vorkommen. Um ein möglichst lückenloses und kein wettbewerbsverzerrendes Schutzniveau zu erreichen, erwarten Unternehmen und KI-Betreiber, dass Vorgaben und Normen einheitlicher und in Zusammenarbeit aller Betroffenen und Verantwortlichen erarbeitet und umgesetzt werden.

Die Optimierung des Informationsaustausches zwischen den Akteuren der Wirtschaft wie auch den IK-Betreibern und den Behörden ist für die Problemlösung und Schadensminimierung entscheidend. Bislang wird aber anscheinend wenig über die Firmengrenzen hinaus (inkl. Behörden) zusammengearbeitet. Die grossen Wirtschaftsverbände haben sich bislang mit dem Thema Cyber-Sicherheit und ihrer diesbezüglichen Rolle zu wenig befasst. Gemäss Befragung besteht das Bedürfnis, dass insbesondere zum Austausch von Lageinformationen und Massnahmen zum Krisenmanagement Zusammenarbeitsformen zwischen Wirtschaft und Behörden weiterentwickelt und ausgebaut werden[8]. Oft werden festgestellte Cyber-Angriffe aber verschwiegen; damit wird anderen potenziell Betroffenen eine rechtzeitige Warnung vorenthalten. Die befragten Unternehmen und KI-Betreiber fordern Zusammenarbeitsformen, die mehrheitlich auf Freiwilligkeit basieren. Die Eigenverantwortung bleibt zentral; Zusammenarbeit soll aber dazu beitragen, Lücken gemeinsam zu schliessen und lagerelevante Informationen zur Unterstützung des eigenen Risiko-Managements zu erhalten.

In der Zusammenarbeit zwischen den IK-Betreibern und dem Bund zur Reduzierung von Cyber-Risiken wurden in den letzten Jahren Fortschritte erzielt: Bei der langfristigen, strategischen Planung, Risikoanalyse und dem Kontinuitätsmanagement findet eine Zusammenarbeit zwischen dem Bundesamt für wirtschaftliche Landesversorgung, den Kantonen und Teilen der kritischen Infrastrukturen statt. Überdies besteht zwischen der Melde- und Analysestelle Informationssicherung (MELANI) des Bundes, den Kantonen und der Privatwirtschaft eine funktionierende *Public Private Partnership* (PPP), wobei MELANI die KI-Betreiber der Schweiz in ihrem Informationssicherungsprozess unterstützt und den Informationsaustausch zu Cyber-Angriffen unter den Unternehmen fördert. 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 und wie sich dies im Hinblick auf die Ressourcen auswirkt..

Knappe Gewinnmargen und starke internationale Konkurrenz erlauben es nicht, schärfere Sicherheitsanforderungen festzulegen, die nur für die Schweiz gelten. Die daraus entstehenden Mehrkosten würden der Schweizer Wirtschaft einen Wettbewerbsnachteil bescheren. Es wird deshalb erwartet, dass Schutzvorgaben und Umsetzungslösungen in einem internationalen Kontext erarbeitet werden. Die internationale Kooperation ist jedoch nicht nur in Bezug auf Normen und Vorschriften zu intensivieren, sondern auch zur Risikoerkennung und für gemeinsames Krisenmanagement. Dabei sind nicht nur staatliche Akteure, sondern auch Vertreter der Wirtschaft und Gesellschaft einzubeziehen.

Eine grosse Herausforderung ist der Mangel an Fachkräften und die Beschaffung sowie der Erhalt von spezialisiertem Wissen. Die befragten Unternehmen und KI-Betreiber erwarten, dass die Forschung und Entwicklung von spezialisiertem Wissen wie auch die Ausbildung und Rekrutierung von Fachkräften gefördert wird.

[8] Vgl. dazu die Studie „Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz (MELANI)“, die von der ETH Zürich 2010 veröffentlicht wurde. Die Studie überprüft die Wirksamkeit von MELANI, stellt einen Vergleich mit internationalen Modellen zur Informationssicherung dar und leitete daraus Weiterentwicklungsmöglichkeiten und Empfehlungen ab.

3.2 Bund

In den letzten Jahren hat der Bund diverse Massnahmen ergriffen, um Schutzdispositiv und Mittel der Bundesverwaltung gegen Cyber-Angriffe zu verstärken. Auf Stufe Bund befassen sich verschiedene Stellen mit Cyber-Sicherheit:

Bundesanwaltschaft (BA)

Die BA ist Ermittlungs- und Anklagebehörde des Bundes. Sie ist zuständig für die Verfolgung strafbarer Handlungen, die der Bundesgerichtsbarkeit unterstehen (der weitaus grösste Teil der Delikte fällt in die Zuständigkeit der Kantone) sowie für die Kooperation mit dem Ausland.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Der EDÖB ist eine Aufsichts- und Beratungsstelle für Bundesorgane und Privatpersonen. In seiner Funktion erläutert er insbesondere das Datenschutzgesetz und die Vollzugsverordnungen. Er berät sowohl in rechtlichen Fragen, als auch in technischen Aspekten der Datensicherung.

Bundeskriminalpolizei (BKP)

Die BKP ist Ermittlungsbehörde des Bundes. In ihrem Zuständigkeitsbereich stellt sie die Zusammenarbeit zwischen den in- und ausländischen Partnern sicher und verfolgt insbesondere die technische Entwicklung im Bereich Cyberkriminalität. Sie stellt den Erhalt und die Entwicklung des technischen bzw. forensischen Wissens in diesen Bereichen sicher. Die BKP ist dann zuständig, wenn ein Ereignis in die Bundeskompetenz fällt. Ist die Zuständigkeit des Bundes oder eines Kantons noch nicht geklärt, kann sie erste Ermittlungstätigkeiten durchführen. Sie übernimmt auch die Koordination von überkantonalen Verfahren.

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)

KOBIK ist eine von Bund und Kantonen gemeinsam betriebene Stelle, die dafür zuständig ist, Straftaten im Internet rechtzeitig zu erkennen, Doppelspurigkeiten bei der Strafverfolgung zu vermeiden und die Internetkriminalität zu analysieren[9]. KOBIK ist bei der BKP angesiedelt. Sie ist die zentrale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Die Meldungen werden nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. KOBIK steht der Öffentlichkeit, Behörden und Internet-Dienstleistern für kriminalistische, rechtliche und technische Fragen zur Internetkriminalität zur Verfügung. KOBIK hält auch aktiv im Netz nach kriminellen Inhalten Ausschau. Sie ist zuständig für die ermittlungstechnische Entwicklung und – mit Unterstützung der Kantone – für die landesweite Übersicht der Verfahren sowie die Beobachtung der Rechtsentwicklung im Bereich der Internetkriminalität. Sie ist ausserdem Ansprechpartnerin für ausländische Stellen mit analogen Aufgaben. Zusammen mit MELANI stellt die KOBIK den cyber-relevanten Informationsaustausch zwischen Strafverfolgungsbehörden und dem Nachrichtendienst sicher. Weil KOBIK über wenig Ressourcen verfügt, kann sie die Erstellung einer Verfahrensübersicht und die damit verbundene Koordination nicht ohne Unterstützung der Kantone gewährleisten.

[9] Vergleiche dazu die Verwaltungsvereinbarung zum koordinierten Vorgehen bei der Bekämpfung der Internetkriminalität vom 19. Dezember 2001 und die Geschäftsordnung für die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) vom 30. März 2011.

Einsatzzentrale des Bundesamts für Polizei

Die Einsatzzentrale des Bundesamts für Polizei ist die permanente Kontaktstelle für ausländische Behörden. Sie unterstützt nationale und internationale Strafuntersuchungen in Fällen von Computerkriminalität. Die Kontaktstelle kann selbst keine Massnahmen in den Bereichen juristische Beratung, Rechtshilfe, Beweiserhebung, Datensicherung oder Strafuntersuchung ergreifen. Sie hat aber den Auftrag, als Anlaufstelle den Kontakt zwischen den mit den jeweiligen Aufgaben betrauten ausländischen und inländischen Behörden (insbesondere KOBIK) zu erleichtern.

Nachrichtendienst des Bundes (NDB)

Der NDB beschafft mit nachrichtendienstlichen Mitteln Informationen, die analysiert, ausgewertet und verbreitet werden. Er konzentriert sich im Inland auf die Themen Terrorismus, gewalttätiger Extremismus, Proliferation, Angriffe auf die kritischen Infrastrukturen und verbotenen Nachrichtendienst, im Ausland auf Proliferation, Terrorismus, Streitkräfteentwicklung, Einsatzgebiete der Armee im Ausland sowie Rüstungstechnologie und Rüstungshandel. Diese Themengebiete weisen eine immer stärkere Cyber-Ausprägung auf. Um diese zu erfassen, verfolgt der NDB auch die Entwicklung der Risikolage im Cyber-Bereich. Der NDB führt in Zusammenarbeit mit dem Informatiksteuerungsorgan des Bundes (ISB) den nachrichtendienstlichen Teil der Melde und Analysestelle für die Informationssicherung (MELANI).

Melde- und Analysestelle Informationssicherung (MELANI)

MELANI ist ein Organ, das vom ISB (Steuerung MELANI und *Government Computer Emergency Response Team, GovCERT*[10]) und dem Nachrichtendienst des Bundes (Operations- und Informationszentrum) gemeinsam betrieben wird. MELANI unterstützt subsidiär den Informationssicherungsprozess der kritischen Infrastrukturen durch Informationen über Vorfälle und Bedrohungen. Sie beschafft technische und nicht technische Informationen, wertet diese aus und leitet die relevanten Daten an die KI-Betreiber weiter. Dadurch unterstützt MELANI den Risikomanagement-Prozess innerhalb der kritischen Infrastrukturen, indem sie beispielsweise Lageeinschätzungen und Analysen zur Früherkennung von Angriffen oder Vorfällen anbietet, deren Auswirkungen auswertet und bei Bedarf Schadprogramme untersucht.

MELANI betreut zurzeit einen geschlossenen Kundenkreis, bestehend aus ausgesuchten Unternehmen, die kritische Infrastrukturen für die Schweiz betreiben (ca. 100 Mitglieder wie z.B. Banken, Telekommunikationsunternehmen und Energieversorger). Für die übrige Wirtschaft und die breite Bevölkerung bietet MELANI Unterstützung in Form von Checklisten, Anleitungen und Lernprogrammen an. In einer Krise ist MELANI im Bereich Informationssicherung für die Alarmierung und Führungsunterstützung des Sonderstabs Informationssicherung (SONIA) zuständig. Der Grundauftrag von MELANI kann aber zurzeit wegen ungenügender personeller Ressourcen nicht vollumfänglich erfüllt werden.

Bundesamt für Bevölkerungsschutz (BABS)

Der Zweck des Bevölkerungsschutzes ist es, die Bevölkerung und ihre Lebensgrundlagen bei Katastrophen und in Notlagen sowie im Falle bewaffneter Konflikte zu schützen und so wesentlich zur Begrenzung und Bewältigung von Schadenereignissen beizutragen. Katastrophen und Notlagen können auch aus schwerwiegenden Cyber-Angriffen oder anderweitigen Störungen der IKT resultieren. Im Rahmen des Programms zum Schutz Kritischer Infrastrukturen koordiniert das BABS im Auftrag des Bundesrates die Arbeiten zur Erstellung des SKI-Inventars, indem zum einen die Kritischen IKT-Infrastrukturen, aber auch die sicherheitsrelevanten IKT-Anwendungen in den anderen KI-Sektoren erfasst werden. Als Melde- und Lagezentrum des Bundes für ausserordentliche Ereignisse ist die Nationale Alarmzentrale (NAZ) des BABS auch in Krisensituationen zwingend auf funktionierende Informatiksysteme, Kommunikationsnetze und damit auf eine unterbruchfreie Stromversorgung angewiesen; diese wird erst teilweise durch Notstromversorgungen sichergestellt. In Zukunft soll die Führungskommunikation zwischen Bundes- und Kantonsstellen (POLYCONNECT/POLYDATA) über krisen- und stromsichere Netze erfolgen, die dank entsprechender Verschlüsselung geschützt ist. Die Warnung und Alarmierung (POLYALERT) wird zur Zeit ebenfalls auf eine krisensichere Technologie überführt, die auf dem Sicherheitsnetz Funk der Schweiz (POLYCOM) basiert.

Bereich Verteidigung

Der Bereich Verteidigung des VBS ist verfassungsrechtlich für die Verteidigung, Unterstützung ziviler Behörden und Friedensförderung über alle Lagen verantwortlich. Dazu baut er Mittel auf, um diese Auftragserfüllung sicherzustellen.

[10] CERT sind Organisationen, die für vorfallübergreifende technische Analysen zuständig sind. Sie sammeln und werten technisches Wissen im Gesamtrahmen einer Vorfallsreihe aus. Sie nehmen auch eine koordinierende Rolle ein. Auf Stufe Bund heisst diese Organisation GovCERT, die zusätzlich eine koordinierende Rolle bei internationalen Vorfällen wahrnimmt.

Für die verteidigungsbezogenen Schutzaufgaben sind insbesondere die folgenden Organisationen zuständig:

Informations- und Objektsicherheit (IOS)

Die beim Armeestab angesiedelte IOS betreut die integrale Sicherheit des VBS. Sie ist insbesondere für die Vorgaben im Bereich der Sicherheit von Personen, Informationen, Informatik und Sachwerten (Material und Immobilien) zuständig.

In dieser Rolle erarbeitet sie Sicherheitsvorgaben, um die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen und Daten sowie die Verfügbarkeit und die Integrität von IKT-Mitteln sicherzustellen.

Sie betreibt die Koordinationsstelle für den Informationsschutz im Bund und ist Ansprechstelle für nationale und internationale Fragen bezüglich des Schutzes von klassifizierten Informationen. Aufgrund einiger internationaler Abkommen (insbesondere mit der EU) gilt die IOS als nationale Sicherheitsbehörde für alle Belange der Informationssicherheit.

Sie ist bei der Erarbeitung eines Gesetzes über die Informationssicherheit im Bund federführend.

Führungsunterstützungsbasis der Armee (FUB)

Die FUB ist IKT-Leistungserbringerin für die Armee über alle Lagen, was hohe Verfügbarkeit und Sicherheit verlangt. Sie betreibt das Zentrum für elektronische Operationen (ZEO), das Leistungen für die Nachrichtendienste erbringt. Das ZEO beschäftigt Kryptologen und betreibt den Bereich für Computer-Netzwerk-Operationen (CNO), der damit über technische Fähigkeiten zur Analyse der Bedrohung und der Vorfälle und zur Operationsführung verfügt. Die FUB betreibt zudem das militärische Computer Emergency Response Team (milCERT), das die für die Armee relevanten IKT-Infrastrukturen überwacht. Die FUB unterstützt primär die Armee aber auch die zivile/politische Führung (VBS und mehr) und hat damit auch entsprechende Mittel zur Verfügung zu halten (ZEO zu Gunsten NDB, Redundanzen, Übermittlungsmittel)

Informatiksteuerungsorgan des Bundes (ISB)

Das Informatiksteuerungsorgan des Bundes (ISB) erlässt Vorgaben bezüglich IKT und übernimmt die zentrale Führung der Informatikleistungen, die in der Bundesverwaltung verwendet werden (z.B. Telekommunikation). Es führt das GovCERT und den strategischen Teil von MELANI. In der Krise leitet es den SONIA. Bei einem Angriff auf die Informatik- und Kommunikationsinfrastrukturen der Bundesverwaltung kann das ISB zusätzliche Sicherheitsmassnahmen ergreifen.

Sonderstab Informationssicherung (SONIA)

Der Sonderstab Informationssicherung umfasst Entscheidungsträger aus Verwaltung und Wirtschaft (KI-Betreiber), wird vom Delegierten für die Informatiksteuerung des Bundes geleitet und tritt bei nationalen Krisen im Bereich der Informationssicherung auf Antrag von MELANI zusammen. SONIA ist heute nur bedingt handlungsfähig, weil nach der letzten Übung im Jahr 2005 festgestellt wurde, dass Struktur, Prozesse und Aufbau in der Praxis nicht funk-

tionsfähig sind; die vorgesehenen Mitglieder des Stabes sind im Ereignisfall in der Regel bereits in übergeordneten Krisenmanagementprozessen engagiert.

Bundesamt für Informatik und Telekommunikation (BIT)

Das BIT ist ein Informatik- und Telekommunikationsleistungserbringer für die Bundesverwaltung. Es kann in der normalen Lage bei Vorfällen in Netzwerken des Bundes eine genügende Leistung für Prävention und Reaktion erbringen (Computer Security Incident Response Team, CSIRT[11]). Erhöht sich jedoch die Anzahl der Aufgaben oder die Intensität der Angriffe bzw. das Schadenspotenzial, fehlen dem BIT die personellen Ressourcen für die Leistungserbringung.

Wirtschaftliche Landesversorgung (WL)

Die WL ist eine Milizorganisation mit vollamtlicher Stabsorganisation und Sekretariat (Bundesamt für wirtschaftliche Landesversorgung, BWL). Sie verfügt über eine Kaderorganisation aus Vertretern der Wirtschaft. Der Bereich ICT-Infrastrukturen (ICT-I) der WL ist zuständig für die Sicherstellung der für die Versorgung des Landes notwendigen Informationsinfrastruktur (Datenproduktion, -übertragung, -sicherheit und -verfügbarkeit) und die Fernmeldeverbindungen, insbesondere mit dem Ausland. Er definiert die systemrelevanten Versorgungsinfrastrukturen der Schweiz und erstellt für diese ein Kontinuitätsmanagement. Der Bereich ICT-I beobachtet und analysiert fortlaufend die allgemeinen Risiken der Datenübertragung, -sicherheit und -verfügbarkeit. Er trifft für den Notfall Massnahmen zur Sicherstellung geeigneter Fernmeldeverbindungen mit mobilen Teilnehmern im Ausland, die für die Landesversorgung von Bedeutung sind. Er bereitet Massnahmen zur Sicherstellung lebenswichtiger Informations- und Kommunikationsinfrastrukturen vor und erstellt die für die Sicherstellung der Grundversorgung erforderliche Bereitschaft. Er vertritt auch die bereichsspezifischen Interessen der wirtschaftlichen Landesversorgung in internationalen Organisationen.

Erkenntnisse

Die Strukturen auf Stufe Bund zur Bewältigung von Cyber-Risiken sind bisher dezentral organisiert. Es werden relativ geringe Mittel aufgewendet. Die Aufgaben sind zumeist in jenen Organisationseinheiten angesiedelt, deren Aufträge eine starke Cyber-Ausprägung aufweisen. Dieser Ansatz hat gewisse Vorteile und entspricht der Annahme, dass die Cyber-Problematik kein abgegrenztes Phänomen darstellt; er ermöglicht flexible Lösungen, begünstigt Synergien und verhindert, dass aufwendige Gremien etabliert werden, bevor über ein Problem und dessen tatsächliche Dimension Klarheit besteht. Das bestehende System funktioniert denn auch reaktiv gut in einer relativ entspannten Lage. Gewisse antizipative und präventive Fähigkeiten sind vorhanden; diese reichen aber bei Weitem nicht aus (z.B. personelle und finanzielle Ressourcen; Austausch von nachrichtendienstlichen, technischen und polizeilichen Informationen zur Unterstützung der Wirtschaft und KI-Betreiber, Forschung; Risikoanalysen und daraus folgende Definitionen von Sicherheitsanforderungen, Durchhaltefähigkeit). Es stellt sich deshalb die Frage, inwieweit die dezentralen Strukturen auf Stufe Bund verstärkt und mögliche Synergien besser genutzt werden müssen, um Cyber-Risiken umfassend identifizieren zu können und grösseren Cyber-Angriffen zu genügen.

[11] Dieses Organ ist auf Vorfälle fokussiert und stellt sicher, dass das Tagesgeschäft in einer bestimmten Verwaltungseinheit reibungslos funktioniert.

3.3 Kantone

Wie die Wirtschaft sind auch die Kantone von grosser Heterogenität geprägt. Es gibt Kantone, die bezogen auf die Bevölkerung kaum grösser sind als mittelgrosse Städte. Auch wirtschaftlich und strukturell sind grosse Unterschiede zu verzeichnen. So unterschiedlich deren Strukturen, Aktivitäten oder Leistungserbringung (z.B. Gesundheit, Transport, Energie) sind, so unterschiedlich sind auch deren Anforderungen im Umgang mit Gefahren und Bedrohungen. Es ist deshalb nachvollziehbar, dass nicht alle Kantone qualitativ und quantitativ über die gleichen Kompetenzen verfügen, die es braucht, um Risiken, insbesondere im Cyber-Bereich, zu bekämpfen.

Die Kantone sind auf ihrem Hoheitsgebiet für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung verantwortlich. Nur jene Kantone, die über grosse Polizeikorps verfügen und eine enge Zusammenarbeit mit Wirtschaft, Hochschulen und anderen im Sicherheitsbereich tätigen Organisationen (z.B. Zoll, Sicherheitsdienste von Nachbachländern) pflegen, haben die Fähigkeit, im Bereich der Cyber-Kriminalität Probleme zu antizipieren und sich die notwendigen Informationen zu beschaffen. Kein Kanton ist aber in der Lage, dies systematisch zu tun. Alle Kantone sind deshalb auf die subsidiäre Unterstützung des Bundes angewiesen – insbesondere für polizeiliche, juristische und nachrichtendienstliche Belange.

Die präventiven Vorkehrungen der Kantone zur Minimierung von Cyber-Risiken hängen in erster Linie davon ab, ob die Kantone kritische Infrastrukturen betreiben. Ist dies der Fall, verfügen sie mehrheitlich über Organisations- und Kontrollstrukturen, Sicherheitsbeauftragte in den verschiedenen Diensten, IT-Polizeiforensiker oder spezialisierte Führungszellen im Krisenfall. Wie auf Stufe Bund sind diese Mittel aber oft ungenügend koordiniert und reichen nicht aus, um den heutigen Cyber-Risiken umfassend zu begegnen. Das Problem akzentuiert sich in kleineren Kantonen, die oftmals gezwungen sind, spezifische Dienstleistungen an Dritte zu delegieren.

Weiter ist festzustellen, dass die rechtlichen Regelungen in Bezug auf Informationstechnologien häufig entweder nicht ausreichend oder nicht bekannt genug sind. Klassifizierungssysteme (intern, vertraulich, geheim) werden praktisch nicht angewendet, und sensible Daten (personelle, polizeiliche oder juristische Daten) werden auf ungenügend geschützten Systemen bewirtschaftet.

Manche Kantone sensibilisieren die Bevölkerung im Sinne der Prävention bereits heute mit spezifischen Kampagnen für die Gefahren im Internet, zum Beispiel in den Schulen. Im interkantonalen Kontext ist die Schweizerische Kriminalprävention in derselben Richtung tätig. Viele Kantone sind aber noch inaktiv oder verlassen sich in diesem Bereich auf Einzelinitiativen von Lehrkräften oder Bildungsinstitutionen, die nicht aufeinander abgestimmt sind. Ausserdem werden Programmangebote der IKT-Branche wenig genutzt, weil sie zum Teil nicht bekannt sind.

Den Kantonen stehen Führungsorganisationen zur Verfügung, um auf Cyber-Angriffe zu reagieren. Diese Stäbe werden mit Partnern (z.B. mit den militärischen Kommandos der Territorialregionen) regelmässig beübt und sind in der Lage, die Auswirkungen von Krisen aller Art zu bewältigen. Sie sind aber nicht spezifisch auf Cyber-Risiken ausgerichtet und wären wohl häufig nicht in der Lage, die Wirtschaft und die Bevölkerung bei Cyber-Angriffen kompetent zu unterstützen.

Für die Umsetzung der nationalen Strategie zum Schutz vor Cyber-Risiken verfügen die Kantone und der Bund über mehrere Instrumente, die in diesem Bereich wertvolle Beiträge leisten können:

- das Haus der Kantone mit mehreren interkantonalen Regierungs- und Direktorenkonferenzen für Justiz, Polizei, Bevölkerungsschutz, Erziehung, Finanzen, Gesundheit etc. und weiteren Institutionen wie der Schweizerischen Kriminalprävention;
- der Sicherheitsverbund Schweiz, der im Aufbau begriffen ist und die Aktivitäten der Kantone und des Bundes im Bereich Sicherheit koordinieren und bündeln wird;
- das Programm zur Harmonisierung der Polizeiinformatik mit dem Ziel, Applikationen aufeinander abzustimmen und somit die Arbeit der Polizei zu erleichtern;
- die von Bund und Kantonen gemeinsam finanzierte und betriebene Stelle zur Bekämpfung der Internetkriminalität (KOBIK), die den Cyber-Bereich überwacht und den Kantonen Informationen im Hinblick auf die Aufnahme von polizeilichen Ermittlungen liefert;
- Ergänzend zu den staatlichen Organen und Gremien besteht der Verein Swiss Police ICT, der verschiedene Polizeikorps und die ICT-Wirtschaft direkt und fachspezifisch vernetzt. Sein Kongress, der Schweizer Polizei Informatik Kongress (SPIK), leistet als Plattform einen wichtigen Beitrag für den Informationsaustausch über die Polizeiinformatik und die Bewältigung von Cyber-Risiken.

3.4 Bevölkerung

Bei der privaten Nutzung von Informations- und Kommunikationssystemen ist der einzelne Anwender grundsätzlich selber für die Sicherheitsvorkehrungen verantwortlich. In der Regel sind die auf dem Endverbrauchermarkt erhältlichen Sicherheitswerkzeuge im Einsatz (z.B. Virenscanner und Router mit eingebauter Firewall, Wireless-Local-Area-Network- Verschlüsselung).

Massnahmen zur allgemeinen Verbesserung der Sicherheit auf privaten IKT-Systemen wie auch die Angebote für die individuelle Ausbildung und Information sind nicht koordiniert und nicht auf einen gemeinsamen Sicherheitsstandard ausgerichtet. Da ein zunehmender Teil der Bevölkerung auch auf schützenswerten Rechnern in Unternehmen arbeitet, ist zur Erhöhung des gesamten Schutzes eine Sensibilisierung über Cyber-Risiken und sichere Verhaltensweisen wünschbar, analog zu anderen Präventionstätigkeiten.

3.5 Internationale Kooperation auf staatlicher Ebene

Die Direktion für Völkerrecht des Eidgenössischen Departements für auswärtige Angelegenheiten verfolgt die internationalen Entwicklungen auf völkerrechtlicher Ebene, namentlich den Zusammenhang zwischen dem Einsatz von Cyber-Mitteln in zwischenstaatlichen Konflikten und dem humanitären Völkerrecht.

In verschiedenen Initiativen werden zurzeit internationale Regelungen diskutiert, mit denen der permanente Informationsaustausch über Technologien, Schutzmassnahmen, Risikoentwicklung und Täterschaften institutionalisiert, eine effizientere Amts- und Rechtshilfe in Strafverfolgungsverfahren sowie die Entwicklung und Umsetzung gemeinsamer Sicherheitsmassnahmen ermöglicht würden.

In den letzten Jahren haben viele Länder umfassende Cyber-Strategien verabschiedet (z.B. Deutschland, Frankreich, die Niederlande), während sie sich zuvor nur in ausgewählten bi- und multilateralen Aktivitäten und Themenbereichen engagierten. Es gibt einzelne Staaten, die mittlerweile eine breite Palette von Instrumentarien einsetzen, um sich vor Cyber-Risiken

zu schützen (z.B. nationale Strategien, Massnahmen und Abwehrzentren mit Führungsstrukturen). Ein periodischer Vergleich mit diesen Strategien ist angezeigt. Gerade auch im Hinblick auf die Tatsache, dass die Schweiz einen Ansatz wählt, der Mängel in der Wahrnehmung der Cyber-Ausprägung innerhalb bestehender Geschäfts-, Produktions- und Verwaltungsprozesse und fehlende operative Zusammenarbeit nicht einfach mit der Schaffung einer zentralen Koordinationsplattform zu lösen sucht, sondern innerhalb der zuständigen und verantwortlichen Stellen und Strukturen über alle Ebenen.

3.6 Rechtliche Grundlagen

Rechtliche Grundlagen für den Cyber-Bereich finden sich heute in einer Vielzahl von Bundesgesetzen und Verordnungen. Dies ist in erster Linie eine logische Konsequenz, da mit zunehmender Vernetzung und Einsatz von Kommunikationsmitteln auch eine zunehmende Cyber-Ausprägung bestehender Aufgaben und Verantwortlichkeiten einhergeht, die sich in den jeweiligen Gesetzen und Verordnungen niederschlagen. Problematisch dabei ist, dass diese Regelungen kaum aufeinander abgestimmt und zum Teil noch lückenhaft sind.

Die Informationsschutzvorgaben für Bundesverwaltung und Armee hat der Bundesrat in der bis zum 31. Dezember 2014 befristeten Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes zusammengefasst. Die Parlamentsdienste, die Gerichte des Bundes, die Bundesanwaltschaft sowie Dienststellen der Kantone, die vom Bund Informationen erhalten, werden davon jedoch nicht oder nur beschränkt erfasst.

Die Informatiksicherheit der Bundesverwaltung ist in der Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung nur summarisch geregelt. Die meisten Grundsätze und Sicherheitsvorgaben sind auf Weisungsebene (Weisungen des Informatikrats des Bundes über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004)[12] zu finden.

Das Bundesgesetz über den Datenschutz (DSG)[13] und die Verordnung zum Bundesgesetz über den Datenschutz (VDSG)[14] enthalten allgemein gültige Mindestanforderungen an die Datensicherheit im Umgang mit Personendaten, die für den Bund und Private gelten.

Das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), das sich insbesondere mit Massnahmen für die Erkennung und Bekämpfung von Terrorismus, verbotenem Nachrichtendienst, gewalttätigem Extremismus und Gewalt anlässlich von Sportveranstaltungen befasst, trägt mit den Personensicherheitsüberprüfungen auch zur Informationssicherheit innerhalb der Bundesbehörden bei.

Das Bundesgesetz über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes (ZNDG)[15] regelt Teile der Aufgaben des zivilen Nachrichtendienstes des Bundes. Zu den Tätigkeiten gehören die Beschaffung sicherheitspolitisch relevanter Informationen über das Ausland und deren Auswertung zuhanden der Departemente und des Bundesrates sowie die Wahrnehmung nachrichtendienstlicher Aufgaben im Bereich der inneren Sicherheit.

---

[12] Weisungen des Informatikrats des Bundes (IRB) über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004 (Stand 1. November 2007).

[13] SR 235.1 Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2011).

[14] SR 235.11 Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 1. Dezember 2010).

[15] SR 121 Bundesgesetz über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 3. Oktober 2008 (Stand am 1. Januar 2010).

Mit Beschluss vom 12. Mai 2010 hat der Bundesrat das VBS beauftragt, formell-gesetzliche Grundlagen für den Informationsschutz und die Informationssicherheit zu erarbeiten. Neu sollen Informationsschutz und Informationssicherheit in einem Spezialgesetz einheitlich geregelt werden. Das zu erlassende Gesetz muss nicht nur die Vertraulichkeit von Informationen, sondern auch deren Integrität, Verfügbarkeit und Nachvollziehbarkeit schützen sowie die Sicherheit der Mittel, mit denen diese Informationen bearbeitet werden, gewährleisten.

Das Fernmeldegesetz (FMG)[16] stellt zusammen mit den ausführenden Verordnungen, Vorschriften und Richtlinien sicher, dass der Bevölkerung und der Wirtschaft vielfältige, preiswerte, qualitativ hochstehende sowie national und international konkurrenzfähige Fernmeldedienste angeboten werden. Laut Zweckartikel des FMG muss die Grundversorgung eine „zuverlässige" sein. Verbindliche Qualitätsanforderungen an die Grundversorgung ergeben sich aus der Verordnung über Fernmeldedienste (FDV)[17] und den entsprechenden Vorschriften des BAKOM. Des Weiteren soll das FMG einen „störungsfreien, die Persönlichkeits- und Immaterialgüterrechte achtenden Fernmeldeverkehr sicherstellen".

Das FMG und die FDV enthalten je ein Kapitel über „wichtige Landesinteressen", das jeweils verschiedene sicherheitsrelevante Bestimmungen enthält. Davon abgeleitet hat das BAKOM Richtlinien erlassen, die Massnahmen zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und –diensten empfehlen.

Bezüglich der Sicherheit der Fernmeldedienste selbst ist zudem festzuhalten, dass die gesetzlich verlangten Vorkehrungen lediglich das technisch einwandfreie Funktionieren der Anlagen betreffen. Das FMG sieht zwar die „Sicherheit und Verfügbarkeit der Fernmeldeinfrastrukturen und -dienste" vor, zudem sind Zuverlässigkeit und Störungsfreiheit im Gesetz und in weiteren Verordnungen geregelt. Wie genau der Schutz der Fernmeldedienste – und damit der Telekommunikation und der Informationstechnologien – vor äusseren Risiken oder Naturereignissen gewährleistet wird, ist in den Gesetzen nicht definiert[18].

Das Landesversorgungsgesetz (LVG)[19] und die zugehörigen Verordnungen[20,] regeln die vorsorglichen Massnahmen der wirtschaftlichen Landesverteidigung sowie die Massnahmen zur Sicherstellung der Landesversorgung mit lebenswichtigen Gütern und Dienstleistungen bei schweren Mangellagen, denen die Wirtschaft nicht selber begegnen kann. Dabei ist der Bereich ICT-Infrastruktur für die Sicherstellung der Informationsinfrastrukturen (z.B. Datensicherheit und -übertragung) und die Fernmeldeverbindungen mit dem Ausland zuständig. Derzeit wird eine Vorlage zu einer umfassenden Revision des Landesversorgungsgesetzes ausgearbeitet. Die Neuausrichtung sieht einen Wechsel von der Sicherheits- zur Risikologik, eine Erhöhung der Widerstandsfähigkeit lebenswichtiger Wirtschaftszweige und die Verlagerung der Schwerpunkte von Gütern zu Dienstleistungen vor.

Das Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) [21] und die Strafprozessordnung (StPO) ermöglichen bei einem dringendem Tatverdacht die Auf-

---

16 SR 784.10 Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. Juli 2010).

17 SR 784.101.1 Verordnung über Fernmeldedienste (FDV) vom 9. März 2007 (Stand 1. März 2012).

18 Crisis and Risk Network (CRN), Center for Security Studies (CSS) (2011): "Die rechtlichen Grundlagen zum Schutz Kritischer Infrastrukturen in der Schweiz" (in Bearbeitung; im Auftrag des BABS).

19 SR 531 Bundesgesetz über die wirtschaftliche Landesversorgung (LVG) vom 8. Oktober 1982 (Stand am 1. Januar 2011).

20 SR 531.11 Verordnung über die Organisation der wirtschaftlichen Landesversorgung (Organisationsverordnung Landesversorgung) vom 6. Juli 1983 (Stand 6. Juli 2003); SR 531.12 Verordnung über die Vorbereitungsmassnahmen der wirtschaftlichen Landesversorgung vom 2. Juli 2003 (Stand am 22. Juli 2003).

21 SR 780.1 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000 (Stand am 1. Januar 2011).

zeichnung der Post- und Telekommunikation, inklusive E-Mail. Gesetzlich zulässig ist zudem eine rückwirkende Erhebung von Verkehrs- und Rechnungsdaten sowie eine Teilnehmeridentifikation.

Die Europaratskonvention über die Cyberkriminalität, die am 1. Januar 2012 in der Schweiz in Kraft getreten ist, verpflichtet die Vertragsstaaten, Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mit Hilfe eines Computers oder das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen. Die Konvention regelt, wie in der Strafuntersuchung Beweise in Form von elektronischen Daten erhoben und gesichert werden. Die Untersuchungsbehörden sollen rasch auf elektronisch bearbeitete Daten zugreifen können, damit diese im Laufe des Verfahrens nicht verfälscht oder vernichtet werden. Das Schweizerische Strafgesetzbuch findet mit seinen Strafnormen, insbesondere den Bestimmungen des sogenannten Computerstraftrechts, Anwendung auf Fälle von Cyberkriminalität. Die Europaratskonvention regelt auch die internationale Zusammenarbeit in Strafsachen zwischen den Staaten (z.B. Rechtshilfe und Auslieferung). Das Zusammenwirken zwischen den verschiedenen Ländern soll im Ablauf schnell und effizient gestaltet werden.

3.7 Fazit

Die Analyse der bestehenden Strukturen zeigt, dass in der Wirtschaft, beim Bund und bei den Kantonen viele Fähigkeiten vorhanden sind, die es erlauben, die Cyber-Ausprägung der bestehenden Aufträge und Verantwortlichkeiten zu erfassen und damit einhergehende Risiken zu identifizieren. Es bestehen auch Ansätze und Konzepte zur Verbesserung der Cyber-Sicherheitslage und Gefässe, die den Informationsaustausch und die Koordination zwischen einzelnen Akteuren ermöglichen. Grosse Unternehmen, kantonale Polizeikorps und der Bund verfügen über Stellen mit spezialisiertem Fachwissen. Forschungsanstalten betreiben ebenfalls Projekte im Kontext der Cyber-Sicherheit und der Identifizierung und Bewertung von Cyber-Risiken. Oftmals sind aber nicht alle Verantwortungsträger, von der technisch-operativen bis zur strategisch-politischen Ebene, in die Prozesse einbezogen oder aber sie nehmen sich bewusst davon aus.

Aus den Befragungen mit Vertretern der Wirtschaft und KI-Betreibern geht aber auch hervor, dass grosse Lücken und Schwächen beim Umgang mit Cyber-Angriffen bestehen. So sind die Fähigkeiten und Wahrnehmungen auf den verschiedenen Ebenen unterschiedlich ausgeprägt, oft ungenügend, nur teilweise koordiniert und zu einem guten Teil von kommerziellen Interessen bestimmt. Die ergriffenen oder geplanten Verbesserungsmassnahmen für die Cyber-Sicherheit sind Abbild unterschiedlicher Risikoeinschätzungen und damit auch entsprechend heterogen. Sie führen zu nicht abgestimmten Vorgehensweisen, der Informationsaustausch zwischen den Akteuren funktioniert kaum und ist oft auf den eigenen Betrieb beschränkt.

Mängel bei der Cyber-Sicherheit werden oft auf die fehlenden finanziellen und personellen Ressourcen zurückgeführt. Dies gilt nicht nur für die Wirtschaft, sondern insbesondere auch für den Bund, wo die personellen Ressourcen nicht ausreichend vorhanden sind, sodass die geforderten Aufgaben sogar in der normalen Lage nur unzureichend erfüllt werden können. Ein Problem ist auch, dass es nach allgemeiner Einschätzung zu wenig IKT-Spezialisten gibt.

In der Zusammenarbeit zwischen der Wirtschaft und den Behörden gibt es bei der Aufteilung der Aufgaben, Fähigkeiten und Kompetenzen diverse Schwachstellen und Klärungsbedarf. Die Analyse der bestehenden Strukturen hat insbesondere gezeigt, dass der Bundesverwaltung die Mittel zur Identifikation von Risiken und zur gesamtheitlichen Auswertung von Infor-

mationen und Lageeinschätzungen zuhanden der Wirtschaft, KI-Betreiber und Behörden fehlen und somit der Schutz vor Cyber-Risiken wegen ungenügendem Informationsaustausch unzureichend erreicht werden kann. Weiter sind Synergien unter den bestehenden behördlichen Stellen besser zu nutzen und die Meldesysteme und -wege mit Blick auf den Informationsaustausch auf ihre Effizienz hin zu untersuchen. Ausserdem fehlen Risikoanalysen und daraus abgeleitete Definitionen für Sicherheitsanforderungen bei IKT-Infrastrukturen mit der daraus folgenden Aufteilung der Verantwortung und der Mehrkosten.

Insgesamt kann festgehalten werden, dass das heutige System kaum in der Lage ist, grössere, gezielte Cyber-Angriffe aktiv abzuwehren oder deren Folgen, sofern diese gravierend sind in der gebotenen Kürze zu beheben. Die befragten Unternehmen und KI-Betreiber fordern deshalb, dass gemeinsam mit den Behörden minimale Sicherheitsvorgaben definiert und umgesetzt werden, und dass die Massnahmen zur Verbesserung der Sicherheitslage, zur Bewältigung von Angriffen sowie zur Sensibilisierung besser koordiniert werden. Ausserdem wird vom Bund gefordert, den Informationsaustausch zu institutionalisieren, ein umfassendes aktuelles Cyber-Lagebild zur Verfügung zu stellen und eine erweiterte subsidiäre Unterstützungsleistung sicherzustellen.

Die bestehenden, verschiedenen Rechtsgrundlagen widerspiegeln die Cyber-Ausprägung von bestehenden Aufgaben und Verantwortlichkeiten. Entsprechend ist eine Lösung im Rahmen eines einzigen Cyber-Spezial-Gesetzes ungeeignet. Die bestehenden Gesetzeswerke sind daher fortlaufend, im Rahmen der Revision an die Entwicklungen im Cyber-Bereich innerhalb ihres Geltungsbereiches anzupassen.

4 DISPOSITIV FÜR DEN SCHUTZ VOR CYBER-RISIKEN

4.1 Übergeordnete Ziele

Der Bundesrat erkennt, dass die Cyber-Problematik primär eine Ausprägung bestehender Aufgaben und Verantwortlichkeiten von Behörden, Wirtschaft und Gesellschaft darstellt. Die Minimierung von Cyber-Risiken ist somit Sache der jeweiligen Verantwortungsträger.

Der Bundesrat will die Chancen und Vorteile, die der Cyber-Bereich mit sich bringt, für die Schweizer Wirtschaft, Politik und Bevölkerung fördern. Er stellt aber auch fest, dass die Entwicklungen in diesem Bereich mit Risiken verbunden und entsprechende Minimierungsmassnahmen nötig sind.

Die vorliegende nationale Strategie regelt die Anwendung der beschriebenen Massnahmen in Friedenszeiten über alle Lagen und schliesst damit den Kriegsfall explizit aus.

Der Bundesrat verfolgt mit der nationalen Strategie der Schweiz zum Schutz vor Cyber-Risiken folgende übergeordnete Ziele:

- Risiken im Cyber-Bereich sollen frühzeitig erkannt und bewertet werden, damit risikominimierende- und vorsorgliche Massnahmen in Zusammenarbeit mit allen Beteiligten aus Wirtschaft, Politik und Gesellschaft getroffen werden können.
- Die Widerstandsfähigkeit (Resilienz) von kritischen Infrastrukturen gegenüber Cyber-Angriffen, also die Fähigkeit, möglichst rasch wieder den Normalbetrieb zu gewährleisten, soll in Zusammenarbeit mit deren Betreibern und dem vom Bund geführten Programm zum Schutz kritischer Infrastrukturen (SKI-Programm) erhöht werden.
- Es sollen Voraussetzungen für eine wirksame Bekämpfung von Cyber-Risiken, insbesondere der Cyber-Kriminalität und der Cyber-Spionage sichergestellt, und wo nötig geschaffen werden.

Diese Ziele können in den bestehenden dezentralen Strukturen auf verschiedene Arten erreicht werden. In jedem Fall sind das Handeln in *Eigenverantwortung* in den verschiedenen Wirtschaftsbereichen sowie der *Dialog* und die *Zusammenarbeit* zwischen der Wirtschaft und den Behörden wesentliche Voraussetzungen. Durch einen permanenten gegenseitigen *Informationsaustausch* sollen *Transparenz* und *Vertrauen* geschaffen werden, und der Staat soll nur dann eingreifen, wenn öffentliche Interessen auf dem Spiel stehen und er im Sinne der *Subsidiarität* handelt.

Der Umgang mit Cyber-Risiken ist eine Querschnittsaufgabe, die von Wirtschaft, IK-Betreibern und Behörden auf kantonaler sowie Bundesebene wahrgenommen werden muss. Diese müssen als Teil eines integralen Geschäfts-, Produktions-, oder Verwaltungsprozesses verstanden werden. In diese Prozesse sind alle Akteure von der administrativ-technischen bis hin zur strategisch-politischen Ebene einzubeziehen. Ein wirksamer Umgang mit Gefahren und Bedrohungen aus dem Netz setzt die Erkenntnis voraus, dass bestehende Aufgaben und Verantwortlichkeiten von Behörden, Wirtschaft und Bevölkerung eine Cyber-Ausprägung haben. Jede Organisationseinheit aus Politik, Wirtschaft und Gesellschaft trägt die Verantwortung, diese Cyber-Ausprägung zu erkennen, die damit einhergehenden Risiken in ihren jeweiligen Prozess aufzunehmen und damit zu reduzieren. Zu diesem Zweck sollen die dezentral bestehenden Strukturen befähigt, allenfalls gestärkt werden, um die cyber-spezifische Ausprägung ihrer Aufgaben und Verantwortlichkeiten umfassend abzudecken.

4.2 Rahmenbedingungen und Voraussetzungen

Rechtliche Grundlagen

Da die Cyber-Problematik eine Ausprägung bestehender Aufgaben und Verantwortlichkeiten ist, muss in einem ersten Schritt überprüft werden, ob die bestehenden Rechtsgrundlagen dieser gerecht werden. Wird Handlungsbedarf festgestellt, geht es vorerst darum, notwendige Bestimmungen in die geltenden und geplanten Gesetze zu integrieren (z.B. Nachrichtendienstgesetz). Der vom Cyber-Bereich erforderte Regelungsbedarf ist deshalb eng mit laufenden und vorgesehenen Rechtssetzungsprojekten abzustimmen (z.B. die Gesetzgebung für die Informationssicherheit, das Nachrichtendienstgesetz, das Landesversorgungsgesetz, Bundesgesetz zur Überwachung des Fernmeldewesens, Übereinkommen über Cyberkriminalität etc.)

Die Anpassung der rechtlichen Grundlagen an die raschen Entwicklungen des Cyber-Bereichs und der Cyber-Risiken ist ein permanenter Prozess. Wo nötig sollen für komplexe Fragen Rechtsgutachten erstellt werden. Die Rechtsgrundlagen der Strafverfolgung (insbesondere das Strafgesetzbuch, die Strafprozessordnung, die kantonalen Polizeigesetze und die Zuständigkeit) und präventiv tätiger Einheiten (Nachrichtendienst des Bundes und Kantonspolizeikorps) sind auf die spezifischen Herausforderungen (z.B. geografische Distanzen, Geschwindigkeit und Vergänglichkeit von Spuren und somit die Gerichtsverwertbarkeit von Indizien) des Cyber-Bereichs hin zu überprüfen. Es geht vor allem um die Frage, wie Taten, die mittels elektronischen Netzwerken ausgeführt werden, frühzeitig erkannt und verhindert bzw. wirksam ermittelt werden können. Besonderes Augenmerk ist dabei auf die Güterabwägung zwischen Persönlichkeitsschutz sowie öffentlicher und innerer Sicherheit zu legen.

Weiter sind die Verantwortlichkeiten von (Computer-)System- und Netzwerk-Betreibern, (Netzwerk-)Infrastruktur- und Dienstleistungsanbietern sowie allfälligen weiteren im Internet tätigen Akteuren zu überprüfen. Auch hier ist eine rechtliche und politische Abwägung zwischen Datenschutzpflicht und Datenbearbeitungsrecht aller Parteien vorzunehmen, um Kooperationen zum Schutz von Informations- und Kommunikationsinfrastrukturen sowie privaten und öffentlichen Personen zu ermöglichen.

Armee

Die Armee als strategische Reserve der Schweiz muss ihre verfassungsmässige Auftragserfüllung über alle Lagen und in allen Einsatzformen sicherstellen können. Sie trifft deshalb weitreichende Massnahmen zum Schutz der eigenen Infrastrukturen und stellt die Kommunikation in der Krise mit ausfallsresistenten Infrastrukturen sicher. Die Erkenntnisse aus der Tätigkeit der Armee und der Zugang zu den ausfallresistenten Infrastrukturen werden, wo gefordert, anderen Behörden und Betreibern kritischer Infrastrukturen subsidiär zur Verfügung gestellt.

Strafverfolgung

Im Rahmen der Strafverfolgung sollen gerichtsverwertbare Informationen über Straftaten im Cyber-Bereich gewonnen, die Täter verfolgt, die Straftaten geahndet und die Zusammenarbeit mit ausländischen Strafverfolgungsbehörden sichergestellt werden. Gerade im Hinblick auf die Kriminalstrategische Priorisierung 2012 – 2015 des Bundesrates ist die Strafverfol-

gung dazu angehalten, auf Cyberangriffe als besondere Form von Wirtschaftskriminalität zu fokussieren.

Zusammenarbeit im Inland

Die Cyber-Ausprägung von Aufgaben und Verantwortlichkeiten und die damit einhergehenden Risiken müssen erkannt und analysiert werden. Dies obliegt den jeweiligen Behörden im Austausch mit Akteuren aus Wirtschaft und Gesellschaft. Eine enge Zusammenarbeit privater und öffentlicher Akteure in Form von *Public Private Partnerships (PPP)* hat sich bewährt und ist weiterhin zu verfolgen[22].

Um eine umfassende Lagedarstellung zu erstellen, müssen technische und nicht technische Informationen koordiniert gesammelt, analysiert und bewertet werden. Die Erkenntnisse aus den Untersuchungen werden anschliessend allen Akteuren zur Verfügung gestellt.

Vom Staat wird erwartet, dass er über Mittel verfügt, die es ihm ermöglichen, verantwortliche Stellen subsidiär zu unterstützen, wenn aufgrund der Lage diese nicht mehr fähig sind, Massnahmen zu deren Bewältigung selber sicherzustellen.

Zusammenarbeit mit dem Ausland

Cyber-Risiken sind länderübergreifend. Für eine fundierte und realistische Risikoanalyse ist internationale Kooperation wesentlich. Der Austausch von Erfahrungen, Forschungs- und Entwicklungsarbeiten, vorfallbezogenen Informationen sowie Ausbildungs- und Übungstätigkeiten soll deshalb verstärkt werden.

Bemühungen, den Cyber-Raum mit international vereinbarten Regeln und Standards vor Missbrauch zu schützen, liegen im Interesse der Schweiz als technologisch hochentwickeltes Land. Die Schweiz beteiligt sich deshalb im Rahmen von internationalen staatlichen und nicht-staatlichen Organisationen bei der Suche nach völkerrechtlichen Vereinbarungen zur Minderung von Cyber-Risiken. Strukturbedingte Probleme der globalen Vernetzung, sowie die Schaffung und Beeinflussung von internationalen Standards, Regeln und Normen werden idealerweise in globalen Foren angegangen. Entsprechend sind die Schweizer Interessen von Wirtschaft, Behörden und Gesellschaft bereits auf dieser Stufe einzubringen.

Dasselbe gilt für den Ausbau der Kooperation bei der gemeinsamen Krisenbewältigung. Durch verstärkte Zusammenarbeit im nachrichtendienstlichen Bereich, in der technischen Analyse und bei der Strafverfolgung (Rechts- und Amtshilfe) kann die Schweiz die eigene Handlungsfähigkeit und Wirksamkeit ihrer Massnahmen erhöhen. Dabei ist der Einbezug auch nichtstaatlicher Akteure auf den jeweiligen Ebenen, wie beispielsweise Verbände, Interessenorganisationen, internationalen Arbeitsgruppen oder Nicht-Regierungsorganisationen unabdingbar.

4.3 Handlungsfelder und Massnahmen

Bei der Umsetzung der Massnahmen für einen besseren Schutz der Schweiz vor Cyber-Risiken gilt es, die politische und wirtschaftliche Zweckmässigkeit, Verhältnismässigkeit und Wirksamkeit zu berücksichtigen und der dezentralen Staats- und Wirtschaftsstruktur der

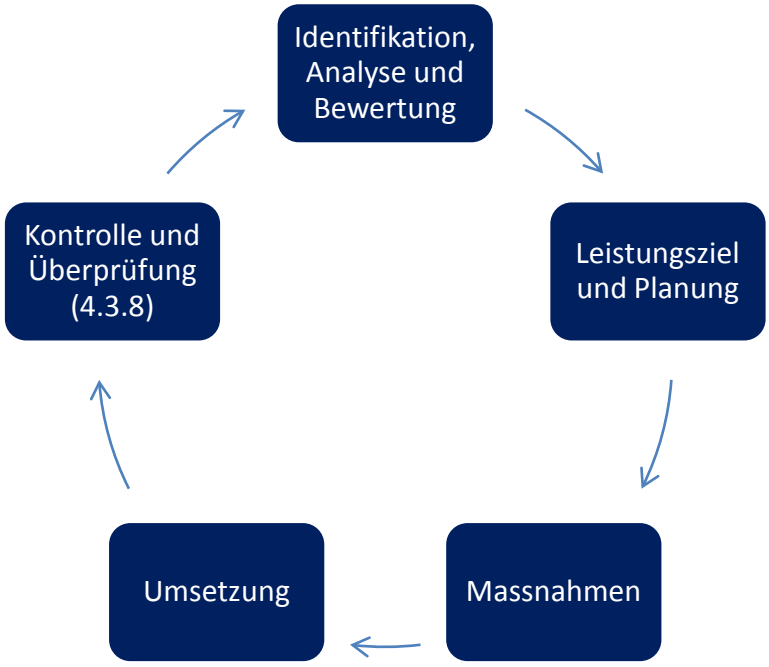
[22] Vgl. BRB 2003 und 2007

Schweiz Rechnung zu tragen. Dies setzt bei allen Akteuren die Erkenntnis voraus, inwiefern ihre jeweiligen Aufgaben und Verantwortlichkeiten eine Cyber-Ausprägung aufweisen und mit welchen Partnern aus Wirtschaft, Politik und Gesellschaft die Massnahmen zur Risikominimierung angegangen werden müssen.

Nachfolgend werden Handlungsfelder und Massnahmen aufgeführt, die zur Reduktion der Cyber-Risiken dienen sollen. Diese Handlungsfelder werden entlang eines Risikomanagement- und Schutzkreislaufes umschrieben[23]. Während der Risikomanagement- und Schutzkreislauf fünf Teilprozesse umfasst (Identifikation, Analyse und Bewertung; Leistungsziel und Planung; Massnahmen; Umsetzung und Kontrolle sowie Überprüfung), geht die vorliegende Strategie für jedes einzelne Handlungsfeld nur auf die ersten drei Schritte ein (Identifikation, Analyse und Bewertung; Leistungsziel und Planung und Massnahmen).

Die Umsetzung der Massnahmen erfolgt durch die zuständigen Akteure aus der Verwaltung, Wirtschaft und Gesellschaft. Soweit Umsetzungsschritte Bundestellen betreffen, sind diese beschrieben. Dabei handelt es sich in erster Linie um erste Umsetzungsschritte auf Stufe Bund zur Einleitung der Umsetzungsplanung auf allen Ebenen in Zusammenarbeit mit den jeweiligen Partnern aus Verwaltung, Wirtschaft und Gesellschaft..

Die Kontrolle und Überprüfung der umgesetzten Massnahmen obliegt, in enger Zusammenarbeit mit den verantwortlichen Stellen, der zu schaffenden Koordinationsstelle.



[23] Der Risikomanagement- und Schutzkreislauf lehnt sich stak an den Schutzzyklus an, der in der nationalen Strategie zum Schutz kritischer Infrastrukturen (BABS) eingesetzt und von der wirtschaftlichen Landesversorgung im Bereich ICT-I verwendeten wird.

4.3.1 Handlungsfeld 1: Forschung und Entwicklung

Identifikation, Analyse und Bewertung

Entwicklungen von Chancen und Risiken im Zusammenhang mit der Cyber-Problematik sollen erforscht werden, damit Entscheide in Politik, Wirtschaft und Forschung frühzeitig und informiert getroffen werden können. Die Forschung und Entwicklung fokussiert auf technologische, gesellschaftliche, politische und wirtschaftliche Tendenzen, die sich auf Cyber-Risiken auswirken können. Forschung und Entwicklung ist Sache der zuständigen Akteure aus Wissenschaft, Wirtschaft, Gesellschaft und Behörden.

Leistungsziele und Planung

Die Fähigkeiten, potenzielle Chancen und Risiken im Zusammenhang mit der Cyber-Problematik in der eigenen Verantwortungsdomäne eigenständig zu identifizieren, zu bewerten und zu analysieren, müssen vorhanden sein. Dies erfolgt in enger Zusammenarbeit und Absprache mit den Verantwortlichen der „Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz“ (UVEK-BAKOM) und der „Nationalen Strategie zum Schutz kritischer Infrastrukturen“(VBS-BABS).

Massnahmen

Massnahme 1

Die verantwortlichen Akteure tauschen sich zu aktuellen und zu erforschenden Entwicklungen im Zusammenhang mit Cyber-Risiken aus. Dieser Austausch wird von den akademischen Forschungseinrichtungen in eigener Verantwortung gefördert und vertieft. **(EDI[24])**

Umsetzung

Das EDI (ab 2013 EVD) prüft zusammen mit den beteiligten Departementen und den Kantonen die staatlichen Möglichkeiten den akademischen Informationsaustausch und gegebenenfalls die Forschungspriorisierung im Bereich der Cyber-Risiken zu unterstützen. Es beteiligt sich dabei finanziell an Plattformprojekten zur Wissenssammlung.

Massnahme 2

Der Bund soll Projekte der Wirtschaft mit Fachwissen und finanziellen Ressourcen subsidiär unterstützen, Kredite anbieten, sowie selber eigene Forschungsaufträge erteilen. **(EDI, EVD, VBS, EJPD)**

Umsetzung

Das EDI (ab 2013 EVD) prüft zusammen mit den beteiligten Departementen und den Kantonen die Möglichkeiten einer höheren, koordinierten finanziellen Beteiligung bei der Förderung von Forschungsprojekten im Bereich von Cyber-Risiken. Die verschiedenen Unterstützungskredite des Bundes für priorisierte Forschungsprojekte der Wirtschaft sind zu überprüfen und gegebenenfalls kontinuierlich per 2017 an die Nachfrage anzupassen. Das EVD erstellt dazu eine Übersicht der verfügbaren Forschungskredite und Vorschläge für mögliche Anpassungen per Mitte 2013.

[24] Das Eidgenössische Departement des Innern (EDI) ist noch bis Ende 2012 für Bildung und Forschung zuständig. Ab 2013 wird dies vom Eidgenössischen Volkswirtschaftsdepartement (EVD) übernommen.

4.3.2 Handlungsfeld 2: Risiko- und Verwundbarkeitsanalyse

Identifikation, Analyse und Bewertung

Risiken, die sich aus der Cyber-Ausprägung ergeben, müssen von allen zuständigen behördlichen Stellen, IK-Betreibern und Verbänden (im Sinne einer Branchenbündelung) auf ihrer Stufe identifiziert, deren Eintrittswahrscheinlichkeit und potenziellen Auswirkungen bewertet und analysiert werden.

Leistungsziele und Planung

Die verantwortlichen Akteure aus Politik, Wirtschaft und Gesellschaft sollen über Mittel und Fähigkeiten verfügen, um frühzeitig Cyber-Risiken identifizieren, die Bedrohungslage bewerten und die Implikationen in Form von gemeinsamen Risikoanalysen für ihren Bereich analysieren zu können. Dies erfolgt in der Umsetzung in enger Zusammenarbeit mit der „Nationalen Strategie zum Schutz kritischer Infrastrukturen".

Massnahmen

Massnahme 3

Risikoanalysen sollen auf allen Stufen (Bund, Kantone und KI-Betreiber) geschaffen werden. Dies umfasst die selbstständige und regelmässige Überprüfung der Systeme durch die verantwortlichen Betreiber. Die Erarbeitung von (sektoriellen) Risikoanalysen erfordert die enge Zusammenarbeit mit den regulierenden Behörden. **(EVD, EFD, UVEK)**

Umsetzung

Das EVD passt im Rahmen der Revision des LVG seine Kompetenzen entsprechend an, um mit allen Teilsektoren des Bereiches ICT-I der Wirtschaftlichen Landesversorgung (WL) periodische Risikoanalysen durchführen zu können. Es bindet bei der Umsetzung der Erkenntnisse situativ die zuständigen regulierenden Behörden (in erster Linie beim UVEK und EFD) ein. Entsprechend wird der Bereich ICT der WL per Ende 2015 personell gestärkt und sein Auftrag geschärft.

Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein. Diese wird bis 2017 kontinuierlich zur Bewältigung dieser Anforderung personell verstärkt.

Massnahme 4

Die Behörden, Unternehmen und Forschungseinrichtungen untersuchen IKT-Infrastrukturen auf Verwundbarkeiten. Dazu gehören organisatorische, systemische und technische Schwächen. Die Erkenntnisse werden konsolidiert und bewertet und bei öffentlichem Interesse in entsprechenden Berichten publiziert[25]. **(EVD, EFD, VBS, UVEK)**

Umsetzung

Das Informatiksteuerungsorgan Bund (ISB) im EFD erstellt in Zusammenarbeit mit den IKT-Dienstleistern ein Konzept per Mitte 2013 zur periodischen Überprüfung der IKT-Strukturen

[25] Kryptographische Methoden und Produkte zum Schutz von klassifizierten (VERTRAULICH / GEHEIM) Informationen nach Informationsschutz-Verordnung müssen durch die Fachstelle für Kryptologie des VBS freigegeben werden.

der Bundesverwaltung auf organisatorische, systemische und technische Schwächen. Dieses wird von den zuständigen Leistungserbringern und den jeweiligen verantwortlichen in den Generalsekretariaten der Departemente umgesetzt. Der personelle Mehrbedarf zur Umsetzung und Schaffung zusätzlicher (technischer) Fähigkeiten wird innerhalb der zuständigen Bundestellen ab Mitte 2014 kontinuierlich bis 2015 aufgebaut.

Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein. Diese wird bis 2017 kontinuierlich zur Bewältigung dieser Anforderung personell verstärkt.

4.3.3 Handlungsfeld 3: Analyse Bedrohungslage

Identifikation, Analyse und Bewertung

Vorfälle von nationaler Bedeutung und von besonderer Relevanz sollen identifiziert, bewertet und analysiert werden. Die Erkenntnisse daraus sollen stufengerecht für die jeweiligen Verantwortungsbereiche ausgearbeitet und verfügbar gemacht werden.

Leistungsziele und -planung

Die verantwortlichen Akteure aus Politik, Wirtschaft und Gesellschaft sollen über Mittel und Fähigkeiten verfügen, um die Bedrohungslage in enger Zusammenarbeit untereinander mit den Verantwortungsträgern identifizieren, bewerten und analysieren zu können. Soweit nötig soll eine Meldeermächtigung für die verantwortlichen und zuständigen Stellen und KI-Betreiber geprüft werden[26].

Massnahmen

Massnahme 5

Aus nicht öffentlichen und öffentlichen Quellen werden nachrichtendienstliche, polizeiliche, forensische und technische Informationen zur Bedrohungs- und Risikolage im Cyber-Bereich beschafft, bewertet und analysiert. Diese Erkenntnisse sollen im Rahmen des Public-Private-Partnership-Modell von MELANI gesammelt, gesamthaft bewertet, analysiert und in einer Lagedarstellung und Lagefortschreibung fusioniert, sowie mit Lageentwicklungsmöglichkeiten versehen werden. Diese Ergebnisse werden zugunsten der relevanten und verantwortlichen Akteure zur Verfügung gestellt. **(EFD, VBS)**

Umsetzung

Der Nachrichtendienst des Bundes wird gemäss dem Bedarfsausweis von 2011 personell per Ende 2016 kontinuierlich personell verstärkt um die Cyber-Ausprägung seines Auftrages wahrzunehmen. Dies passiert unter Einbezug der FUB als technischer Dienstleistungserbringer für den NDB. Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

Die technischen Kapazitäten zur konstanten (24/7) Überwachung der Bundesnetze sind innerhalb der Dienstleistungserbringer (CERTs) per Ende 2015 aufzubauen. Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

[26] Auf Grund des PPP-Ansatzes ist prinzipiell von einer Meldepflicht bei Vorfällen abzusehen. Allerdings müssen die Akteure die rechtliche Möglichkeiten haben, Meldungen zu Vorfällen erstatten zu dürfen. Soweit dies nicht bereits möglich ist, muss eine solche Ermächtigung rechtlich geprüft werden.

MELANI stärkt den freiwilligen Informationsaustausch mit den KI-Betreibern und seinen internationalen Partnern. Auf Grund des erhöhten Bedarfs an forensischer Fähigkeiten, zunehmenden Informationsflusses und der Stärkung des Informationsaustausches mit KI-Betreibern und der Wirtschaft wird MELANI per Ende 2017 kontinuierlich zur Bewältigung dieser Aufgabe personell verstärkt.

Massnahme 6
Der Bund, die Kantone und die KI-Betreiber sollen relevante Vorfälle nachbereiten und Möglichkeiten zur Weiterentwicklung der eigenen Massnahmen im Umgang mit Vorfällen im Zusammenhang mit Cyber-Risiken überprüfen. Dies erfolgt grundsätzlich im Rahmen des eigenen Auftrags individuell. Diese Erkenntnisse sollen im Rahmen des Public-Private-Partnership-Modell von MELANI gesammelt, gesamthaft bewertet, analysiert und die Ergebnisse zugunsten der relevanten Akteure zur Verfügung gestellt werden. **(EFD, VBS)**

Umsetzung
MELANI stärkt den freiwilligen Informationsaustausch mit den KI-Betreibern untereinander und unterstützt die Nachbearbeitung von relevanten Vorfällen. Auf Grund des erhöhten Bedarfs an forensischer Fähigkeiten, zunehmenden Informationsflusses und der Stärkung des Informationsaustausches mit KI-Betreibern und der Wirtschaft wird MELANI per Ende 2017 kontinuierlich zur Bewältigung dieser Aufgabe personell verstärkt.

Zur Bewältigung und Nachbearbeitung von Staatschutz relevanten Vorfällen, wird der Nachrichtendienst des Bundes gemäss dem Bedarfsausweis von 2011 personell per Ende 2016 kontinuierlich ausgebaut um die Cyber-Ausprägung seines Auftrages wahrzunehmen. Dies passiert unter Einbezug der FUB als technischer Dienstleistungserbringer für den NDB. Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

Die technischen Kapazitäten zur konstanten (24/7) Überwachung der Bundesnetze sind innerhalb der Dienstleistungserbringer (CERTs) per Ende 2015 aufzubauen. Die Erkenntnisse fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

Massnahme 7
Es sollen auf nationaler Ebene eine möglichst vollständige Fallübersicht geführt und interkantonale Fallkomplexe koordiniert werden. Die Erkenntnisse und daraus gewonnen Informationen dienen der Vervollständigung der Lagedarstellung. **(EJPD)**

Umsetzung
Das EJPD legt in Zusammenarbeit mit den Kantonen per Ende 2013 ein Konzept zur Stärkung und Effizienzsteigerung im Bereich der Koordination interkantonaler Fallkomplexe und der Führung einer gesamtheitlichen Fallübersicht vor.

Die Erkenntnisse der daraus gewonnen Informationen fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

4.3.4 Handlungsfeld 4: Sensibilisierung und Ausbildung

Identifikation, Analyse und Bewertung
Alle Akteure aus Wirtschaft, Gesellschaft und Behörden sollen für Cyber-Risiken sensibilisiert und ausgebildet werden, damit sie die notwendigen Massnahmen zur Minimierung ihrer Risikoexponierung erfassen und umsetzen können.

Leistungsziele und -planung

Um das Bewusstsein für Cyber-Risiken und den richtigen Umgang damit zu erhöhen, sollen Sensibilisierungs- und Ausbildungsmassnahmen unter Berücksichtigung bereits bestehender Ansätze und Initiativen erarbeitet werden, die in den jeweiligen Verantwortungsbereichen umgesetzt werden. Dies erfolgt in enger Zusammenarbeit in der Umsetzung der „Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz“.

Massnahmen

Massnahme 8

Es werden bestehende Ausbildungs- und Informationsgrundlagen (z.B. Kampagnen, Broschüren, Webseiten) vernetzt oder neue geschaffen, die für alle Betroffenen zugeschnitten sind. **(EDI, UVEK)**

Umsetzung

Das EDI (ab 2013 EVD) erarbeitet in enger Absprache mit der „Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz“ und den Kantonen bis Ende 2014 ein Umsetzungskonzept zur Koordinierung und Unterstützung von stufengerechten Kampagnen und Ausbildungsleitfäden zum Umgang mit Cyber-Risiken.

Massnahme 9

Der Bund soll Projekte der Wirtschaft mit Fachwissen und finanziellen Ressourcen subsidiär unterstützen, Kredite anbieten, sowie selber eigene Sensibilisierungs- und Ausbildungsaufträge erteilen. **(EDI, EFD, VBS, EJPD)**

Umsetzung

Das EDI (ab 2013 EVD) prüft zusammen mit den beteiligten Departementen und den Kantonen die staatlichen Möglichkeiten einer höheren, koordinierten finanziellen Beteiligung bei der Förderung von Sensibilisierungs- und Ausbildungsprojekten im Bereich der Cyber-Risiken. Die verschiedenen Unterstützungskredite des Bundes sind zu überprüfen und gegebenenfalls kontinuierlich per 2017 an die Nachfrage anzupassen. Das EVD erstellt dazu eine Übersicht der verfügbaren Kredite und konzipiert Vorschläge für mögliche Anpassungen per Mitte 2013.

Massnahme 10

Es werden alle relevanten und zuständigen Akteure von der administrativen, technischen bis hin zur strategischen Ebene ausgebildet und trainiert. **(EDI)**

Umsetzung

Das EDI (ab 2013 EVD) erarbeitet in enger Absprache mit der „Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz“ und den Kantonen bis Ende 2015 eine Übersicht und ein Umsetzungskonzept, zur Stärkung der stufengerechten Ausbildung im Cyber-Bereich. Dies soll technische Lehrgänge ebenso erfassen, wie Ausbildungen im strategischen Risikomanagement unter Einbezug der Cyber-Ausprägung von Geschäfts-, Produktions-, und Verwaltungsprozessen.

4.3.5 Handlungsfeld 5: Internet-Governance und Internationale Policies

Identifikation, Analyse und Bewertung

Internet-Governance[27] funktioniert nach einem Multi-Stakeholder-Ansatz. Alle relevanten und zuständigen Akteure (Behörden, Wirtschaft und Gesellschaft) können sich in diesen Prozess einbringen. Die Spielregeln für die Nutzung und Verwaltung des Internets sind fundamental für die Entwicklung von Bürgern, Unternehmen und Staaten in einer vernetzten, freien und kompetitiven Welt. Auf Grund der globalen und diversen Natur des Internets können Regulierungen nur sehr beschränkt unilateral von einzelnen Staaten beschlossen und durchgesetzt werden. Dies gilt auch für die Formulierung von so genannten Policies, Best Practices und Gremien zu Ausschaffung von de facto Sicherheitsstandards für Produkte und Prozesse.

Insbesondere Interessen von kleinen Staaten wie der Schweiz können global nur durch „proaktive" Diplomatie und gutes, koordiniertes Multistakeholder-Networking vertreten werden.

Leistungsziele und Planung

Strukturbedingte Probleme der globalen Vernetzung werden idealerweise im globalen Forum angegangen. Entsprechend sind die Schweizer Interessen von Wirtschaft, Gesellschaft und Behörden soweit möglich koordiniert einzubringen.

Die Verwaltung der Internet-Kernressourcen soll zwar weiterhin nach freiheitlichen Grundsätzen geleistet werden, soll aber weniger von den Interessen der (US-) Internetindustrie dominiert werden, sondern die Regierungen sollen gewisse Leitplanken (Rechtstaat, Menschenrechte, etc.) setzen und auch durchsetzen können. Die Stabilität und Verfügbarkeit des Internets für Alle soll sichergestellt und die Freiheit der Bürger und Unternehmen im Internet nicht in unverhältnismässiger Weise eingeschränkt werden.

Im Hinblick auf die Schaffung internationaler Best Practices, Policies und Vereinbarungen im Bereich von Sicherungs- und Sicherheitsstandards ist ein koordiniertes Auftreten vor allem wirtschaftlicher Akteure und behördlicher Stellen zur Einbringung der Schweizer Interessen unabdingbar.

Massnahmen

Massnahme 11

Die Schweiz (Wirtschaft, Gesellschaft, Behörden) setzt sich aktiv und soweit möglich koordiniert für eine Internet-Governance ein, welche möglichst mit den Schweizer Vorstellungen von Freiheit und (Selbst-)Verantwortung, Grundversorgung, Chancengleichheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist. Die Schweiz setzt sich zudem für eine vernünftige Internationalisierung und Demokratisierung der Internetverwaltung ein. Durch ihre Erfahrung im demokratischen Entscheidfindungsprozess erbringt sie einen Mehrwert bei der Konsensfindung. **(EDA, EFD, VBS, UVEK)**

Umsetzung

Das EDA erarbeitet in Zusammenarbeit mit den beteiligten Departementen, eine Übersicht zu den prioritären Veranstaltungen, Initiativen und internationalen Gremien im Bereich der

[27] „Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." Bericht der Working Group on Internet Governance (WGIG) 2005: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0

Internet-Governance per Ende 2013. Die Teilnahme an diesen vorrangigen Gremien wird vom EDA und den beteiligten Departementen sichergestellt. Das EDA wird auf Grund dieser neuen Anforderungen per Ende 2014 personell verstärkt.

Massnahme 12
Im Rahmen privater und staatlicher Initiativen und Standardisierungsprozessen koordinieren sich die Betreiber, Verbände und Behörden, um sich in diese Gremien einzubringen. **(EDA, VBS, EFD, UVEK)**

Umsetzung
MELANI stärkt den Informationsaustausch unter den KI-Betreibern und den Verbänden zu internationalen Ansätzen und Initiativen. Damit unterstützt MELANI die koordinierte Einbringung des Wirtschaftstandortes Schweiz in diesen internationalen Gremien. Sofern gewünscht stellt MELANI in Absprache mit dem EDA die Teilnahme sicher. MELANI wird per Ende 2017 kontinuierlich zur Bewältigung der zusätzlichen Aufgaben personell verstärkt. Der Bedarf des EDA zur Erfüllung dieser Aufgabe wird per Ende 2014 gedeckt.

4.3.6 Handlungsfeld 6: Kontinuitäts- und Krisenmanagement

Identifikation, Analyse und Bewertung
Die Aktivitäten der verschiedenen Akteure sollen je nach Eskalationsstufe koordiniert werden.

Es werden dabei drei verschiedenen Eskalationsstufen unterschieden.

Der zivile Alltag ist durch die normale Betriebsführung der gesamten IKT-Infrastruktur charakterisiert. In dieser Lage steht die Bundesverwaltung unter permanenten Angriffen, die erkannt / detektiert werden müssen und durch Gegenmassnahmen abgewehrt werden müssen. Im Vordergrund stehen präventive Massnahmen in Infrastruktur und Betrieb, mit regelmässigen reaktiven Interventionen ohne relevante Konsequenzen.

Die Cyber-Krise zeichnet sich durch einen gelungenen Angriff mit gravierenden Konsequenzen aus, wobei die Konsequenzen noch keine ausserordentliche Lage für das Land darstellen. Dazu gehören beispielsweisse Spionagevorfälle auf die Bundesverwaltung oder Angriffe auf bestimmte Wirtschaftszweige. Im Vordergrund stehen reaktive Massnahmen in Infrastruktur und Betrieb, welche auch für die Bundesverwaltung und möglicherweise auch für die Öffentlichkeit spürbare Konsequenzen haben (Systeme schliessen etc.). Die KI-Betreiber werden auf der Basis von Vereinbarungen in den Entscheidungsprozess einbezogen.

Die ausserordentliche Lage zeichnet sich durch einen gelungenen Angriff mit einer Bedrohung bzw. mit Konsequenzen für das Land (wie z.B. Störung der landesweiten Stromversorgung oder Kontrollübernahme von Steuersystemen). Im Vordergrund steht ein Zusammenspiel von politischen Handlungen, welche von politisch geführten technischen Massnahmen auf Landesebene zu begleiten sind. In der ausserordentlichen Lage wird das Krisenmanagement durch eine Führungsorganisation des Bundes wahrgenommen.

Leistungsziele und Planung
Die individuellen und sektoriellen Risikoanalysen sollen als Grundlage für Sektorenvereinbarungen und der Kontinuitätsplanung dienen. Diese sind in enger Zusammenarbeit mit den Betreibern und regulierenden Behörden auszuarbeiten oder abzustimmen. Für Krisenfälle

und ausserordentliche Lagen sind die entsprechenden Planungen in enger Abstimmung mit den zuständigen Behörden und Wirtschaftsvertretern auszuarbeiten, respektive wo nötig Vereinbarungen zu treffen. Dies erfolgt in enger Zusammenarbeit in der Umsetzung der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen".

Die Schweiz soll in der Lage sein, Angriffe welche sie betrifft oder betreffen könnten, alleine oder in Kooperation mit ausländischen Partner, aktiv zu ermitteln und abzuwehren und somit das reaktive Krisenmanagement zu unterstützen. Die verantwortlichen Stellen werden befähigt, gezielte Operationen zur Beschaffung über und Beeinträchtigung von Angriffsinfrastrukturen zu führen.

Massnahmen

Massnahme 13
In der normalen Lage sollen die relevanten und zuständigen Akteure aus Wirtschaft, Gesellschaft und Behörden mit einem Kontinuitätsmanagement die Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen in enger Zusammenarbeit stärken und verbessern. **(EVD, EFD, VBS, UVEK)**

Umsetzung
Das EVD passt im Rahmen der Revision des LVG seine Kompetenzen entsprechend an, um mit allen Teilsektoren des Bereiches ICT-I der Wirtschaftlichen Landesversorgung (WL) periodische (mindestens einmal jährliche) Risikoanalysen durchführen zu können und die Ergebnisse mit diesen in entsprechenden Kontinuitätsmanagementplänen umzusetzen. Entsprechend wird der Bereich ICT der WL personell per Ende 2015 personell gestärkt.

MELANI stärkt den freiwilligen Informationsaustausch mit KI-Betreibern untereinander zur Unterstützung der Kontinuität und Widerstandsfähigkeit in der normalen Lage auf der Basis der Selbsthilfe. Auf Grund des erhöhten Bedarfs an forensischer Fähigkeiten, zunehmenden Informationsflusses und der Stärkung des Informationsaustausches mit KI-Betreibern und der Wirtschaft wird MELANI per Ende 2017 kontinuierlich zur Bewältigung dieser Aufgabe personell verstärkt.

Massnahmen 14
In einer Krise sollen die Aktivitäten in erster Linie mit den direkt betroffenen Akteuren durch MELANI koordiniert und die Entscheidfindungsprozesse mit fachlicher Expertise unterstützt werden, um ein kohärentes Handeln zur Bewältigung der Krise zu gewährleisten. Der nationale und internationale Informationsaustausch spielt für die Krisenbewältigung eine wesentliche Rolle und muss deshalb sichergestellt werden und koordiniert erfolgen. **(EVD, EFD, VBS, EJPD)**

Umsetzung
Zur Unterstützung der betroffenen Akteure in einer Krise, stärkt MELANI den freiwilligen Informationsaustausch mit den KI-Betreibern und seinen internationalen Partnern und stellt bei Bedarf den Einbezug polizeilicher Stellen sicher. Auf Grund des erhöhten Bedarfs an forensischer Fähigkeiten, zunehmenden Informationsflusses und der Stärkung des Informationsaustausches mit KI-Betreibern und der Wirtschaft wird MELANI per Ende 2017 kontinuierlich zur Bewältigung dieser Aufgabe personell verstärkt.

Massnahme 15
Im Falle einer spezifischen Bedrohung, werden aktive Massnahmen zur Identifikation der Täterschaft und ihrer Absichten, zur Ermittlung der Fähigkeiten der Täterschaft und zur Beeinträchtigung ihrer Infrastruktur vorgesehen. **(EFD, VBS)**

Umsetzung
Der Nachrichtendienst des Bundes wird gemäss dem Bedarfsausweis von 2011 personell per Ende 2016 personell gestärkt um die Cyber-Ausprägung seines Auftrages wahrzunehmen. Dies passiert unter Einbezug der FUB als technischer Dienstleistungserbringer für den NDB. Die Erkenntnisse der Analyse der Bedrohungslage durch MELANI und polizeiliche Erkenntnisse fliessen in die Massnahmen ein.

Massnahme 16
Für den Fall der ausserordentlichen Lage ist in Zusammenarbeit mit den zuständigen Stellen (in erster Linie BR, BK und VBS) ein Konzept für eine Führungsorganisation auszuarbeiten. Dieses erfolgt in enger Abstimmung mit der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen". **(BK, VBS, EVD, EFD)**

Umsetzung
Die BK bildet per Ende 2012 in enger Zusammenarbeit mit dem VBS, dem EFD, dem EVD und der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen" eine Arbeitsgruppe zur Erarbeitung eines Konzeptes für eine Führungsorganisation in ausserordentlichen Lagen. Dieses Konzept soll rechtliche, strukturelle und personelle Fragen klären dem Bundesrat per Ende 2015 vorgelegt werden.

4.3.7 Handlungsfeld 7: Rechtliche Grundlagen

Identifikation, Analyse und Bewertung
Rechtliche Grundlagen für den Cyber-Bereich finden sich heute in einer Vielzahl von Bundesgesetzen und Verordnungen. Problematisch dabei ist, dass diese Regelungen kaum aufeinander abgestimmt und zum Teil noch lückenhaft sind.

Ungeklärt ist auch die Möglichkeit der Verwaltung, über ihre Stellen hinaus rechtlich verpflichtende Auflagen zu machen im Zusammenhang mit der Minimierung von Cyber-Risiken.

Leistungsziele und Planung
Die bestehenden, verschiedenen Rechtsgrundlagen widerspiegeln die Cyber-Ausprägung von bestehenden Aufgaben und Verantwortlichkeiten. Entsprechend ist eine Lösung im Rahmen eines einzigen Cyber-Spezial-Gesetzes ungeeignet. Die bestehenden Gesetzeswerke sind daher fortlaufend, im Rahmen der Revision an die Entwicklungen im Cyber-Bereich innerhalb ihres Geltungsbereiches anzupassen. Die Kohärenz und Konsistenz dieser Arbeiten ist jedoch zwingend sicherzustellen. Auch ist die Frage zu klären, in welchem Ausmasse rechtliche Grundlagen zur Verpflichtung relevanter Akteure über die Behördenstellen hinaus bereits existieren, respektive welche Grundlagen geschaffen werden müssten um dies zu erreichen.

Massnahmen

Massnahme 17
Bestehende rechtliche Grundlagen sind im Hinblick auf die Massnahmen auf ihre Kohärenz und Lückenlosigkeit hin zu überprüfen. Dabei ist eine Priorisierung vorzunehmen um jene Grundlagen unverzüglich anzupassen, die nicht erst im Rahmen einer periodischen Revision einer Überarbeitung bedürfen. **(EJPD)**

Umsetzung
Das EJPD erarbeitet per Ende 2013 eine erste Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarfs im Cyber-Bereich, auf Grund der dargelegten Massnahmen. Als prioritär identifizierte Gesetzgebungslücken und rechtliche nötige Anpassungen sind von den jeweiligen Departementen ab 2014 prioritär anzugehen und per Ende 2014 abzuschliessen.

Massnahme 18
Das EJPD prüft die Grundlagen und Möglichkeiten zur rechtlichen Verpflichtung von Stellen und Organisationen über die Bundesbehörden hinaus im Hinblick auf Massnahmen zur Minimierung von Cyber-Risiken.

Umsetzung
Das EJPD erarbeitet per Ende 2017 ein Konzept und rechtliche Optionen, welche Anpassungen nötig würden, um insbesondere KI-Betreiber und im Falle einer ausserordentlichen Lagen die relevanten Akteure rechtlich verpflichten zu können. Dies geschieht in enger Zusammenarbeit mit der Umsetzung der „Nationalen Strategie Schutz Kritischer Infrastrukturen“ des BABS.

4.3.8 Koordinationsstelle zur Strategieumsetzung

Die stufengerechte Erarbeitung und Umsetzung der Massnahmen ist Sache der jeweiligen verantwortlichen Stellen innerhalb ihres Auftrages und erfolgt *in Zusammenarbeit* mit deren jeweiligen, zuständigen Partnern in Behörden (auf Stufe Bund, Kantone und Gemeinden), aus Wirtschaft (Betreiber und Verbände) und Gesellschaft. Die zuständigen Stellen sind verantwortlich, den Einbezug dieser Akteure sicher zu stellen.

Eine Koordinationstelle unterstützt in enger Zusammenarbeit mit den verantwortlichen Stellen die fortlaufende Erfüllung der geforderten Massnahmen. Dies soll im Zeitraum von vier bis sechs Jahren soweit möglich innerhalb bestehender Strukturen aufgebaut oder ausgebaut und erreicht werden.

Aufgaben dieser Koordinationstelle sind:

- Setzt einen interdepartementalen Steuerungsausschuss ein, der aus Vertretern der verantwortlichen Bundesstellen besteht.
- Begleitet die Fachgruppe „Cyber“, die im Rahmen des Konsultations- und Koordinationsmechanismus des Sicherheitsverbundes Schweiz (KKM-SVS) geschaffen wird und die Umsetzung der Massnahmen mit den Kantonen fördert und begünstigt.
- 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 eine Koordination der Umsetzung im Rechtssetzungsbereich. Insbesondere mit bereits bestehende und zukünftige Rechtssetzungsprojekten und Gesetzesrevisionen (FOGIS, PolAG, NDG, LVG, BÜPF).
- Ist für die Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken zuständig, unter Berücksichtigung der Nationalen Strategie zum Schutz kritischer Infrastrukturen (VBS-BABS) und der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz (UVEK-BAKOM).
- Überprüft mit den verantwortlichen Stellen eine mögliche Vereinfachung und Verschlankung der Meldewege und –systeme.
- Überprüft mit den verantwortlichen Stellen mögliche Synergien (z.B. im technisch-operativen Bereich).
- Überprüft nach vier Jahren die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken und deren Umsetzungsplanung im Hinblick auf die Entwicklung im Cyber-Bereich und den getroffenen Massnahmen. Dazu wird ein systematisches Benchmarking erstellt.