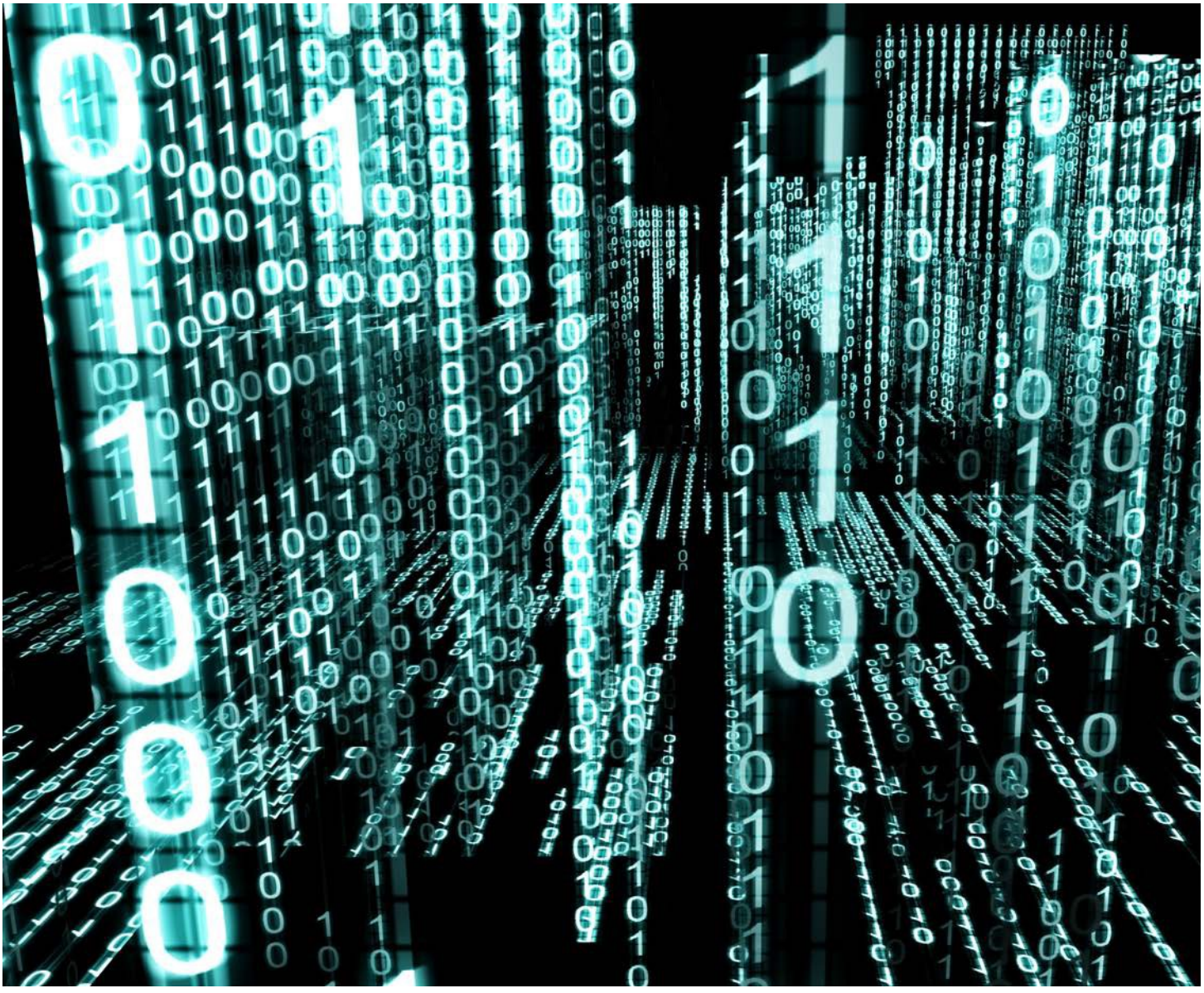
Mai 2014 | www.isb.admin.ch

# Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

# Jahresbericht 2013 des Steuerungsausschusses NCS



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
**Informatiksteuerungsorgan des Bundes ISB**
Melde- und Analysestelle Informationssicherung MELANI

**Publikation:** Mai 2014

**Redaktion:** Koordinationsstelle NCS

Eidgenössisches Finanzdepartement EFD

**Informatiksteuerungsorgan des Bundes ISB**
Melde- und Analysestelle Informationssicherung MELANI

Schwarztorstrasse 59
CH-3003 Bern

Tel +41 (0)31 322 45 38
E-Mail: info@isb.admin.ch

**Jahresbericht unter:** www.isb.admin.ch/...

# Inhaltsverzeichnis

# Vorwort

Das Internet ist in den letzten Jahren zu einem gesellschaftlich und wirtschaftlich wichtigem Lebensraum herangewachsen. Die Nutzung des Internets stellt einen wesentlichen Baustein für Freiheit, Produktion, Handel, Information und Selbstbestimmung dar. Jeder kennt es, jeder nutzt es und jeder möchte sich dort aufhalten und aktiv sein. Grösste Börsenkapitalisierungen sind diejenigen von Internetfirmen. Doch leider ist der Lebensraum Internet wie das reale Leben nicht frei von Gefahren. Anfeindungen, Kriminalität und geopolitische, staatliche Interessen sind hier ebenfalls Realität geworden. Der Bundesrat hat diese Gefahren erkannt. Mit der Verabschiedung der Strategie zum Schutz der Schweiz vor Cyber Risiken (NCS) und dessen Umsetzungsplan hat er die Grundlage gelegt, das Thema Internet und Sicherheit anzugehen. Die Strategie beschreibt die Massnahmen und Mechanismen die ergriffen werden, um der Schweiz eine friedliche und freiheitliche Nutzung des Internets auf allen Ebenen der Gesellschaft zu ermöglichen. Es geht darum, alle betroffenen Akteure – und das sind naturgemäss im Internet sehr viele – in der Schweiz zu sensibilisieren und zu befähigen, ihre Verantwortung wahrzunehmen und die Cyber Risiken bzw. deren Auswirkungen im Rahmen ihres Risiko Managements zu minimieren.

In 16 Massnahmen wird die Strategie umgesetzt. Bei der Melde und Analysestelle Informationssicherung MELANI sorgt eine kleine Koordinationsstelle für eine vernetzte Umsetzung. Damit wird sichergestellt, dass nicht nur alle Beteiligten berücksichtigt werden, sondern auch ein gemeinsames Ziel „Sicherheit im Internet“ erreicht werden kann. Mit diesen Massnahmen wird ein Überblick über die schweizerische Gesamtlage der Cyberbedrohungen als auch der Umgang mit kritischen Cyberangriffen behandelt. Die Bedrohungslagen sind vielfältig, die Technologien sind sehr komplex und Politik und Wirtschaft müssen sich auf die neuen Phänomene einstellen. Da sowohl die Technisierung als auch die Vernetzung weiter zunehmen wird, wird sich das globale System Internet weiter entwickeln.

Der vorliegende erste Jahresbericht zur Umsetzung der NCS gibt einen Überblick über die aktuelle Bedrohungslage, v.a. aber über die eingeleiteten Massnahmen und deren Stand. Er zeigt die Vernetzung der Thematik auf und unterstreicht die Verantwortung aller Beteiligten. Mit der Strategie konnte eine breite Bewegung ausgelöst werden. Nun ist es an allen, diese Bewegung zu gemeinsamen Ergebnissen zu führen. Die Voraussetzungen sind geschaffen. Die Erwartungen gross.

# 1 Management Summary

Cyber-Bedrohungen sind real, vielfältig und haben in den letzten Jahren stark zugenommen. Zudem sind auch neue Akteure aufgetreten, die besser organisiert sind. Wer diese neuen Akteure und welches die wichtigsten Tendenzen rund um die Gefahren im Cyber-Bereich in der Schweiz und international sind, wird im Halbjahresbericht 2013/I der Melde- und Analysestelle Informationssicherung (MELANI) und im Jahresbericht 2013 der Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) erläutert und zusammengefasst. Diese Berichte bieten Beurteilungen der Cyber-Bedrohungen und Empfehlungen der zu treffenden Massnahmen.

Cyber-Risiken entstehen, wenn Verwundbarkeiten oder Schwachstellen der Informations - und Kommunikations-Infrastrukturen auf Gefärdungen treffen. Deshalb hat der Bundesrat die «Nationale Strategie zum Schutz der Schweiz vor Cyber Risiken (NCS)»[1] verabschiedet, um die Schweiz gegen diese Cyber-Bedrohungen zu schützen. Das Parlament (sicherheitspolitische Subkommissionen des Nationalrates und Ständerates) nimmt sich dieser Cyber-

[1] http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de

Problematik auch zunehmend an und hat dies in zahlreichen parlamentarischen Vorstössen in den vergangenen Jahren behandelt. Die wichtigsten parlamentarischen Vorstösse der letzten Jahre zu diesem Thema sind im Anhang aufgeführt.

Mit der Verabschiedung der NCS am 27. Juni 2012 und deren Umsetzungsplan am 15. Mai 2013 (Umsetzungsplan zur «Nationale Strategie zum Schutz der Schweiz vor Cyber Risiken (UP NCS)»)[2] hat der Bundesrat den Grundstein gelegt, die Cyber-Problematik anzugehen (s. Anhang 7.1). Die NCS fokussiert insbesondere auf die frühzeitige Erkennung vor Cyber-Risiken und Bedrohungen sowie auf eine Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen. Ebenfalls bezweckt sie eine generelle Reduktion von Cyber-Bedrohungen, insbesondere Cyber-Spionage, Cyber-Sabotage und Cyber-Kriminalität. Die Kompetenzen und Aufgaben der Strafverfolgungsbehörden von Bund und Kantonen zur Bekämpfung der Internetkriminalität, werden durch die NCS jedoch nicht berührt.

Die Rahmenbedingungen und Voraussetzungen dafür sind das Handeln im Rahmen der bestehenden Kompetenzen und die nationale Zusammenarbeit zwischen Wirtschaft und Behörden, sowie eine internationale Kooperation. Die Strategie verfolgt einen dezentralen-Ansatz und behandelt Cyber-Risiken als Teil der bestehenden Geschäfts- oder Verwaltungsprozesse. Politik, Staat, Wirtschaft und die Betreiber von kritischen Infrastrukturen analysieren die Cyber-Risiken in ihren jeweiligen Bereichen und reduzieren sie falls notwendig. Mit der Strategie wird zudem sichergestellt, dass Wirtschaft und Betreiber kritischer Infrastrukturen subsidiär unterstützt werden können.

Die Strategie enthält 16 Massnahmen, die in sieben Handlungsfelder eingeteilt sind und bis 2017 umgesetzt werden sollen. In 2017 findet dann eine Wirkungsanalyse statt, um das weitere Vorgehen und den Stand der Erkenntnisse zu den finanziellen und personellen Auswirkungen der NCS zu evaluieren. Die für die Umsetzung notwendigen Ressourcen sind im Frühjahr 2013 von den verantwortlichen Bundesstellen ausgewiesen worden. Basierend auf diesem Nachweis hat der Bundesrat im Rahmen der Verabschiedung des Umsetzungsplans 28 neue Stellen für Cyber-Expertinnen und -Experten in den verantwortlichen Departementen gutgeheissen. Der Umfang der benötigten Ressourcen für die Strafverfolgungsbehörden von Bund und Kantonen zur Umsetzung des im Rahmen der Massnahme 6 NCS zu erstellenden Konzepts, wird erst darin ausgewiesen und beantragt werden können.

Es ist wichtig festzuhalten, dass die Strategie einen Umsetzungsprozess ausgelöst hat und einen kontinuierlichen Prozess darstellt, der periodisch überprüft und aktualisiert werden muss. Es wäre falsch zu denken, dass die Umsetzung im 2013 beginnt und 2017 beendet ist. Im Gegenteil, die Strategie wird bereits 2014 und 2015 auf der operativen Ebene erste Wirkungen erzielen und wird auch nach 2017 nicht abgeschlossen sein. Die daraus hervorgehenden Aktivitäten müssen laufend überprüft und der sich verändernden Bedrohungslage angepasst werden. Auch zielen die Massnahmen zur Umsetzung der Strategie darauf ab, die Fähigkeiten von Wirtschaft und Verwaltung so zu entwickeln, dass sie in der Lage sind, auch langfristig mit den Cyber-Bedrohungen umzugehen.

Um die Umsetzungsarbeiten zu koordinieren hat der Bundesrat eine im Informatiksteuerungsorgan des Bundes (ISB) angesiedelte Koordinationsstelle (KS NCS) damit beauftragt. Sie hat mit den für die NCS Massnahmen verantwortlichen Ämtern den Zielzustand, die Meilensteine und den Zeitplan für die jeweiligen Massnahmen definiert und in einer Roadmap visualisiert. Der Bundesrat hat einen Steuerungsausschuss (STA NCS) und seine Mitglieder ernannt, der im Auftrag des Bundesrates die koordinierte, zielgerechte Umsetzung der NCS sicherstellt. Er überprüft anhand eines strategischen Controllings den zielgerechten Fortschritt der Massnahmen und berichtet diesen via die Generalsekretärenkonferenz (GSK) an den Bundesrat. Die konstituierende Sitzung des Steuerungsausschusses hat am 30. Oktober 2013 stattgefunden.

[2] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=de

Zudem wurden zwei weitere Fachgruppen konstituiert. Einerseits die Fachgruppe Cyber (FG-C) des KKM SVS (Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz). Andererseits die Fachgruppe Cyber International (FG-CI) unter der Federführung des Eidgenössisches Departements für auswärtige Angelegenheiten (EDA), um einerseits den Informationsfluss zwischen Bund und Kantonen und anderseits die Arbeiten im internationalen Bereich sicher zu stellen.

Die Umsetzungsarbeiten der NCS erfolgen in Zusammenarbeit mit den Verantwortlichen der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz (BAKOM)[3], der Nationalen Strategie zum Schutz kritischer Infrastrukturen (BABS)[4] und dem Risikomanagement Bund[5]. Wie geplant haben die Umsetzungsarbeiten NCS der meisten Massnahmen begonnen und bei einigen sind die ersten Meilensteine Ende 2013 erreicht. Im vorliegenden Jahresbericht informieren die verantwortlichen Stellen in Kapitel 4 über den Stand der Umsetzungsarbeiten.

[3] http://www.bakom.admin.ch/themen/infosociety/index.html?lang=de. Der Bundesrat hat am 19. Februar 2014 vom Stand der Arbeiten zur Umsetzung der Strategie für eine Informationsgesellschaft in der Schweiz Kenntnis genommen (siehe Informationsnotiz UVEK vom 12. Februar 2014): Berichterstattung über die Umsetzung der Strategie Informationsgesellschaft

[4] http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.html

[5] http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf

# 2 Eckdaten

**27. Juni 2012: Bundesrat verabschiedet «Nationale Strategie zum Schutz der Schweiz gegen Cyber Risiken (NCS)» (s. Anhang)**

- Grundstein ist gelegt für eine umfassende Behandlung der Cyber-Problematik.
- Fokus: frühzeitige Erkennung vor Cyber-Risiken; Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen; generelle Reduktion von Cyber-Risiken (Cyber-Kriminalität, Cyber-Spionage, Cyber-Sabotage).
- 16 Massnahmen, die in sieben Handlungsfelder eingeteilt sind.

**15. Mai 2013: Bundesrat verabschiedet den Umsetzungsplan zur «Nationalen Strategie zum Schutz der Schweiz vor Cyber Risiken (UP NCS)» (s. Anhang)**

- Detaillierter Umsetzungsplan NCS für die 16 Massnahmen, die bis Ende 2017 umzusetzen sind, liegt vor.
- Die im Informatiksteuerungsorgan des Bundes (ISB) angesiedelte Koordinationsstelle (KS NCS) ist verantwortlich für die Koordination der Strategieumsetzung.
- Die dazu notwendigen Ressourcen sind im Frühjahr 2013 von den verantwortlichen Bundesstellen ausgewiesen worden.
- Es wurde ein Umsetzungsprozess ausgelöst, ‚der vor 2017 auf operativer Ebene Wirkung zeigt.
- Der gesamte Umsetzungsprozess wird auch nach 2017 nicht abgeschlossen sein.

**15. Mai 2013: Bundesrat verabschiedet das Mandat Steuerungsausschuss NCS (s. Anhang)**

- Der Steuerungsausschuss NCS stellt im Auftrag des Bundesrates die koordinierte, zielgerichtete Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber Risiken (NCS)» sicher.
- Der Steuerungsausschuss NCS überprüft durch ein strategisches Controlling den zielorientierten und terminlichen Fortschritt des Massnahmenportfolios der Strategie und rapportiert diesen via GSK an den Bundesrat.
- Die Mitglieder des STA NCS sind ernannt worden. Die konstituierende Sitzung hat am 30. Oktober 2013 stattgefunden.

**25. Oktober 2013: Schaffung der Fachgruppe Cyber-International (FG-CI) unter der Leitung des EDA**

- Die FG-CI bezweckt, einen Überblick über die jeweiligen internationalen Aktivitäten der einzelnen Bundesstellen zu schaffen.
- Die FG-CI dient der Koodinationsstelle NCS als weitere Plattform, um den Umsetzungsstand der Cyber-Strategie zu präsentieren.
- In der interdepartementalen Fachgruppe sind folgende Stellen vertreten: EDA-PD und DV; UVEK-BAKOM und BFE; EFD-ISB; VBS-SIPOL, NDB, Armeestab und FUB; EJPD-fedpol und BJ.

**18. Dezember 2013: Schaffung der Fachgruppe Cyber (FG-Cyber) des KKM Sicherheitsverbund Schweiz (SVS)**

- Die FG-C koordiniert die NCS-Umsetzung auf Stufe Kanton.
- Sie bildet die Schnittstelle zwischen Bund und Kantonen.
- Die Koordinationsstelle NCS ist Mitglied der FG-C und bildet auf Stufe Bund die Brücke mit den Projektarbeiten der FG-C, um Synergien optimal zu nutzen.
- Aufgaben: Einbezug der Kantone als zentrale Partner in sämtliche sie betreffenden Umsetzungsmassnahmen.
- Die konstituierende Sitzung hat am 18. Dezember 2013 stattgefunden.

# 3 Aktuelle Bedrohungen, Ziele und Kernpunkte der NCS

## 3.1 Cyber-Bedrohungen

In den letzten Jahren haben die Bedeutung und der Einsatz von Informations- und Kommunikationsmitteln (IKT-Mitteln) stark zugenommen und somit die Wirtschaft, den Staat und die Gesellschaft grundlegend verändert. Auch ist die Anzahl der Teilnehmenden an diesen Prozessen gestiegen. Der Zugang zu wertvollen Informationen ist wesentlich einfacher geworden. Für die Entwicklung der schweizerischen Volkswirtschaft ist der Einsatz von IKT-Mitteln sowohl für den Umgang der steigenden Informationsbedürfnisse als auch für das Wachstum, die Innovation und den Wohlstand unerlässlich. Leider hat die Nutzung des Cyber-Bereichs nicht nur viele Vorteile und Chancen gebracht. Zwielichtige Personen, Organisationen und Staaten nutzen den Cyber-Raum für kriminelle Handlungen oder verfolgen machtpolitische Ziele. Informationstechnologien können für Spionage, Erpressung oder Sabotage böswillig verwendet werden. Dabei handelt es sich bei der Täterschaft oft nicht um Einzelpersonen, sondern um hervorragend organisierte Gruppierungen. Teilweise werden diese vermutlich von Staaten finanziert, oder gewisse Staaten sind direkt daran beteiligt. Cyber-Angriffe haben nicht nur zugenommen, sondern sind gezielter, besser organisiert und insgesamt professioneller geworden.

Störungen, Manipulationen und Angriffe, die einen Ausfall des Internets herbeiführen, könnten verheerende Konsequenzen für unsere Gesellschaft haben. Insbesondere Cyber-Angriffe auf kritische Infrastrukturen (Energie, Verkehr, usw.) können gravierende Folgen haben, weil sie deren Funktionieren beeinträchtigen und fatale Kettenreaktionen auslösen können. Die kritischen Infrastrukturen in der Schweiz werden sowohl von privatwirtschaftlichen als auch von öffentlich-rechtlichen Akteuren betrieben. Zu den kritischen Infrastrukturen gehören unter anderem auch die Behörden und Verwaltungen aller Ebenen (Bund, Kantone, Gemeinden). Sie können u.a. durch Cyber-Risiken in ihrer Funktion als Legislative, Exekutive oder Judikative gehindert werden, können aber auch als Nutzende anderer kritischer Infrastrukturen indirekt betroffen sein. Cyber-Risiken betreffen letztlich aber alle Nutzer privater und beruflicher Informations- und Kommunikationssysteme sowie kritischer Infrastrukturen.

Der Halbjahresbericht 2013/I der Melde- und Analysestelle Informationssicherung (MELANI)[6] und der Jahresbericht 2013 der Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) erläutern die aktuellen und wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) in der Schweiz und international einhergehen.

Nachfolgend sind die aktuellen Cyber-Bedrohungen kurz zusammengefasst.

**CYBER-BEDROHUNGEN 2013**

Das Jahr 2013 war primär geprägt von den Enthüllungen durch Edward Snowden und den Machenschaften von grossen Nachrichtendiensten wie beispielsweise die National Security Agency (NSA) in den USA oder Government Communications Headquarters (GCHQ) in England. Solche Enthüllungen decken die Dominanz einzelner Länder auf und zeigen, wie Staaten Einfluss auf Firmen nehmen können, die Hard- oder Software entwickeln und verkaufen. Dies hat zur Folge, dass sich Betreiber von kritischen Infrastrukturen aber auch KMU klar überlegen müssen, was für vertrauliche oder sogar geheime Daten und Informati-

[6] MELANI ist vom Bundesrat mit dem Schutz kritischer Infrastrukturen in der Schweiz beauftragt: http://www.melani.admin.ch/

onen sie haben und wie diese adäquat zu schützen sind.

Die Verwaltung, die Betreiber kritischer Infrastrukturen aber auch die KMU sind nach wie vor den Cyber Gefahren ausgesetzt. Die Möglichkeiten des Internets sind hierbei enorm, und gezielte Spionageangriffe gehören unterdessen zur Tagesordnung. Die Angreifer passen sich sehr schnell neuen Technologien an. So haben diese beispielsweise im Bereich des e-Bankings Trojaner entwickelt, die gezielt mobile Anwendungen wie beispielsweise. e-Banking Apps über das Handy angreifen und entsprechend manipulieren. Somit können neu auch SMS, die zur Transaktionssignierung dienen, abgefangen und missbräuchlich verwendet werden.

Der Halbjahresbericht 2013/I von MELANI berichtet, dass Angriffe und Attacken auf kritische Infrastrukturen der Schweiz sowie im Ausland zugenommen haben: DDos-Attacken, Phishing-Trends, Schadsoftware, Ransomware und e-Mail Links mit Trojanern, sowie gezielte Social Engineering-Angriffe sind in den letzten Jahren zahlreicher und intensiver geworden. So ereigneten sich in der ersten Hälfte 2013 die bisher grössten DDos- Attacken (Spamhaus-Amplifikationsattacke, Operationen von Anonymous) in der Geschichte des Internets. Auch konnte eine starke Zunahme von e-Banking-Schadsoftwarte auf Smartphones (Trojaner Gozi, Citadel Malware und Reveton Randsomeware) und e-Mails mit Link auf eine infizierte Seite sowie VoIP (Voice over IP)[7] Missbrauch beobachtet werden. Im ersten Halbjahr 2013 wurde auch eine neue Angriffswelle auf Schweizer e-Banking-Geschäfte mit SMS-Transaktionssignierung gemeldet, die missbräuchliche Zahlungen zur Folge hatten.

Auf internationaler Ebene stehen nebst den Entdeckungen von Edward Snowden (Cyber-Spionage Programme: Prism, Tempora, XKeyscore), auch weitere politische Spionage und Sabotage (z. B. Flame, Red October, Stuxnet)[8] im Vordergrund.[9]

[7] Die ist die Bezeichnung für die Technologie, mit der über IP-Netze telefoniert werden kann, entweder auf einem privaten, kontrollierten Netz oder via öffentliches Internet.

[8] **Flame** ist die größte Cyber-Waffe, die bis jetzt entdeckt wurde. Das Programm wurde dazu entwickelt, Cyber-Spionage zu betreiben. Es kann wertvolle Informationen stehlen, einschließlich, aber nicht begrenzt auf, Bildschirminhalte des Computers, Informationen über Zielsysteme, gespeicherte Dateien, Kontaktdaten und sogar Audio-Gespräche. Seine Komplexität und Funktionalität übertreffen die aller anderen bekannten Cyber-Waffen. **Operation Red October** ist ein weiteres Spionage-Netzwerks. Seine Struktur soll sich auf dem Niveau der hochkomplexen Infrastruktur des Flame-Virus bewegen. Bei **Stuxnet** handelt es sich um eine Cyber-Sabotage. Das Schadprogramm wurde speziell für ein bestimmtes System zur Überwachung und Steuerung technischer Prozesse (SCADA-Systeme) entwickelt. So wurde die iranische Atomanlage Busher angegriffen. Stuxnet gilt aufgrund seiner Komplexität und des Ziels, Steuerungssysteme von Industrieanlagen zu sabotieren, als bisher einzigartig.

[9] Für Details dieser Cyber-Angriffe siehe MELANI Halbjahresberichte 2011, 2012 und 2013 auf www.melani.admin.ch

## 3.2 Ziele der NCS

Cyber-Risiken sind ernst zu nehmen, sie wachsen in ihrer Dimension und in ihrer Dynamik rapide, wie dies die letzten Jahre aufgezeigt haben. Der Bundesrat hat entschieden, dass der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt und hat deshalb die «Nationale Strategie zum Schutz der Schweiz vor Cyber Risiken (NCS)» in Auftrag gegeben und diese am 27. Juni 2012 und den Umsetzungsplan (UP NCS) dazu am 15. Mai 2013 verabschiedet. Er verfolgt damit drei strategische Hauptziele: die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich, die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen und die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.

Mit der NCS und dem UP NCS hat der Bundesrat den Grundstein für eine umfassende Behandlung der Cyber-Problematik gelegt. Auch wurden in mehreren parlamentarischen Vorstössen, die im Anhang beschrieben sind, Massnahmen gegen diese Cyber-Bedrohungen gefordert.

Die NCS ist eine integrale Strategie, die mit ihren 16 Massnahmen (M1-M16, s. Abbildung 1) einen umfassenden Ansatz verfolgt und die Schweiz gegenüber Cyber-Bedrohungen schützen will. Der Bundesrat hat entschieden, dass die 16 NCS Massnahmen entsprechend ihrer zeitlichen Entfaltung und Abhängigkeiten in vier Bereiche aufgeteilt werden. Um eine Cyber-Widerstandsfähigkeit zu erreichen braucht es ein Prävention, eine Reaktion, eine Kontinuität und unterstützende Prozesse.

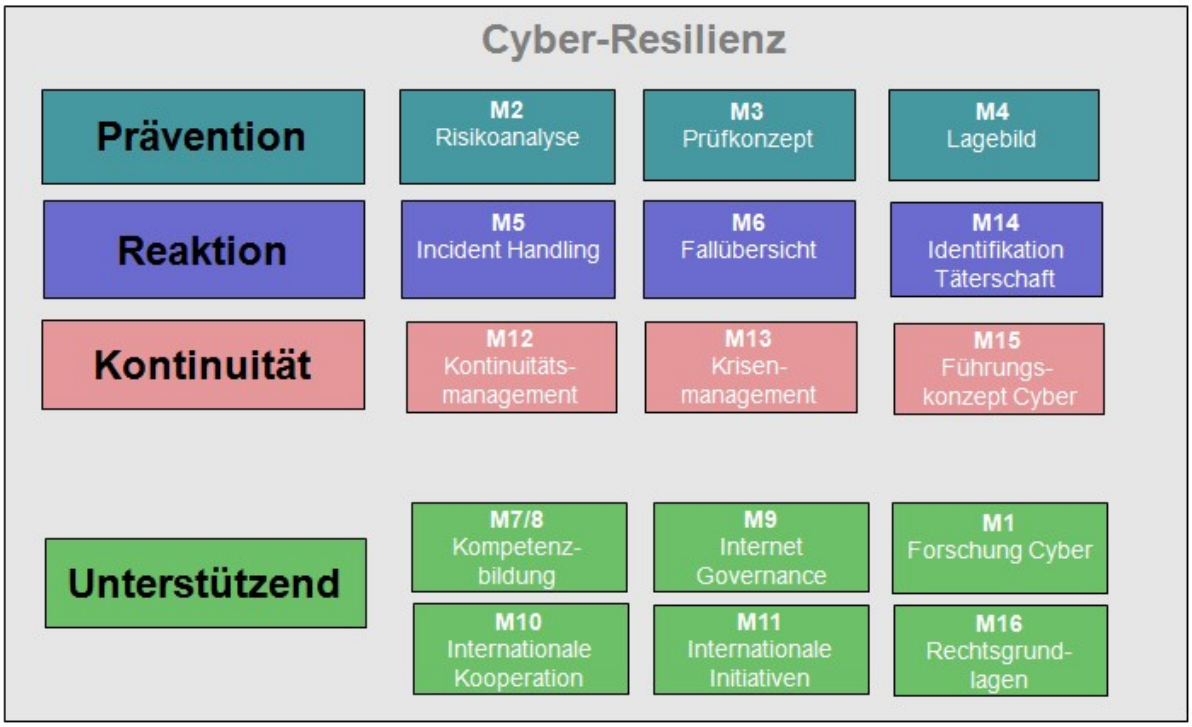


Abbildung 1: Die 16 Massnahmen der NCS

Die vier Bereiche sind:

- Prävention: Ohne eine klare Einschätzung der Cyber-Bedrohungen können keine geeigneten Sicherheitsmassnahmen implementiert werden. Deshalb braucht es im Bereich Prävention eine Risiko- und Verwundbarkeitsanalyse sowie eine Bedrohungsanalyse. Auch die besten präventiven Massnahmen können nicht verhindern, dass Vorfälle passieren, daher müssen wir die Fähigkeiten ausbauen, um auf Vorfälle reagieren zu können.

- Reaktion: Eine effiziente Reaktion umfasst das «Incident Handling», die Identifikation der Täterschaft sowie die Schnittstellen mit der Strafverfolgung. Sobald der Vorfall erfolgreich behoben worden ist, fliessen die Erkenntnisse zurück in den Bereich Prävention, als «lessons learned», damit man im Bereich der Prävention immer auf einem aktuellen Stand ist.
- Kontinuität: Sollte sich aber ein Vorfall zu einer Krise ausweiten, braucht es ein Krisen- und Kontinuitätsmanagement.
- Unterstützende Prozesse: Dieser Prozess wird durch zahlreiche unterstützende Prozesse, in den Bereichen internationale Entwicklung, Rechtsgrundlagen und Kompetenzbildung unterstützt.

## 3.3 Kernpunkte der NCS

Die NCS betont drei Kernpunkte: Dezentraler Ansatz mit Wahrung bestehender Strukturen und Kompetenzen /Eigenverantwortung, Risikomanagement, nationale und internationale Kooperation. Diese Kernpunkte werden nun untenstehend beschrieben.

Dezentraler Ansatz mit Wahrung bestehender Strukturen und Kompetenzen/Eigenverantwortung:

Die NCS reduziert die Cyber-Risiken grundsätzlich im Rahmen bestehender Strukturen und Zuständigkeiten. Die Strategie geht davon aus, dass Cyber-Risiken Teil bestehender Verantwortlichkeiten und Prozesse sind. Die verschiedenen Akteure aus Staat, Wirtschaft und Politik sind deshalb gefordert, zunächst in ihrem Zuständigkeitsbereich die eigenen Risiken zu identifizieren und zu reduzieren. Die zuständigen Fachbehörden und Betreiber kritischer Infrastrukturen analysieren zudem die Risiken, die durch IKT-Verwundbarkeiten der kritischen Infrastrukturen für die Schweiz resultieren und reduzieren diese falls notwendig. Der Staat stellt zudem eine wirkungsvolle, subsidiäre Unterstützung sicher. Der Staat erbringt bereits heute subsidiäre Leistungen zum Schutz vor Cyber-Risiken, z. B. durch Informationsaustausch und nachrichtendienstliche Erkenntnisse. Wo notwendig, werden diese Fähigkeiten ausgebaut (z.B. bei MELANI) und bestehende Prozesse optimiert, um Cyber-Risiken wirksam reduzieren zu können.

Gesamtheitlicher Ansatz:

Die NCS-Strategie verfolgt einen integralen Risikoansatz. Ausgehend von Verwundbarkeits- und Risikoanalysen werden in den kritischen Teilsektoren ein Risikomanagement implementiert sowie ein Kontinuitäts- und Krisenmanagement aufgebaut. Ein Risiko entsteht, wenn Gefährdungen auf Verwundbarkeiten treffen. Es braucht deshalb zuerst eine Verwundbarkeitsanalyse und dann eine Risikoanalyse, um das Restrisiko zu evaluieren. Die Ergebnisse der Risikoanalyse sind in entsprechende Risiko-, Kontinuitäts- und Krisenmanagementpläne umzusetzen. Die NCS geht davon aus, dass Cyber-Risiken ein Bestandteil des Gesamtrisikos sind. Daher müssen neben den Cyber-Risiken, die hauptsächlich technischer Natur sind, auch personelle, physische und organisatorische Risiken in Betracht gezogen werden. Die zur Risikominimierung erforderlichen Massnahmen dürfen sich nicht nur auf die IKT-Sicherheit konzentrieren, sondern müssen immer alle Dimensionen in Betracht ziehen. Dies wiederum heisst, dass die Zuständigkeit beim jeweils obersten Leitungsorgan liegt und nicht an einen IKT-Sicherheitsverantwortlichen delegiert werden kann.

Nationale Kooperation:

Die Wirtschaft und Behörden werden durch die NCS zu einer engen nationalen Zusammenarbeit verpflichtet. Die NCS fördert dabei die Stärkung der Zusammenarbeit auf operativer Ebene zur Unterstützung der strategischen Ebene. Dazu soll die Schweiz ihr gefestigtes und seit 2004 funktionierendes Public Private Partnership Modell (PPP) konsequent nutzen. ME-

LANI fördert den Informationsaustausch zu Cyber-Angriffen unter den Unternehmen und unterstützt die schweizerischen kritischen Infrastruktur Betreiber subsidiär in ihrem Informationssicherungsprozess. 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 einen geschlossenen Kundenkreis, bestehend aus ausgesuchten Unternehmen/Verwaltungseinheiten, 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.

Internationale Kooperation

Die sicherheitspolitischen Interessen in Sachen Cyber müssen gegenüber der internationalen Gemeinschaft gewahrt werden. Der Cyber-Raum, der vor Landesgrenzen keinen halt macht, zeigt sich vermehrt als neue Dimension der Aussenpolitik. Bei der aussenpolitischen Interessenwahrung muss dieser neue Bereich ebenfalls berücksichtigt werden und in aussenpolitische Überlegungen Eingang finden, da die Schweiz und ihre Wirtschaft und Gesellschaft digital sehr stark vernetzt sind. Die Cyber-Sicherheit gewinnt für die Schweiz und ihren Wirtschaftsstandort kontinuierlich an Bedeutung.

Eine langfristige Erhöhung der Sicherheit der nationalen Infrastrukturen kann jedoch nur erreicht werden, wenn die Staaten auf internationaler Ebene kooperieren und zu einem gemeinsamen Verständnis kommen, wo die Grenzen zur Nutzung des Cyber-Raumes für die gewaltsame Austragung von Konflikten liegen. Auch die illegalen Aktivitäten von nichtstaatlichen Akteuren können nur verhindert werden, wenn die Staaten mittels Verhaltensnormen in die Pflicht genommen werden, diese auf ihrem Territorium zu unterbinden. In diesem Zusammenhang laufen bereits viele Prozesse und Initiativen auf internationaler Ebene, die das Ziel haben, gemeinsame Regeln zu schaffen. Die Schweiz nimmt an diesen Prozessen und Initiativen teil

## 3.4 Abgrenzung der NCS und Cyber-Defence

Die NCS konzentriert sich vor allem auf Risiken im zivilen Bereich. Die Armee erarbeitet zusätzlich eine Cyber-Defense-Strategie zum Schutz ihrer eigenen Systeme und zum Aufbau von Fähigkeiten zur subsidiären Unterstützung der zivilen Partner. Die Armee ist für den Schutz und die Abwehr von Gefahren für die eigenen Infrastrukturen und Systeme in allen Lagen selbst verantwortlich. Sie soll dennoch in ihrem Auftrags- und Verantwortungsspektrum Lösungsansätze für die Behandlung der Cyber-Bedrohung und ihre Konsequenzen bestimmen und sich auf Spezialfälle vorbereiten. Die Armee ist eng mit dem zivilen Bereich verknüpft und soll deshalb beim Aufbau ihrer Fähigkeiten zur Minimierung von Cyber-Risiken die Umsetzung mit den anderen Behörden abstimmen. Diese vorhandenen Fähigkeiten der Armee können von den verantwortlichen Ämtern in ihren Umsetzungsprozessen bei Bedarf eingebaut und abgerufen werden können. Der Chef der Armee (CdA) hat für die Erarbeitung eines Cyber-Defense-Konzeptes für die Armee einen Delegierten bestimmt. Dieser hat sein Amt am 2. Januar 2013 angetreten.

Die Minimierung der Cyber-Risiken wird auch durch eine effiziente Strafverfolgung der Internetkriminalität erreicht. Entsprechend hat die Strategie die relevanten Schnittstellen und den NCS-relevante Informationsaustausch zu regeln. Die Kompetenzen und Aufgaben der Strafverfolgungsbehörden von Bund und Kantonen zur Bekämpfung der Internetkriminalität, werden durch die NCS jedoch nicht berührt. Derzeit verfügt die Schweiz (noch) über keine eigentliche „Nationale Strategie zur Bekämpfung der Internetkriminalität“.

# 4 Stand der Umsetzungsarbeiten NCS 2013

Die Umsetzungsphase hat begonnen und die Arbeiten für die meisten Massnahmen wurden aufgenommen. Bei einigen Massnahmen sind Ende 2013 die ersten Meilensteine erreicht worden. In diesem Kapitel wird nun die Gesamtübersicht der Umsetzung in einer Roadmap NCS visualisiert und von jeder Stelle mit Umsetzungsverantwortung in einem kurzen Bericht der aktuelle Umsetzungsstand der jeweiligen Massnahmen präsentiert. Die Umsetzungsarbeiten einiger NCS Massnahmen erfolgen in Zusammenarbeit mit den Verantwortlichen der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz und der Nationalen Strategie zum Schutz kritischer Infrastrukturen.

## 4.1 Gesamtübersicht: Roadmap

Mit allen verantwortlichen Stellen hat die Koordinationsstelle NCS die Ziele und Meilensteine für die jeweiligen Massnahmen konkret definiert und in einer Roadmap dargestellt:

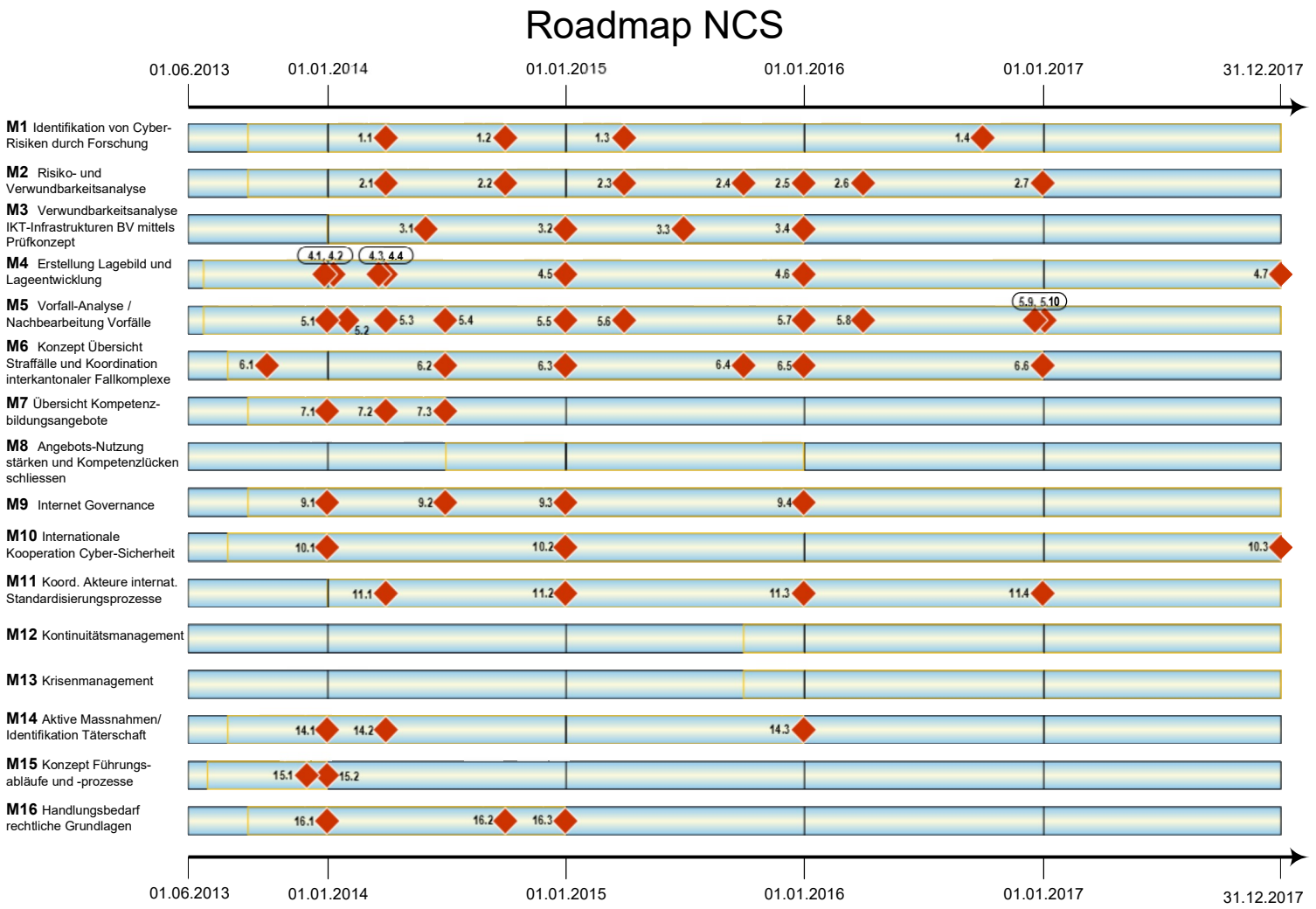



Abbildung 2: Roadmap NCS

Die vollständige Roadmap mit ihren Detailinformationen zu den Zielen und den Meilensteinen findet sich auf der Website des ISB unter www.isb.admin.ch -> Themen -> Cyber-Risiken -> Roadmap[10].

[10] http://www.isb.admin.ch/themen/01709/01841/

## 4.2 Prävention

Im Bereich Prävention sind die Massnahmen der Risiko- und Verwundbarkeitsanalyse, der Überprüfung der IKT-Verwundbarkeiten auf Stufe Bund und der Lagedarstellung enthalten. (M2, M3, M4)

### 4.2.1 Risiko- und Verwundbarkeitsanalyse (M2)

**Zuständigkeiten: WBF-BWL, VBS-BABS, Fachbehörden**; EFD-MELANI

Ziel der Risiko- und Verwundbarkeitsanalysen ist es, die von IKT-Verwundbarkeiten der kritischen Infrastrukturen ausgehenden Risiken für die Schweiz zu ermitteln. Cyber-Risiken entstehen, wenn Gefährdungen (z.B. Cyber-Attacken) auf solche Schwachstellen treffen.

Zu den Verwundbarkeitsanalysen hat das BWL in den vergangenen Jahren in Zusammenarbeit mit der Wirtschaft methodische Grundlagen erarbeitet und in verschiedenen Teilsektoren (z.B. im Energiesektor) bereits angewandt.

Das BABS hat zusammen mit den relevanten Partnern (Fachbehörden, Betreiber usw.) in allen 28 kritischen Teilsektoren (Strassenverkehr, Telekommunikation, Wasserversorgung usw.) die relevanten Prozesse, Systeme und Objekte identifiziert. Zudem wurde eine nationale Gefährdungsanalyse erstellt, die auch Cyber-Risiken beinhaltet.

Im Rahmen der Umsetzung von M2 sind diese bestehenden Arbeiten des BWL und des BABS methodisch aufeinander abzustimmen und die Risiko- und Verwundbarkeitsanalysen für alle 28 kritischen Teilsektoren durchzuführen.

Aktueller Stand:

In einem ersten Schritt sind die bestehenden methodischen Ansätze konsolidiert und das gemeinsame weitere Vorgehen definiert worden. Somit kann die Kohärenz und Vergleichbarkeit der Ergebnisse in den 28 Teilsektoren gewährleistet werden.

### 4.2.2 Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept (M3)

**Zuständigkeiten: EFD-ISB;** EFD-MELANI und BIT, VBS-FUB

Gemäss NCS haben die Bundesstellen ihre IKT-Infrastrukturen unter Einbezug der IKT-Leistungserbringer und Systemlieferanten auf Verwundbarkeit zu überprüfen. Das Informatiksteuerungsorgan Bund (ISB) im EFD wurde dazu gemäss Umsetzungsplan NCS beauftragt, bis Ende 2015 ein Prüfkonzept zur periodischen Überprüfung der IKT-Infrastrukturen der Bundesverwaltung auf systemische, organisatorische und technische Schwächen zu erstellen.

Aktueller Stand:

Die für die Umsetzung von M3 verantwortliche Stelle für den Informatiksicherheitsbeauftragten NCS wurde besetzt. Die zuständige Person konnte am 1. Februar 2014 die Arbeit am Projekt M3 aufnehmen. Im BIT werden Systeme bei der Inbetriebsetzung einer Verwundbarkeitsanalyse unterzogen. Periodische Analysen sind in Vorbereitung. Für Web-Applikationen werden bereits periodische Analysen durchgeführt.

### 4.2.3 Erstellung Lagebild und Lageentwicklung (M4)

**Zuständigkeiten: EFD-MELANI, VBS-NDB, EJPD-KOBIK;** VBS-FUB und MND, EFD-BIT

Ohne eine klare Einschätzung der aktuellen Cyber-Bedrohungen können keine geeigneten Sicherheitsmassnahmen identifiziert werden. Um den Cyber-Widerstand (Resilienz) aufzubauen und zu einer wirkungsvollen Prävention zu gelangen, braucht es daher nicht nur eine Risiko- und Verwundbarkeitsanalyseanalyse, sondern auch eine Analyse der aktuellen Bedrohungslage. Im Bereich der Lageeinschätzung sind heute verschiedene Akteure tätig.

Bereits heute werden durch die Melde- und Analysestelle Informationssicherung (MELANI) die wichtigsten Informationen aus verschiedenen Quellen gesammelt, bewertet, analysiert und in einer Darstellung der Bedrohungslage fusioniert. Diese fliessen ein in Lageberichten, Fachberichte, Factsheets, Halbjahresberichte usw.

Der Nachrichtendienst (NDB) besitzt die Fähigkeiten zur nachrichtendienstliche Informationsbeschaffung, die zur Bedrohungslage beitragen und KOBIK lässt die Erkenntnisse von Polizei und Strafverfolgungsbehörden von Bund und Kantonen einfliessen.

Ziel der NCS ist es, Doppelspurigkeiten zu vermeiden und in enger Zusammenarbeit mit allen Akteuren ein einheitliches Lagebild zu erstellen. Dazu baut MELANI für den Informationsaustausch eine geeignete Plattform auf. Beim NDB werden die Cyber-Fähigkeiten ausgebaut und bei KOBIK wird eine nationale Fallübersicht erstellt (M6). Zudem werden die technischen Kapazitäten der Computer Emergency Response Teams (CERTs) zur konstanten Überwachung der Bundesnetze ausgebaut.

Aktueller Stand:

Das Konzept zur Stärkung von MELANI als Plattform zum Informationsaustausch ist erstellt worden. MELANI/NDB hat zusammen mit dem GovCERT die notwendigen Prozesse zur Erstellung der Bedrohungslage festgelegt. Beim Nachrichtendienst des Bundes (NDB) wurde das interne Konzept zum Aufbau der Cyber-Fähigkeiten finalisiert. Daraus geht hervor, dass ein Bereich Cyber NDB aufgebaut werden soll. Die mit dem Aufbau verknüpften organisatorischen und administrativen Arbeiten sind bereits abgeschlossen und die Stellen besetzt. Dieser Cyber NDB wird für die nachrichtendienstliche Informationsbeschaffung zuhanden des Bedrohungs- und Lagebildes verantwortlich sein. Zwischen der FUB (MilCERT und Computer Network Operations (CNO)) und dem BIT (CSIRT) ist ein periodischer Informationsaustausch über Bedrohungen und Strategien der Targeterkennung in der Netzüberwachung etabliert worden.

Im MND wurde die von der NCS vorgesehene Stelle ausgeschrieben damit ab 1. April es schrittweise möglich wird, die Integration des Cyber-Lagebildes aus Sicht der Armee ins Gesamtlagebild des NDB zu integrieren.

## 4.3 Reaktion

Im Bereich Reaktion muss eine koordinierte Vorfall-Analyse und Nachbearbeitung betrieben werden, um einen Vorfall so rasch wie möglich beheben und um zum Tagesgeschäft über gehen zu können. (M5, M6, M14)

### 4.3.1 Vorfall-Analyse und Nachbearbeitung von Vorfällen (M5)

**Zuständigkeiten: EFD-MELANI, VBS-NDB;** VBS-FUB und MND, EFD-BIT

Die Fähigkeiten, auf Cyber-Vorfälle vorbereitet zu sein und darauf reagieren zu können, sind

wesentliche Rahmenbedingungen für die Reduktion von Cyber-Risiken. Gemäss Umsetzungsplan NCS sollen Vorfälle im Rahmen der Vorfall-Analyse und Nachbearbeitung überprüft und weiterentwickelt werden. Die Erkenntnisse aus relevanten Vorfällen werden dann an MELANI weitergegeben. Erkenntnisse zu staatsschutzrelevanten Vorfällen werden vom NDB via MELANI an KOBIK (Strafverfolgung) weitergegeben. Für die Vorfalls-Analyse sind die Computer Emergency Response Teams (CERTs) beim Bund, der Armee und der Betreiber kritischer Infrastrukturen zuständig.

Das bei MELANI angesiedelte GovCERT ist schon seit Jahren im Bereich Malware-Analyse aktiv. Bereits heute ist es dem GovCERT möglich, Daten bei einem Vorfall so zu analysieren und aufzubereiten, dass die angegriffene Organisation technische Gegenmassnahmen ergreifen können. Weiter stellt MELANI seit 2013 ausgewählten kritisch Infrastruktur-Betreibern technische Informationen zum Schutz ihrer Infrastruktur bereit.

Mit der Verabschiedung der NCS wurde der Auftrag zur Vorfallbearbeitung erweitert. Um diesen Auftrag zu erfüllen, müssen erstens die technischen Kapazitäten und das Spezialwissen ausgebaut werden sowie eine umfassende Analyse und Bewertung von Bedrohungen vorgenommen werden. Dazu gehört eine Erhöhung der Durchhaltefähigkeit, sowie Reaktionsfähigkeit aller CERTs sowie deren zunehmende Vernetzung untereinander.

Aktueller Stand:

Das GovCERT hat seine Fähigkeiten weiter ausgebaut. Auf technischer Ebene wurde die Organisationsstruktur im GovCERT definiert (www.GovCERT.ch)[11] sowie die erste Phase zur Erhöhung der 24/7 Durchhaltefähigkeit abgeschlossen. Dies konnte durch die Besetzung zweier zusätzlicher Stellen erreicht werden. Auf nachrichtendienstlicher Seite wurden die Konzeptarbeiten zur Strukturierung der Cyberfähigkeiten des NDB abgeschlossen und die relevanten Stelleprofile geschaffen. Zwischen der FUB (MilCERT und Computer Network Operations (CNO)) und dem BIT (CSIRT) ist die operative Zusammenarbeit bei der Bewältigung von Cyber-Vorfällen systematisiert worden. Weiter wird zur Zeit die Instrumentierung für den Informationsaustausch weiter ausgebaut und laufend eingesetzt. Auch wurden in der FUB die von der NCS zwei freigegebenen Stellen ausgeschrieben damit man diese ab Frühjahr 2014 bereits operationalisieren kann. Zusätzlich hat die Armee entschieden (siehe Kapitel 4.7) ihre eigene Detektions- und Analysemittel schrittweise zu verstärken.

### 4.3.2 Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe (M6)

**Zuständigkeiten: EJPD-KOBIK;** EFD-MELANI

Um nachhaltig Cyber-Risiken zu minimieren, bedarf es einer effizienten nationalen und internationalen Strafverfolgung zur Bekämpfung der Cyber-Kriminalität. Zu diesem Zwecke wurde in M6 der NCS festgehalten, dass die im eidgenössischen Justiz- und Polizeidepartement (EJPD) angesiedelte KOBIK, in Zusammenarbeit mit den Kantonen per Ende 2016 ein Konzept «Fallübersicht und Koordination interkantonaler Fallkomplexe» vorzulegen hat.

Im Rahmen des Konzeptes geht es nun darum, die verschiedenen Aufgaben im Zusammenhang mit der Entwicklung und Organisation der Fallübersicht anzugehen. In Zusammenarbeit mit den Kantonen soll ein Konzept zum Aufbau einer gesamtheitlichen Fallübersicht und zur Koordination interkantonaler Fallkomplexe erarbeitet werden. Dabei geht es insbesondere um die Klärung von organisatorischen, technischen, rechtlichen, ressourcenmässigen (z.B. Personalbedarf, Infrastruktur, Informatik usw.) und fachlichen Aspekten der Fragestellungen.

[11] http://www.melani.admin.ch/org/00101/01098/index.html?lang=de

Aktueller Stand:

Eine detaillierte Auftragsanalyse wurde erstellt und die Projektorganisation sowie Anspruchsgruppen definiert. Diese besteht aus Vertretern von fedpol, der Bundesanwaltschaft (BA), der Konferenz der Kantonalen Justiz Direktoren (KKJPD), der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS), der SSK (ehemals Konferenz der Strafverfolgungsbehörden der Schweiz (KSBS)), sowie aus einem Vertreter der Swiss Police ICT (Schweizer Polizei Informatik Kongress) und des Bundesamts für Justiz (BJ).

### 4.3.3 Aktive Massnahmen und Identifikation der Täterschaft (M14)

**Zuständigkeiten: VBS-NDB;** EFD-MELANI, EJPD-KOBIK, VBS-MND

Ein wichtiger Teil im Bereich der Reaktion ist nicht nur die Fähigkeiten, auf Cyber-Vorfälle vorbereitet zu sein und darauf reagieren zu können, sondern auch die Identifikation der Täterschaft. Grundsätzlich ist der NDB dafür verantwortlich, mit nachrichtendienstlichen Mitteln Informationen zu beschaffen, diese zu analysieren und auszuwerten. Er verfügt bereits heute über die Fähigkeiten zur Durchführung der Identifikation der Täterschaft. Jedoch müssen mit M14 diese Fähigkeiten (Akteur- und Umfeldanalyse und die Entwicklung technischer Hilfsmittel) weiter ausgebaut werden. Der NDB wird dabei von MELANI und KOBIK unterstützt.

Im Bereich der Akteur- und Umfeldanalyse besteht durch die Arbeiten von MELANI/NDB bereits ein hoher Grad an spezifischen Erkenntnissen. Diese Arbeiten werden nun weitergeführt und vertieft. Die Ergebnisse dieser Arbeit schaffen dabei die Grundlage zur Identifikation der Täterschaft zu erreichen.

Im Rahmen strafrechtlicher Ermittlungen können die Strafverfolgungsbehörden diverse Massnahmen zur Identifikation der Täterschaft ergreifen. KOBIK spielt eine wichtige Rolle bei der Strafverfolgung und Identifikation der Täterschaft. Werden strafrechtlich relevante Vorfälle im Rahmen der NCS erkannt, so sind diese über KOBIK den Strafverfolgungsbehörden zukommen zu lassen.

Die von der Armeeführung beschlossenen Entwicklungen (siehe Kapitel 4.7) sind für die Umsetzung dieser Massnahme auch relevant.

Aktueller Stand:

Die Organisationsstruktur für den Cyber NDB ist erstellt und die Stellen im Bereich der Akteur-Analyse sowie für die technische Entwicklungen gesprochen.

## 4.4 Kontinuität

Um das Krisenmanagement gezielt durchführen zu können, braucht es klar definierte Führungsabläufe und -prozesse für den Cyber-Fall. Das Kontinuitätsmanagement sorgt dafür, dass die Geschäftsprozesse trotz einer Krise weiterlaufen. (M12, M13, M15)

### 4.4.1 Kontinuitätsmanagement (M12)

**Zuständigkeiten: WBF-BWL, VBS-BABS, Fachbehörden;** EFD-MELANI

Auf Grundlage der Ergebnisse der Risiko- und Verwundbarkeitsanalyse (Massnahme M2) definieren das federführende BWL und das BABS mit den relevanten Unternehmern und zuständigen Fachstellen die notwendigen Massnahmen zur Sicherstellung der Kontinuität. Dabei wird ein integraler Ansatz verfolgt, mit dem gewährleistet werden soll, dass kritische

Funktionen im Fall interner oder externer Ereignisse aufrechterhalten oder zeitgerecht wiederhergestellt werden können. Es zielt darauf ab, im Ereignisfall den Ausfall der betroffenen Leistungserbringung möglichst gering zu halten.

Aktueller Stand:

Die Umsetzung der Massnahme beginnt ab Mitte 2015, da sie der Massnahme 2 nachgelagert ist.

### 4.4.2 Krisenmanagement (M13)

**Zuständigkeiten: WBF-BWL, EFD-MELANI, VBS-BABS;** EDA-PD, EJPD-KOBIK

Mit Massnahme M13 sollen die kritischen Infrastrukturen und der Bund die notwendigen Prozesse zur Bewältigung einer durch Cyber-Risiken verursachten, ausserordentlichen Lage, definieren. Die Arbeiten stützen sich dabei auf die Erkenntnisse der Risiko- und Verwundbarkeitsanalysen (Massnahme M2). Beim Krisenmanagement kann zwischen einer strategischen- und einer operativen Ebene unterschieden werden. Für Definition der Prozesse auf strategischer Ebene ist das BWL und BABS zuständig, für diejenigen der operativen Ebene MELANI.

Aktueller Stand:

Die Arbeiten für das strategische Krisenmanagement beginnen ab Mitte 2015, da sie der Massnahme 2 nachgelagert sind.

### 4.4.3 Konzept Führungsabläufe und -prozesse mit Cyber-Ausprägung (M15)

**Zuständigkeit: BK**

Im Gegensatz zum Risikomanagement sind Notfall- und Krisenmanagement Szenario-unabhängig. Führungsabläufe und Entscheidungsprozesse sind prozess-orientiert und müssen immer dieselben sein, unabhängig davon, was geschehen kann oder bereits geschehen ist. Das Krisenmanagement einer Organisation legt Struktur, Prinzipien, Vorschriften, Infrastruktur sowie Prozesse fest, um eine ausserordentliche Lage effizient bewältigen zu können.

Aktueller Stand:

Das Konzept über die Führungsabläufe und Entscheidungsprozesse ist erstellt und wurde vom Steuerungsausschuss NCS abgenommen. Es erläutert für den Fall einer cyberspezifischen Krise einzelne Eigenschaften auf strategischer Ebene. Das Konzept konzentriert sich auf die politisch-strategische Entscheidungsebene des Bundes und nicht auf die operative Ebene. Der operative Teil vom Krisenmanagement wird in M13 behandelt.

## 4.5 Unterstützende Prozesse

Es müssen auch die notwendigen Grundlagen und Prozesse erarbeitet und festgelegt werden, um die Cyber-Problematik anzugehen. Diese umfassen internationale Kooperationen, den Austausch von Erfahrungen im Bereich Bildung und Forschung sowie gegebenenfalls die Anpassung der gesetzlichen Grundlagen. (M1, M7, M8, M9, M10, M11, M16)

### 4.5.1 Identifikation von Cyber-Risiken durch Forschung (M1)

**Zuständigkeiten: Verantwortliche Bundesstelle;** KS NCS

Mit Hilfe der Forschung sollen die relevanten Cyber-Risiken der Zukunft, wie auch die Veränderungen in der Gefährdungslandschaft aufgezeigt werden, damit Entscheide in Politik und Wirtschaft frühzeitig und zukunftsgerichtet erfolgen können. Die Umsetzung dieser Massnahme erfolgt in enger Zusammenarbeit mit den Verantwortlichen der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz.

Die Koordinationsstelle NCS soll mit den Partnern relevante Themen zu Cyber-Bedrohungen identifizieren.

Aktueller Stand:

Die Koordinationsstelle NCS hat mit der Kommission für Technologie und Innovation(KTI) und dem Staatssekretariat für Bildung, Forschung und Innovation (SBFI) 4-5 der wichtigsten Cyber-Forschungsthemen der Zukunft identifiziert.

### 4.5.2 Übersicht Kompetenzbildungsangebote (M7)

**Zuständigkeiten: KS NCS;** UVEK-BAKOM, EDA-PD, EDI-BSV

Um die Cyber-Resilienz in der Schweiz zu erhöhen braucht es das Bewusstsein und Wissen sich vor Cyber-Risiken schützen zu können. Deshalb müssen gezielt spezifische Fähigkeiten (z.B. Ausbildung von IKT-Sicherheitsspezialisten, laufende Weiterbildung aller IKT-Fachkräfte in Sicherheitsbelange, juristisch-technisches Fachwissen bei den Strafverfolgungsbehörden im Zusammenhang mit Cyber-Delikten, usw.) aus- und aufgebaut werden.

Ziel der NCS ist es eine Übersicht zu erstellen, die über die bestehende Kompetenzbildungsangebote Auskunft gibt. Damit wird die Grundlage geschaffen Angebotslücken zu erkennen und über Angebote im Umgang mit Cyber-Risiken zu informieren. Die Umsetzung dieser Massnahme erfolgt in enger Abstimmung mit der Umsetzung der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz.

Das EDA hat der federführenden Stelle eine Liste mit internationalen Organisationen und Kompetenzzentren zugestellt, die cyber-spezifische Ausbildungen anbieten.“ Das EDA ist bei den Arbeiten zur Umsetzung der Massnahme 7 involviert. Der Einbezug des EDA zugunsten der Umsetzung der M7 ist im Jahresbericht 2013 zu reflektieren.

Aktueller Stand:

Die Zielgruppen aus Verwaltung, Wirtschaft und Zivilgesellschaft wurden definiert und Expertinnen und Experten nach den wichtigsten Cyber-Risiken, den notwendigen Kompetenzen und den qualitativ hochwertigen Angeboten für die jeweiligen Zielgruppen befragt.

### 4.5.3 Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken (M8)

**Zuständigkeiten: KS NCS;** UVEK-BAKOM, EDA-PD, EDI-BSV

Mit der M8 soll eine Konzept zur vermehrten Nutzung der bestehenden Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken und zur Schaffung neuer Angebote, die der Schliessung der erkannten Angebotslücken dienen, erarbeitet werden.

Aktueller Stand:

M8 basiert auf den Ergebnissen von M7 und beginnt deshalb erst nach deren Abschluss Mitte 2014.

### 4.5.4 Internet Governance (M9)

**Zuständigkeiten: UVEK-BAKOM;** EDA-PD, VBS-SIPOL, EFD-MELANI, Fachbehörden

Mit der M9 der NCS soll sich die Schweiz (Wirtschaft, Gesellschaft, Behörden) aktiv und soweit möglich koordiniert für eine Internet Governance einsetzen, die mit den Schweizer Vorstellungen von Freiheit und (Selbst-)Verantwortung, Grundversorgung, Chancengleichheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist. Das federführende BAKOM nimmt aktiv an den relevanten internationalen und regionalen Prozessen, wie z.B. ICANN (Internet Cooperation for Assigned Names and Numbers), WSIS (World Summit of the Information Society), UNO Kommission für Wissenschaft und Technik im Dienste der Entwicklung (CSTD), IGF (UN Internet Governance Forum), Europarat, teil.

Auch das EDA ist aktiv im Bereich Internet Governance. So hat es die Prozesse und Initiativen rund um Internet Governance, die eine sicherheitspolitische Komponente aufweisen, identifiziert. Als Basis dazu dienten verschiedene Studien zur Auslegeordnung diverser Prozesse und Initiativen rund um dieses Thema. Gleichzeitig unterstützt das EDA Bestrebungen auf internationaler Ebene, um den Datenschutz und das Recht auf Privatsphäre zu stärken. Dabei kann etwa auf die von der UN-Generalversammlung verabschiedete Resolution „The right to privacy in the digital age“ verwiesen werden. Die Resolution besagt unter anderem, dass Menschenrechte nicht nur offline, sondern auch online gelten.

BAKOM und EDA arbeiten im Bereich Internet Governance eng zusammen, um eine kohärente und konsistente Schweizerische Position zu gewährleisten. Das BAKOM konsultiert zudem regelmässig alle interessierten Vertreter aus Verwaltung, Wirtschaft und Zivilgesellschaft im Rahmen der Plateforme Tripartite.

Aktueller Stand:

Das BAKOM hat eine Übersicht zu den prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet Governance erstellt. Diese Übersicht soll nach ihrer Erstellung regelmässig aktualisiert werden. Zudem wurde beschlossen, die M9 in die vom Eidgenössische Departement für auswärtige Angelegenheiten (EDA) neu gegründete «Fachgruppe Cyber-International (FG-CI)» aufzunehmen.

Das BAKOM hält im Namen der Schweiz im ICANN-Regierungsbeirat (Internet Cooperation for Assigned Names and Numbers) den stellvertretenden Vorsitz inne und vertritt die Schweiz in den Zwischenstaatlichen Institutionen, die sich mit Kernfragen von Internet Governance beschäftigen wie z.B. die für den WSIS und Internet Governance in der UNO verantwortliche Kommission CSTD, die ITU, die UNESCO und den Europarat. Das BAKOM unterstützt im Namen der Schweiz auch die Vorbereitung und Durchführung des UN Internet Governance Forum (IGF) und ist es Mitinitiant und Mitorganisator des europäischen IGF-Dialogforums „EuroDIG“.

### 4.5.5 Internationale Kooperation Cyber-Sicherheit (M10)

**Zuständigkeiten: EDA-PD;** VBS-SIPOL, EFD-MELANI, UVEK-BAKOM

Massnahme 10 umfasst die sicherheitspolitische Interessenwahrung im Cyber-Bereich gegenüber dem Ausland. Mithilfe internationaler Beziehungen und Initiativen setzt sich die

Schweiz dafür ein, dass der Cyber-Raum nicht für kriminelle, nachrichtendienstliche, terroristische und machtpolitische Zwecke missbraucht wird.

Aktueller Stand:

Mit der Verabschiedung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken wurde die Abteilung Sicherheitspolitik (ASP) damit beauftragt, die Cyber-Strategie innerhalb des Departementes umzusetzen. Deshalb hat die ASP ein Konzept zur Umsetzung erarbeitet, das die verschiedenen Aktivitätsfelder und die vorhandenen Strukturen der einzelnen Organisationseinheiten, sowie der gewünschte Zustand darlegt. Der erste Meilenstein wurde somit planmässig 2013 erreicht.

Die ASP hat bereits gezielte Aktivitäten der internationalen Zusammenarbeit eingeleitet, um die Cyber-Bedrohung zu minieren. Dazu gehört im Rahmen multilateraler Kooperation die schweizerische Teilnahme am Prozess der Organisation für Sicherheit und Zusammenarbeit (OSZE) zur Erarbeitung von vertrauensbildenden Massnahmen (VBMs). Die Schweiz hat sich von Anfang an sehr aktiv an diesem Prozess beteiligt. Der Schweizer Vorschlag, vermehrt auch Vertreter des privaten Sektors im Prozess zu berücksichtigen, wurde in einer VBM aufgenommen (i.e. VBM 7: die Zusammenarbeit zwischen den öffentlichen und privaten Stellen).

Die Schweiz beteiligt sich auch am London Prozess, der die Schaffung von internationalen Verhaltensregeln vorsieht. An der „Seoul Conference on Cyberspace“ war die Schweiz mit einer interdepartementalen Delegation unter der Leitung des stellvertretenden Staatssekretärs des EDA vertreten.

Der Informationsaustausch zum Thema „Cyber“ ist ein ständiger Bestandteil der bilateralen und multilateralen sicherheitspolitischen Konsultationen mit Staaten und internationalen Organisationen (nämlich EU, NATO und Finnland) geworden. Parallel dazu wurden mit ausgewählten Staaten cyber-spezifische Konsultationen betrieben (UK) oder vereinbart (Deutschland).

Die Prüfung einer strukturierten und vertieften Zusammenarbeit mit der NATO sowie dem Kompetenzzentrum in Tallinn wurde 2013 eingeleitet. Der interdepartementale Koordinationsausschuss des Euro-Atlantischen Partnerschaftsrates (EAPC) und der Partnerschaft für den Frieden (PfP) hat entschieden, die bilaterale Zusammenarbeit zwischen der NATO und den „nicht-NATO Partner im Bereich Cyber-Sicherheit zu stärken. Deshalb hat eine interdepartementale Delegation unter Federführung des EDA im November 2013 eine Konsultation mit dem Kompetenzzentrum eingeleitet, um die Möglichkeiten einer Zusammenarbeit im zivilen Bereich zu diskutieren.

### 4.5.6 Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit (M11)

**Zuständigkeiten: UVEK-BAKOM;** KS NCS, Fachbehörden, EDA-PD, EFD-MELANI

Um vor Cyber-Risiken zu schützen, sind Sicherheitsstandards für Produkte und Prozesse notwendig. Die globale Vernetzung bedingt, dass die Erarbeitung dieser Standards auf internationaler Ebene erfolgt und die darauf basierende Regulierung multilateral beschlossen und durchgesetzt wird. Die NCS verfolgt mit der M11 das Ziel, dass die Interessen des Wirtschaftsstandortes Schweiz koordiniert in die internationalen privaten und staatlichen Gremien im Bereich Sicherheit, Sicherung und Standardisierung eingebracht werden. Dazu ist ein Prozess zu etablieren, der den Informationsaustausch zwischen den kritischen Infrastruktur-Betreibern, IKT-Leistungserbringern, Systemlieferanten, Verbänden, nationalen Standardisierungsorganisationen, Fachbehörden und Regulatoren stärkt.

Aktueller Stand:

An der ersten Sitzung des Steuerungsausschusses NCS vom 30. Oktober 2013 wurde neu dem BAKOM auf dessen Antrag die Federführung dieser Massnahme übertragen.

### 4.5.7 Handlungsbedarf rechtliche Grundlagen (M16)

**Zuständigkeiten: KS NCS**

Mit der zunehmenden Vernetzung und dem Einsatz von Kommunikationsmitteln kann man eine zunehmende Cyber-Ausprägung bestehender Aufgaben und Verantwortlichkeiten beobachten. Diese schlagen sich in den jeweiligen Gesetzen und Verordnungen nieder. Diese Regelungen sind aber oft nicht auf einander abgestimmt und zum Teil lückenhaft. Obwohl der Bund und die Kantone über die Kompetenzen verfügen, Auflagen in Bezug auf die Sicherheit zu erlassen, sind diese Bestimmungen bezüglich Cyber-Security oft noch zu wenig explizit ausformuliert.

Die M16 sieht vor, dass die Rechtsgrundlagen überprüft und die Cyber-Ausprägung angepasst werden. Im Rahmen der NCS geht es darum, dass die Verwaltungseinheiten für ihr Aufgabengebiet die für den Umgang mit Cyber-Risiken relevanten Rechtsgrundlagen erheben und den Revisions- bzw. Ergänzungsbedarf evaluieren.

Aktueller Stand:

Die Koordinationsstelle NCS hat mit allen zuständigen Departementen eine Übersicht der relevanten Rechtsgrundlagen in Bereichen mit Cyber-Ausprägung erhoben und erfasst, ob ein Revisionsbedarf besteht.

Erwähnenswerte aktuelle Gesetzgebungsprojekte respektive Gesetzesrevisionen sind insbesondere das Informationsschutzgesetz (ISG), das Nachrichtendienstgesetz (NDG), das Landesversorgunggesetz (LVG) und das Stromversorgungsgesetz (StromV).

Das ISG wird die Informationssicherheit einheitlich und integral für den ganzen Bund (nicht nur die Bundesverwaltung) regeln und fasst wichtige gesetzliche Grundlagen betreffend die Informationssicherheit zusammen: Es wird die Informationsschutzverordnung (ISchV), die Geheimschutzverordnung des VBS und die Verordnung über die Personensicherheitsprüfungen (PSPV) ersetzen und die Belange der Informatiksicherheit (z.B. die Meldepflicht innerhalb der Bundesverwaltung) aus der Bundesinformatikverordnung (BinfV, Art. 11) aufnehmen.

Das ISG hält zudem den MELANI-Auftrag (Unterstützung der Betreiber kritischer Infrastrukturen im Bereich der Informationssicherheit durch den Bund) fest und schafft eine formellgesetzliche Rechtsgrundlage für die Datenbearbeitung in diesem Zusammenhang. Zum Entwurf des ISG wird Ende März 2014 die Vernehmlassung eröffnet.

## 4.6 Umsetzungsaktivitäten der Kantone

Der Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) ist die Schnittstelle der NCS zu den Kantonen. Die Koordinationsstelle NCS ist Mitglied der Fachgruppe Cyber des KKM SVS und bildet auf Stufe Bund die Brücke mit den Projektarbeiten der Fachgruppe Cyber, um Synergien optimal zu nutzen und Redundanzen zu vermeiden. Die Politische Plattform SVS mandatierte am 20. August 2013 die Fachgruppe Cyber mit der Steuerung von Teilprojekten, die in vier Arbeitsgruppen (AG) aufgeteilt wurden.

Aktueller Stand:

Es wurden vier Arbeitsgruppen in den Bereichen Risikoanalyse und Prävention (M2 der NCS), Incident Management (M4, M5 der NCS), Krisenmanagement (M15 der NCS) und Übersicht Straffälle (M6 der NCS) gebildet. Die konstituierenden Sitzungen der vier Arbeitsgruppen stehen kurz bevor. Die konstituierende Sitzung der Fachgruppe Cyber hat stattgefunden. In ihr sind Bund und Kantone paritätisch vertreten, zusätzlich entsendet der Gemeinde- und Städteverband einen Vertreter.

Die erste Cyber-Landsgemeinde, zu welcher die Kantone ihre Vertreter aus den Bereichen Informatik- und Informationssicherheit sowie Krisenorganisation entsenden konnten hat im März 2013 Stattgefunden. Die zweite Cyber-Landsgemeinde findet am 20. März 2014 statt.

## 4.7 Umsetzungsaktivitäten der Armee

Die Armee stellt auch eine der kritischen Infrastrukturen des Landes dar. Als solche muss sie die neue Dimension der Cyber-Bedrohungen ebenfalls berücksichtigen, um ihre Funktion als strategische Sicherheitsreserve des Bundes in allen Lagen erfüllen zu können. Gleichzeitig ergeben sich mit dem Cyber-Raum auch neue operationelle Optionen, welche in den militärischen Operationen berücksichtigt werden müssen. Die Armee hat in erster Linie die Aufgabe in ihrem Bereich die Fähigkeiten auszubauen.

Obwohl die NCS (s. Kapitel 3.4) den Kriegs- und Konfliktfall ausklammert und der Armee den Auftrag gibt, sich für Spezialfälle vorzubereiten, verfügt die Armee aufgrund der obengenannten Bedürfnisse über wesentliches Wissen und Fähigkeiten, welche von den verantwortlichen Ämtern bei Bedarf und wenn sie nicht von der Armee selber gebraucht werden, in ihren Umsetzungsprozessen abgerufen werden sollen. Dies entspricht dem bewährten Ansatz der Subsidiarität des Einsatzes der Armee.

Aktueller Stand:

Die Armeeführung hat die Prinzipien der vom Chef der Armee (CdA) am 03.04.2013 veranlassten Konzeptionsstudie Cyber-Defense (KS CYD) gutgeheissen. Die sich in der Umsetzung befindende KS CYD stellt im Wesentlichen die Abwehrfähigkeit und die Weiterentwicklung der Cyber-Operationsfähigkeiten der Armee und deren Mittel, Rollen sowie Kompetenzen dar. Ihre strategischen Hauptziele umfassen die Sicherstellung der dauernden Handlungsfreiheit und –fähigkeit der Armee sowie die Fähigkeit der Armee, mit ihren Partnern zusammenzuarbeiten und wo nötig diese zu unterstützen.

Das weitere Vorgehen sieht nun auch vor, die Arbeit mit der Koordinationsstelle NCS sicherzustellen und die Elemente des Umsetzungsplanes NCS (gem. Ziffer 3.3 im Umsetzungsplan: Subsidiarität der Armee) des Bundesrates zu konkretisieren. Insbesondere geht es darum, die spezifischen Kompetenzen der Armee zu Gunsten der zivilen Behörden und der Betreiber kritischen Infrastrukturen einzubringen, sowie ihre Verantwortung im Konflikt- und Kriegsfall zu präzisieren.

# 5 Umsetzungsorganisation

Der Bundesrat hat einen Steuerungsausschuss NCS eingesetzt, um die koordinierte, zielgerichtete Umsetzung der NCS sicherzustellen. Die konstituierende Sitzung des Steuerungsausschusses NCS hat am 30. Oktober 2013 stattgefunden.

Im Steuerungsausschuss vertreten sind alle Bundesstellen mit federführender Verantwortung für zumindest eine der Umsetzungs-Massnahmen. Die Koordinationsstelle NCS, die die Umsetzung der Strategie auf operationeller und fachlicher Ebene koordiniert, sowie der Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS)[12], der die Arbeiten mit Schnittstellen zu den Kantonen koordiniert, sind ebenfalls im Steuerungsausschuss vertreten. Den Vorsitz des Steuerungsausschusses NCS führt das EFD.

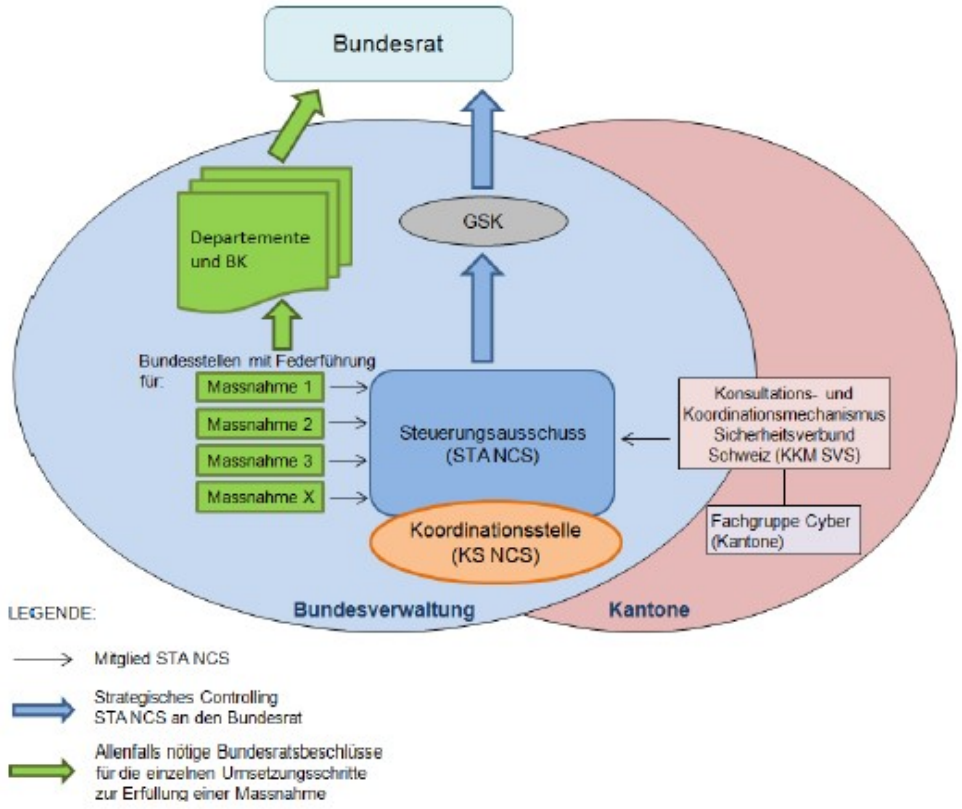



Abbildung 3: Umsetzungsorganisation NCS

Weiter wurde am 25. Oktober 2013 eine interdepartementale Fachgruppe Cyber-International (FG-CI) unter Federführung der Abteilung Sicherheitspolitik des EDA konstituiert. Das Ziel der FG-CI ist es, den Informationsfluss in enger Kooperation/Koordination zwischen allen Beteiligten sicher zu stellen. Da die cyberspezifischen Arbeiten innerhalb der Bundesverwaltung oftmals Schnittstellen zueinander haben und eine internationale Ausstrahlung aufweisen, geht es bei dieser Fachgruppe insbesondere darum, sich einen Überblick über die jeweiligen Aktivitäten zu verschaffen.

[12] Vgl. Kapitel 4.6

## 5.1 Mandat des Steuerungsausschusses NCS

Am 15. Mai 2013 hat der Bundesrat das Mandat des Steuerungsausschusses NCS verabschiedet und diesem damit den Auftrag erteilt, die koordinierte und zielgerichtete Umsetzung der NCS sicherzustellen. Dazu überprüft der STA NCS durch ein Strategisches Controlling regelmässig die Umsetzungsfortschritte der NCS und rapportiert diese via die Generalsekretärenkonferenz (GSK) an den Bundesrat.

Des weiteren sorgt der STA NCS für ein koordiniertes Vorgehen der zuständigen Departemente bei der Umsetzung der Massnahmen, insbesondere wenn dies den Rechtsetzungsbereich tangiert. Er unterstützt aktiv die Zusammenarbeit der Bundesstellen mit den relevanten Stellen aus Kantonen, Wirtschaft und Zivilgesellschaft. Er erstattet dem Bundesrat via Eidgenössisches Finanzdepartement (EFD) jährlich Bericht zum Stand der Strategieumsetzung, Ende 2017 in Form eines umfassenden Schlussberichts. Im Frühjahr 2017 wird er dem Bundesrat eine Wirksamkeitsüberprüfung der Strategie und ihres Umsetzungsplanes vorlegen.

Die Koordinationsstelle NCS koordiniert die Umsetzung der Strategie auf operationeller und fachlicher Ebene, unter Berücksichtigung der Risikopolitik des Bundes, der Nationalen Strategie zum Schutz kritischer Infrastrukturen und Risikomanagement Bund sowie der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz und verfolgt in Absprache mit dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) international die Entwicklungen in Sachen Cyber-Strategien. An einer jährlich durchgeführten Expertenveranstaltung NCS werden die Umsetzungspartner national vernetzt, informiert und erhalten die Gelegenheit sich austauschen.

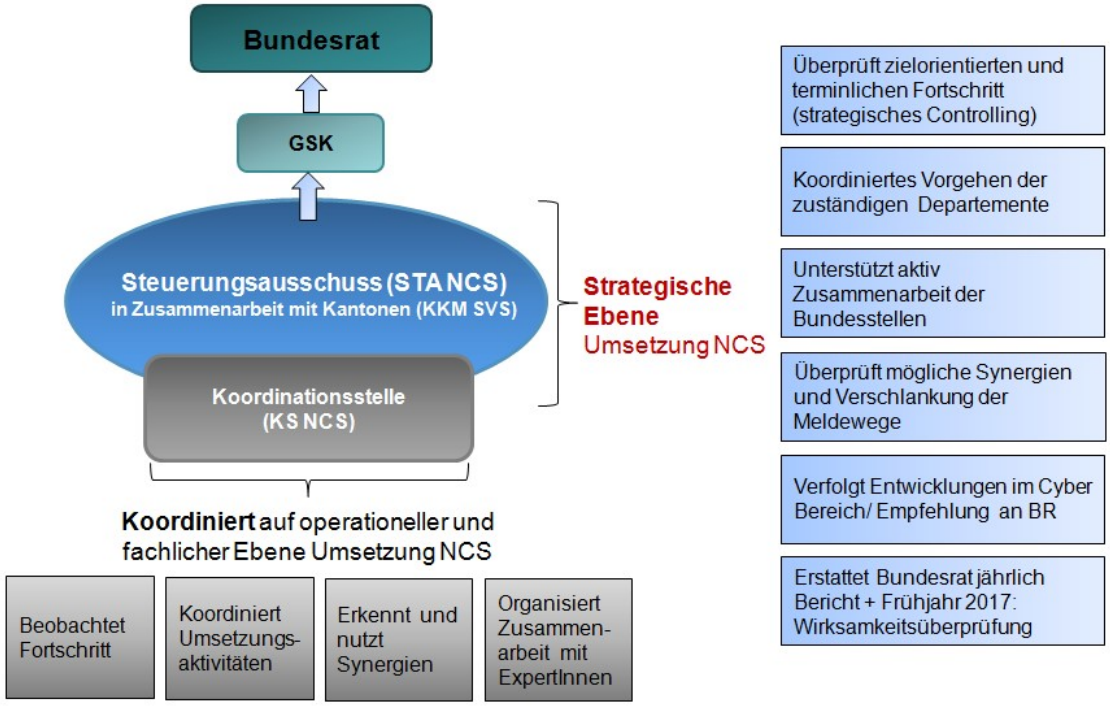



Abbildung 4: Aufgaben Steuerungsausschuss und Koordinationsstelle NCS

## 5.2 Einbezug der Wirtschaft

Der dezentrale Ansatz der Umsetzung und die enge Zusammenarbeit zwischen Bund, Kantonen und Wirtschaft sind Kernelemente der NCS. Obwohl der Einbezug der Wirtschaft auf fachlicher Ebene erfolgt ist und die 28 Teilsektoren und die KI-Betreiber via BABS und BWL direkt angesprochen werden, fehlte bisher der Einbezug der politischen Ebene der Wirtschaft in die Umsetzung NCS. Der STA NCS hat deshalb 2013 nach geeigneten Formen gesucht. 2014 wird diese Situation dadurch verbessert, dass der Dachverband economiesuisse als beobachtendes Mitglied im STA NCS aufgenommen wird, wo er auch eine Vermittlerfunktion zu den Branchen ausüben wird.

# 6 Schlussbetrachtung

Die Zeit seit der Verabschiedung des Umsetzungsplanes NCS 2013 wurde genutzt, um mit den verantwortlichen Stellen ihre NCS-Aufgaben zu konkretisieren. Die KS NCS hat die Ziele und Meilensteine mit ihnen erarbeitet und diese in einem Grundlagedokument erfasst. Gemäss Plan haben alle verantwortlichen Stellen für ihre Massnahmen, die Umsetzungsarbeiten gestartet. Einige Meilensteine wurden schon Ende 2013 erreicht und zahlreiche andere Meilensteine sind gemäss Planung bis Mitte 2014 vorgesehen. Bei den meisten Massnahmen erfolgt die Umsetzung nicht durch eine Bundesstelle alleine, sondern in Zusammenarbeit mit mehreren Umsetzungspartnern. Im Verlauf von 2013 haben sich die Verantwortlichen Ämter gefunden und die Zusammenarbeit aufgenommen. Damit wurde eine stabile Basis für die kommenden Umsetzungsarbeiten geschaffen.

Durch die Gründung der Fachgruppe Cyber des SVS (FG-C) und die Fachgruppe Cyber-International des EDA (FG-CI) besteht auch eine gute Zusammenarbeit mit den Kantonen und auf internationaler Ebene. Die Arbeiten haben bereits begonnen: Die FG-C koordiniert die NCS-Umsetzung auf Stufe Kantone und bildet die Schnittstelle zwischen Bund und Kantonen. Durch das interdepartementale Gremium der Fachgruppe Cyber-International konnte auch die Förderung und Systematisierung des Informationsflusses erreicht werden und das Themenfeld «Cyber-Sicherheit International» von diversen Stellen aus verschiedenen Blickwinkeln innerhalb der Bundesverwaltung behandelt werden.

Es ist wichtig festzuhalten, dass bei vielen der NCS Massnahmen bereits vor der Verabschiedung der NCS Arbeiten und Prozesse im Gange waren. Mit der NCS wurde der Auftrag dieser Stellen erweitert oder neu gewichtet, so auch von MELANI und dem NDB. Hier ist im Rahmen der NCS ein gesamtheitliches und koordiniertes Vorgehen in enger Zusammenarbeit mit den involvierten Stellen notwendig.

Die Strategie hat einen Umsetzungsprozess ausgelöst, der einerseits bereits 2014 und 2015 auf der operativen Ebene erste Wirkungen erzielen wird und andererseits auch nach 2017 nicht abgeschlossen ist. Denn die aus der NCS hervorgehenden Aktivitäten zum Schutz vor Cyber-Risiken müssen periodisch überprüft und der sich verändernden Gefährdungslandschaft angepasst werden.

Im Frühjahr 2017 wird dem Bundesrat ein umfassender Schlussbericht mit Wirksamkeitsüberprüfung der Strategie und des Umsetzungsplanes vorgelegt. Anschliessend wird über das weiter Vorgehen informiert.

# 7 Anhänge

## 7.1 Grundlagendokumente NCS

«Nationale Strategie zum Schutz der Schweiz gegen Cyber Risiken (NCS)»:
http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de

«Umsetzungsplan Nationale Strategie zum Schutz der Schweiz gegen Cyber Risiken (UP NCS)»:
http://www.isb.admin.ch/themen/01709/01711/index.html?lang=de

«Mandat Steuerungsausschuss NCS und Koordinationsstelle NCS»
http://www.isb.admin.ch/themen/01709/01712/index.html?lang=de

«Roadmap NCS»
http://www.isb.admin.ch/themen/01709/01841/index.html?lang=de

## 7.2 Zusammenstellung der Parlamentarischen Vorstösse zu Cyber-Risiken

| **Vorstoss**<br>Ip. = Interpellation; Mo. = Motion; Po. = Postulat | Eingereicht am: | Stand per 31.12.2013: |
|---|---|---|
| 08.3050 Po Schmid-Federer. Schutz vor Cyberbulling | 11.03.2008 | überwiesen |
| 08.3100 Mo. Burkhalter. Nationale Strategie für die Bekämpfung der Internetkriminalität mit Verhandlungen des Ständerates vom 2. Juni 2008 (AB S 2.06.2008), Bericht der SiK-N vom 11. November 2008 sowie Verhandlungen des Nationalrates vom 3. Juni 2009 (AB N 3.06.2009) | 18.03.2008 | erledigt |
| 08.3101 Po. Frick. Die Schweiz wirksamer gegen Cybercrime schützen | 18.03.2008 | erledigt |
| 08.3924 Ip. Graber. Massnahmen gegen den elektronischen Krieg | 18.12.2008 | erledigt |
| 09.3114 Ip. Schlüer. Internet-Sicherheit | 17.03.2009 | erledigt |
| 09.3266 Mo. Büchler. Sicherheit des Wirtschaftsstandorts Schweiz | 20.03.2009 | überwiesen |
| 09.3628 Po Fehr HJ. Bericht über das Internet in der Schweiz | 12.06.2009 | erledigt |
| 09.3630 Ip. Fehr HJ. Fragen rund ums Internet | 12.06.2009 | erledigt |
| 09.3642 Mo. Fehr HJ. Internet-Observatorium | 12.06.2009 | erledigt |
| 10.3136 Po. Recordon. Analyse der Bedrohung durch Cyberwar | 16.03.2010 | erledigt |
| 10.3541 Mo. Büchler Schutz vor Cyber-Angriffen | 18.06.2010 | erledigt |
| 10.3625 Mo. SiK-N. Massnahmen gegen Cyberwar; mit Verhandlungen des Nationalrates vom 2. Dezember 2010 (AB N 2.12.2010), Bericht der SiK-S vom 11. Januar 2011 sowie Verhandlungen des Ständerates vom 15. März 2011 (AB S 15.03.2011) | 29.06.2010 | überwiesen |
| 10.3872 Ip. Recordon. Risiko eines grossflächigen Stromausfalls in der Schweiz | 01.10.2010 | erledigt |

| | | |
|---|---|---|
| 10.3910 Po. FDP-Liberale Fraktion. Leit- und Koordinationsstelle im Bereich der Cyber-Bedrohung | 02.12.2010 | erledigt |
| 10.4020 Mo. Glanzmann. MELANI für alle | 16.12.2010 | erledigt |
| 10.4028 Ip. Malama. Gefahr eines Virus-Angriffs auf Schweizer Kernkraftwerke | 16.12.2010 | erledigt |
| 10.4038 Po. Büchler. Ergänzung des sicherheitspolitischen Berichtes um ein Kapitel zu Cyberwar | 16.12.2010 | erledigt |
| 10.4102 Po. Darbellay. Konzept zum Schutz der digitalen Infrastruktur der Schweiz | 17.12.2010 | erledigt |
| 11.3906 Po. Schmid-Federer. IKT-Grundlagengesetz | 29.09.2011 | überwiesen |
| 12.3417 Mo. Hodgers. Öffnung der Telekommunikationsmärkte. Strategien für die nationale digitale Sicherheit | 30.05.2012 | erledigt |
| 13.3228 Ip Recordon. Abhöreinrichtungen und allgemeine Mängel der Informatik- und Telekommunikationseinrichtungen des Bundes | 22.03.2013 | erledigt |
| 13.3229 Ip Recordon. Cyberkrieg und Cyberkriminalität. Wie gross sind die Bedrohungen, und mit welchen Massnahmen können sie bekämpft werden? | 22.03.2013 | erledigt |
| 13.3558 Ip. Eichenberger. Cyberspionage: Einschätzung und Strategie | 20.06.2013 | erledigt |
| 13.3692 Ip. Hurter. Telekommunikationsmarkt. Sind aktuelle Gesetzgebung und Regulierungsmassnahmen noch zeitgemäss? | 12.09.2013 | im Plenum noch nicht behandelt |
| 13.3696 Mo. Müller-Altermatt. Echter Datenschutz statt Schutzschild für Steuerpreller | 12.09.2013 | im Plenum noch nicht behandelt |
| 13.3707 Po. Fraktion BD. Ganzheitliche und zukunftstaugliche Cyberraumstrategie | 17.09.2013 | im Plenum noch nicht behandelt |
| 13.3773 Ip. FDP-Liberale Fraktion. Zukunftstaugliches Fernmeldegesetz. Für eine übergreifende Cyberraum-Strategie | 24.09.2013 | im Plenum noch nicht behandelt |
| 13.3841 Mo. Rechsteiner. Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit | 26.09.2013 | Motion an 2. Rat |
| 13.4009 Mo. SiK-N. Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken („Der Bundesrat wird beauftragt, die Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken voranzutreiben und die 16 konkrete Massnahmen bis Ende 2016 umzusetzen.“) | 05.11.2013 | im Plenum noch nicht behandelt |
| 13.4077 Ip. Clottu. Datenspionage und Internetsicherheit | 05.12.2013 | im Plenum noch nicht behandelt |
| 13.4086 Mo. Glättli. Nationales Forschungsprogramm Alltagstauglicher Datenschutz in der Informationsgesellschaft | 05.12.2013 | im Plenum noch nicht behandelt |

# 7.3 Abkürzungsverzeichnis

| | |
|---|---|
| ASP | Abteilung Sicherheitspolitik |
| BABS | Bundesamt für Bevölkerungsschutz |
| BAKOM | Bundesamt für Kommunikation |
| BAKOM-IR | Bundesamt für Kommunikation - Dienst Internationales |
| BFE | Bundesamt für Energie |
| BIT | Bundesamt für Informatik und Telekommunikation |
| BK | Bundeskanzlei |
| BSV | Bundesamt für Sozialversicherungen |
| BWL | Bundesamt für wirtschaftliche Landesversorgung |
| CdA | Chef der Armee |
| CERT | Computer Emergency Response Team |
| CNE | Computer Network Exploitation |
| CSIRT | Computer Security Incident Response Team |
| EAPC | Euro-Atlantischen Partnerschaftsrates |
| EDA | Eidgenössisches Departement für auswärtige Angelegenheiten |
| EDA-AIO | Eidgenössisches Departement für auswärtige Angelegenheiten - Abteilung internationale Organisationen |
| EDI | Eidgenössisches Departement des Innern |
| EFD | Eidgenössisches Finanzdepartement |
| EJPD | Eidgenössisches Justiz- und Polizeidepartement |
| Fedpol | Bundesamt für Polizei |
| FG-C | Fachgruppe Cyber |
| FG-CI | Fachgruppe Cyber International |
| FUB | Führungsunterstützungsbasis der Armee |
| FUB ZEO | Führungsunterstützungsbasis der Armee Zentrum elektronische Operationen |
| GCHQ | Government Communications Headquarters |
| GSK | Generalsekretärenkonferenz |
| GS-VBS | Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport |
| ICANN | Internet Cooperation for Assigned Names and Numbers |
| IGF | Internet Governance Forum |
| IKT | Information, Kommunikation, Technology |
| ISB | Informatiksteuerungsorgan des Bundes |
| ISB-SEC | Informatiksteuerungsorgan des Bundes Sicherheit |
| KKJPD | Konferenz der Kantonalen Justiz- und Polizei Direktoren |
| KKM SVS | Koordinationsmechanismus Sicherheitsverbund Schweiz |
| KKPKS | Konferenz der Kantonalen Polizeikommandanten der Schweiz |
| KOBIK | Koordinationsstelle zur Bekämpfung Internetkriminalität |
| KS CYD | Konzeptionsstudie Cyber Defence |
| KS NCS | Koordinationsstelle Nationale Cyber Strategie |
| KTI | Kommission für Technologie und Innovation |
| MELANI | Melde- und Analysestelle Informationssicherung |
| MELANI OIC | Melde- und Analysestelle Informationssicherung Operation Information Center |
| MilCERT | Militärische Computer Emergency Response Team |
| MND | Militärischer Nachrichtendienst |
| NDB | Nachrichtendienst |
| NDG | Nachrichtendienstgesetz |
| NSA | National Security Agency |
| OSZE | Organisation für Sicherheit und Zusammenarbeit in Europa |
| SBFI | Staatssekretariat für Bildung, Forschung und Innovation |
| SKI-Strategie | Schutz Kritischer Infrastrukturen Strategie |
| STA NCS | Steuerungsausschuss Nationale Cyber Strategie |

| | |
|---|---|
| UVEK | Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation |
| V | Verteidigung |
| VBM | Vertrauensbildenden Massnahmen |
| VBS | Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport |
| VBS-SIPOL | Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport - Sicherheitspolitik |
| WBF | Eidgenössisches Departement für Wirtschaft, Bildung und Forschung |
| WL | Wirtschaftliche Landesversorgung |
| WSIS | World Summit on the Information Society |