.

Jahresbericht 2015

Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Publikation: Mai 2016

Redaktion: Koordinationsstelle NCS

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Schwarztorstrasse 59
CH-3003 Bern

Tel +41 (0)58 462 45 38
E-Mail: info@isb.admin.ch

Jahresbericht NCS unter: www.isb.admin.ch

Inhaltsverzeichnis

Vorwort **4**

1 Management Summary **5**

2 Aktivitäten **7**

2.1 Nationale Ebene **7**
2.2 Internationale Ebene **7**

3 Stand der Umsetzungsarbeiten NCS 2015 ..... **8**

3.1 Prävention **10**
3.1.1 Massnahme 2: Risiko- und Verwundbarkeitsanalyse 10
3.1.2 Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept 10
3.1.3 Massnahme 4: Erstellung Lagebild und Lageentwicklung 11

3.2 Reaktion **11**
3.2.1 Massnahme 5: Vorfall-Analyse und Nachbearbeitung von Vorfällen 11
3.2.2 Massnahme 6:Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe 12
3.2.3 Massnahme 14: Aktive Massnahmen und Identifikation der Täterschaft 13

3.3 Kontinuitäts- und Krisenmanagement **13**
3.3.1 Massnahme 12: Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren 13
3.3.2 Massnahme 13: Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise 14
3.3.3 Massnahme 15: Konzept Führungsabläufe und -prozesse mit Cyber-Ausprägung. 15

3.4 Unterstützende Prozesse **15**
3.4.1 Massnahme 1: Identifikation von Cyber-Risiken durch Forschung 15
3.4.2 Massnahme 7: Übersicht Kompetenzbildungsangebote 16
3.4.3 Massnahme 8: Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken 16
3.4.4 Massnahme 9: Internet Governance 17
3.4.5 Massnahme 10: Internationale Kooperation Cyber-Sicherheit 18
3.4.6 Massnahme 11: Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit 18
3.4.7 Massnahme 16: Handlungsbedarf rechtliche Grundlagen 19

3.5 Umsetzungsaktivitäten der Armee **19**
3.6 Umsetzungsaktivitäten Kantone **20**

4 Strategisches Controlling **20**

5 Wirksamkeitsüberprüfung **20**

6 Schlussbetrachtung **21**

7 Anhänge **22**

7.1 Grundlagendokumente NCS **22**
7.2 Zusammenstellung der Parlamentarischen Vorstösse zu Cyber-Risiken **22**
7.3 Abkürzungsverzeichnis **24**

Vorwort

Die digitale Welt wird immer wichtiger, schneller und komplexer. Die Chancen, die sich aus der Digitalisierung für die Schweiz ergeben, gilt es früh zu erkennen und entschlossen zu nutzen. Dabei dürfen aber die Risiken nicht vergessen werden. Auch im Jahr 2015 haben uns verschiedene Ereignisse gezeigt, dass diese Risiken sehr ernst zu nehmen sind. Spionageangriffe, neue Arten von Malware, Datenabflüsse und Erpressungen mit DDos-Angriffen machten deutlich, wie verletzlich der digitale Motor der Wirtschaft und Gesellschaft ist. Besonders eindrückliche Beispiele waren die Spionageangriffe auf den Deutschen Bundestag und auf die Verhandlungen zum Atom-Abkommen mit dem Iran in Genf.

Angesichts solcher Vorkommnisse stellt sich natürlich die Frage, ob wir in der Schweiz genug unternehmen, um uns vor Cyber-Risiken zu schützen. Eine einfache Antwort darauf gibt es nicht. Es liegt in der Natur der sich schnell verändernden Cyber-Risiken, dass wir stets mit neuen Szenarien konfrontiert sind und unsere Schutzmassnahmen laufend überprüfen und anpassen müssen. Wir müssen auch mehr als zuvor die nationale und internationale Kooperation stärken. Mit Bestimmtheit können wir jedoch sagen, dass die Schweiz nicht untätig geblieben ist. Der Bundesrat hat 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» beschlossen und ein Jahr später den Umsetzungsplan dazu verabschiedet. Als strategische Ziele der NCS definierte der Bundesrat die frühe und genaue Erkennung der Cyber-Risiken, deren effektive Reduktion und die Erhöhung der Widerstandsfähigkeit der Schweiz gegenüber diesen Risiken.

Der vorliegende Jahresbericht 2015 soll Ihnen einen Überblick zum Stand der Arbeiten im dritten Jahr der NCS-Umsetzung geben. In allen Bereichen wurden wichtige Fortschritte erzielt. Besonders hervorheben möchte ich die Stärkung der Kooperation zwischen allen Beteiligten. Nur in vertrauensvoller Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Gesellschaft wird es gelingen, die Schweiz besser vor Cyber-Risiken zu schützen. Es ist bereits jetzt als Erfolg der NCS zu werten, dass sich diese Zusammenarbeit stark intensiviert hat. Dank der NCS sind die Verantwortlichkeiten definiert und es ist sichergestellt, dass alle Akteure am gleichen Strick ziehen.

Neben dem Rückblick auf das Erreichte, soll hier auch ein kurzer Ausblick auf das Kommende erlaubt sein. Wir werden die Umsetzung der Strategie auch 2016 auf Hochtouren weitertreiben. Zudem beginnen bereits die Arbeiten zur Weiterentwicklung der NCS. Die aktuelle Strategie ist bis Ende 2017 gültig. Wir werden darum im nächsten Jahr in einer Evaluation prüfen, welche Stärken und Schwächen die NCS aufweist, so dass wir dem Bundesrat im Jahr 2017 einen Vorschlag über das weitere Vorgehen unterbreiten können.

Nun wünsche ich Ihnen eine gute Lektüre mit dem Jahresbericht und freue mich auf die weitere Zusammenarbeit mit allen Partnern, so dass wir möglichst alle von der Digitalisierung profitieren können, ohne dass wir dabei Einbussen bei der Sicherheit in Kauf nehmen müssen.

Peter Fischer
Delegierter für die Informatiksteuerung des Bundes (ISB)

1 Management Summary

Der Bundesrat hat am 27. Juni 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» und am 15. Mai 2013 deren Umsetzungsplan verabschiedet. Die NCS mit ihren 16 Massnahmen fokussiert auf die frühzeitige Erkennung vor Cyber-Risiken, die Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen und die Reduktion der Cyber-Bedrohungen, insbesondere der Cyber-Spionage, der Cyber-Sabotage und der Cyber-Kriminalität.

Die Umsetzung der NCS ist dezentral organisiert. Für jede der 16 Massnahmen ist jeweils einem Bundesamt die Federführung zur Umsetzung übertragen worden. Um diese Umsetzungsarbeiten zu koordinieren, hat der Bundesrat die Koordinationsstelle (KS NCS) eingesetzt, welche bei der Melde- und Analysestelle Informationssicherung (MELANI) im Informatiksteuerungsorgan des Bundes (ISB) angesiedelt ist. Die Gesamtverantwortung trägt der Steuerungsausschuss (STA NCS), welcher beauftragt ist, die Umsetzung mit einem strategischen Controlling zu begleiten.

Die 16 Massnahmen betreffen vier Bereiche: Prävention, Reaktion, Kontinuität und unterstützende Prozesse. In allen Bereichen konnten in den vergangenen Jahren, nicht zuletzt dank der engen Zusammenarbeit und guten Kommunikation aller Beteiligten, wichtige Ziele erreicht werden.

Bei der Prävention haben das Bundesamt für Bevölkerungsschutz (BABS) und das Bundesamt für Wirtschaftliche Landesversorgung (BWL) in bisher zehn kritischen Teilsektoren Risiko- und Verwundbarkeitsanalysen durchgeführt (Erdgasversorgung; Strassenverkehr; Stromversorgung; Luftverkehr; Lebensmittelversorgung; Ärztliche Betreuung und Spitäler; Banken; Labors; Medien; Zivilschutz). Um Risiken zu erkennen, braucht es neben den Kenntnissen über die Verwundbarkeiten auch eine gute Einschätzung der aktuellen Bedrohungslage. Zu diesem Zweck entwickelte MELANI einen interaktiven Lageradar, der die verschiedenen Cyber-Bedrohungen gegen die Infrastrukturen der Schweiz visualisiert und die Relevanz der Bedrohungen aufzeigt. Eine Übersicht der wichtigsten Cyber-Bedrohungen in 2015 liefern der MELANI Halbjahresbericht und der Jahresbericht fedpol (Veröffentlichung Ende Mai 2016).

Im Bereich Reaktion wurden auch im Jahr 2015 die Fachkompetenzzentren zur Analyse von Schadsoftware (z. B. GovCERT.ch, CISIRT-BIT, milCERT-VBS) weiter ausgebaut und zahlreiche Produkte entwickelt. GovCERT hat für den Austausch von technischen Informationen mehrere Plattformen aufgebaut und in Betrieb genommen. Diese dienen dazu, Malware nachzuverfolgen sowie einfach und effizient über längere Zeiträume nach dem Nachweis der Manipulation (sogenannte Indicators of Compromise) von Computersystemen und Netzwerken zu suchen. So können betroffene Firmen und Organisationen rasch informiert und geschützt werden. Zur Reaktion gehört auch die Identifikation der Täterschaft. In diesem Bereich konnte die Fachabteilung Cyber des Nachrichtendienstes des Bundes (NDB) Spezialwissen und Fähigkeiten aufbauen, die es ihm erlauben, die Ziele, Methoden und Akteure eines Angriffs zu analysieren und so mögliche Täter zu identifizieren.

Bei der Kontinuität wurde bei den beiden kritischen Teilsektoren Erdgasversorgung und Medien aufbauend auf der Risiko- und Verwundbarkeitsanalyse ein erster Entwurf der verschiedenen Massnahmen zur Verbesserung der Resilienz erarbeitet. Für die anderen relevanten Teilsektoren sind die Massnahmenberichte gemäss Planung in Erarbeitung.

Im Bereich der unterstützenden Prozesse stehen die Bereiche Forschung und Bildung sowie die internationale Zusammenarbeit im Vordergrund. Das Staatssekretariat für Forschung, Bildung und Innovation (SBFI) hat einen interdepartementalen Steuerungsausschuss eingesetzt, welcher alle Aktivitäten im Bereich Forschung und Bildung zu Cyber-Risiken auf nationaler Ebene koordiniert und vorantreibt.

Die internationale Zusammenarbeit wurde auf bilateraler und multilateraler Ebene unter der Führung der Abteilung für Sicherheitspolitik (ASP) des Eidgenössischen Departementes des

Äussern (EDA) und des Bundesamtes für Kommunikation (BAKOM) weiter gestärkt und ausgebaut. Auf bilateraler Ebene wurden bestehende Kontakte intensiviert und weitere neue geknüpft. Auf multilateraler Ebene wurden die Arbeiten zu den vertrauensbildenden Massnahmen der OSZE weiter entwickelt.

Um zu überprüfen, wie wirksam die 16 Massnahmen sind, wird ab Januar 2016 eine Wirksamkeitsüberprüfung gestartet, die von einer externen und neutralen Stelle durchgeführt wird. Die Ergebnisse werden dem Bundesrat im Frühjahr 2017 als Basis für die Entscheide zum weiteren Vorgehen vorgelegt.

Wichtigste Cyber-Bedrohungen 2015

Das Jahr 2015 war primär geprägt von folgenden Cyber-Bedrohungen:

- **Spionage** (Duqu 2: iranische Atomgespräche wurden abgehört, Carbanak: elektronischer Banküberfall, Hacker-Angriff auf den Deutschen Bundestag),
- **Datenabflüsse** (über 21 Millionen Datensätze beim US Personalamt entwendet, Rex Mundi),
- **Angriffe auf Industrielle Kontrollsysteme** (Honeypot Wasserkraftwerk: 31 Attacken, AutoHack),
- **Einsatz von Crimeware** (E-Banking Trojaner wie Torpig, Dyre, Tinba, Gozi, Zeus),
- **DDOS-Angriffe** (TV5 Monde, Charlie Hebdo, Flüge von Polish Airlines gestrichen),
- **Erpressungen** (Cryptolocker: Cryptowall 3.0, Teslascript),
- **Defacements** (Webseitenverunstaltungen von Islamistischen Sympathisanten in Frankreich und in der Westschweiz nach Cherlie Hebdo),
- **Social Engineering und Phishing** (Angriffe auf Kantonalbanken, Kreditkartendaten).

2 Aktivitäten

In diesem Kapitel werden einige wichtige Aktivitäten und Veranstaltungen aufgelistet, die auf nationaler und internationaler Ebene abgehalten wurden.

2.1 Nationale Ebene

Vom 22.-23. April 2015 fand die «Cyber 9/12 Student Challenge» in Genf statt. Der Atlantic Council zusammen mit dem Geneva Centre for Security Policy (GCSP) waren Gastgeber dieser Veranstaltung, bei welcher sich Studierende von Universitäten aus den USA, Grossbritannien, Frankreich, Polen, Ungarn, Finnland, Estland und der Schweiz auf einen grossen Cyberangriff vorbereiten und adäquate Handlungsempfehlungen entwickeln mussten. Das Schweizer Team war Sieger des Wettbewerbs.

Am 23. April 2015 wurde die dritte «Cyber-Landsgemeinde» durchgeführt. Rund 80 Cyber-Verantwortliche von Bund und allen Kantonen sowie enge Partner des Sicherheitsverbundes Schweiz (SVS) nahmen am Vernetzungsanlass teil. Wie schon in den vergangenen Jahren standen der Umsetzungsstand der Projekte auf Kantonsebene und jener der NCS im Fokus.

Vom 19.-22. Oktober 2015 fand in Luzern der dritte «Europäische Cyber Security Challenge» statt. In diesem länderübergreifenden Wettkampf massen sich Schülerinnen und Schüler sowie Studierende aus Österreich, Deutschland, Rumänien, Grossbritannien, Spanien und der Schweiz im Auffinden, Ausnutzen und Beheben von Schwachstellen in IKT-Systemen. Gastgeber waren der Verein Swiss Cyber Storm, das EDA und das Eidgenössische Finanzdepartement (EFD).

Am 2. November 2015 wurde die zweite «NCS-Tagung» durchgeführt. Ziel der NCS-Tagung war es, Vertretern aus Wirtschaft und Politik einen detaillierten Überblick über den Umsetzungsstand der NCS-Massnahmen zu geben und den Informationsaustausch zwischen allen relevanten Akteuren aus Verwaltung und Wirtschaft (insbesondere den Betreibern kritischer Infrastrukturen) zu fördern.

2.2 Internationale Ebene

Vom 16.-17. April 2015 fand in Den Haag die «Global Conference on Cyberspace (GCCS)» statt, die sich mit der Schaffung von staatlichen Verhaltensnormen befasste. Bundesrat Didier Burkhalter eröffnete die Konferenz und setzte sich in seiner Rede dafür ein, dass auch im Cyber-Raum ein Regelwerk angewendet wird, welches politischer und juristischer Natur ist.

Vom 29.-30. September 2015 wurde der Workshop der European Union Agency for Network and Information Security (ENISA) über die Sicherheit von kritischen Infrastrukturen in der EU und in der Schweiz durchgeführt. Die Schweiz ist als einziger Nicht-EU-Staat in dieser Arbeitsgruppe vertreten. Ziel des Anlasses war, einen Vergleich über den Schutz kritischer Infrastrukturen (Prozesse, Organisation, Akteure) in 15 EU Ländern und der Schweiz zu erstellen. Die Resultate wurden auf der ENISA Webseite veröffentlicht.

2015 beteiligte sich die Schweiz zweimal am «Sino-European Cyber Dialogue». Dabei handelt es sich um einen multilateralen Dialog zwischen europäischen Staaten und China mit dem Ziel, die jeweilige Bedrohungsauffassung besser zu verstehen und Fragestellungen zu identifizieren, deren Vertiefung von gegenseitigem Interesse sind.

Am 28.-29. Oktober 2015 fand die OSZE-Konferenz unter dem Vorsitz von Serbien und unter Beteiligung der Schweiz in Belgrad statt. Schwerpunkt bildete die Fortsetzung des Multistakeholder-Ansatzes in einem sicherheitspolitischen Kontext. Die Konferenz hat einen wertvol-

len Beitrag geleistet, Staaten bei der Entwicklung von nationalen Cyber-Strategien zu unterstützen. Zudem wurde zum ersten Mal eine «Table-Top-Übung» von DiploFoundation abgehalten, um die zwischenstaatliche Zusammenarbeit in einem multilateralen Forum zu stärken. Die Schweiz hat diese Konferenz sowohl konzeptionell wie auch finanziell massgeblich unterstützt.

2015 hat die «Fachgruppe Cyber-International» weiterhin zu einem systematischen Informationsfluss zwischen den interessierten Bundesstellen zwecks kohärenter und konsistenter aussenpolitischer Interessenwahrung beigetragen.

3 Stand der Umsetzungsarbeiten NCS 2015

Die NCS ist eine integrale Strategie, die mit ihren 16 Massnahmen (M1-M16) einen umfassenden Ansatz verfolgt, um die Schweiz vor Cyber-Bedrohungen zu schützen. Die Massnahmen gruppieren sich entsprechend ihrer zeitlichen Entfaltung und Abhängigkeiten wie folgt in die vier Bereiche:

- Prävention: M2, M3, M4
- Reaktion: M5, M6, M14
- Kontinuität: M12, M13, M15
- Unterstützende Prozesse: M1, M7, M8, M9, M10, M11, M16.

Die NCS befindet sich im dritten Jahr der Umsetzung, und die Arbeiten für die meisten Massnahmen sind weit fortgeschritten. In diesem Kapitel wird die Gesamtübersicht der Umsetzung anhand einer Roadmap aufgezeigt. In den nachfolgenden Kapiteln informiert ein kurzer Bericht der jeweiligen federführenden Stelle über den aktuellen Umsetzungsstand der einzelnen Massnahmen in den vier Bereichen.

Roadmap NCS

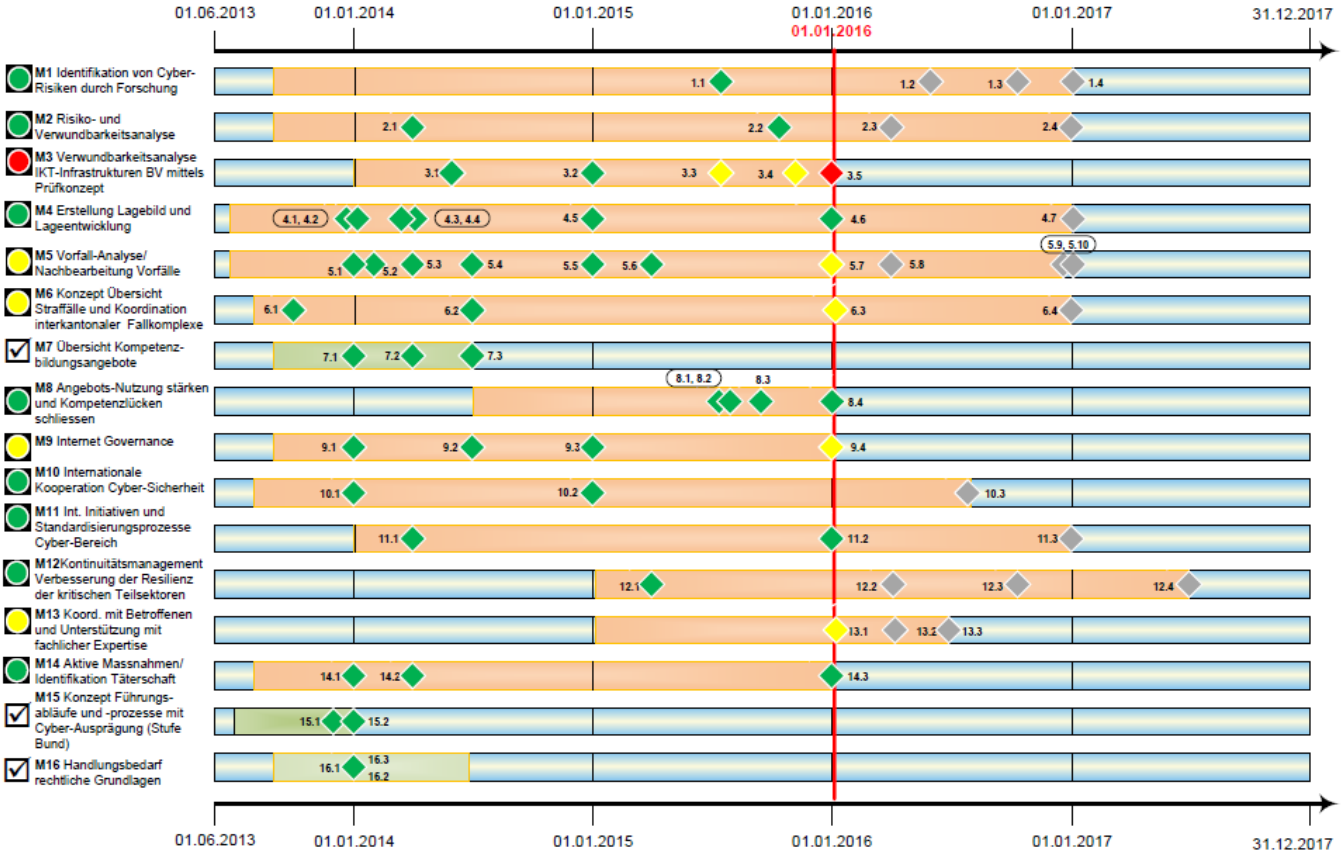

Abbildung 1: Roadmap NCS

Legende:

Meilenstein gefährdet
Meilenstein in Verzug
Meilenstein planmässig in Umsetzung

3.1 Prävention

In der Prävention sind folgende Massnahmen enthalten: Risiko- und Verwundbarkeitsanalyse (M2), Überprüfung der IKT-Verwundbarkeiten auf Stufe Bund (M3) und Lagedarstellung (M4).

3.1.1 Massnahme 2: Risiko- und Verwundbarkeitsanalyse

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

Ziel 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 Verwundbarkeiten treffen.

Das Bundesamt für wirtschaftliche Landesversorgung (BWL) und das Bundesamt für Bevölkerungsschutz (BABS) teilen sich die Arbeiten in den insgesamt 28 Teilsektoren der Schweiz und koordinieren ihr Vorgehen. Die Risiko- und Verwundbarkeitsanalysen konnten in den jeweiligen Teilsektoren weitgehend gemäss Planung abgewickelt werden. Dabei wurden zahlreiche Fachexperten aus den relevanten Unternehmen, Branchenverbänden und den zuständigen Bundesstellen beigezogen. Dadurch sind die Analysen breit abgestützt; gleichzeitig zeigt dies auch das grosse Interesse der involvierten Stellen.

Aktueller Stand

Per Januar 2016 sind die Risiko- und Verwundbarkeitsanalysen in zehn Teilsektoren abgeschlossen: Erdgasversorgung; Strassenverkehr; Stromversorgung; Luftverkehr; Lebensmittelversorgung; Ärztliche Betreuung und Spitäler; Banken; Labors; Medien; Zivilschutz. In weiteren sieben Teilsektoren werden die Analysen zurzeit durchgeführt: Parlament, Regierung, Justiz und Verwaltung; Armee; Blaulichtorganisationen; Wasserversorgung; Abwasser; Mineralölversorgung.

3.1.2 Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept

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 Verwundbarkeiten zu überprüfen. Das Informatiksteuerungsorgan des Bundes (ISB) wurde beauftragt, bis Ende 2015 ein Konzept zur periodischen Überprüfung der IKT-Infrastrukturen der Bundesverwaltung auf systemische, organisatorische und technische Schwächen zu erstellen.

Aktueller Stand:

Ein Entwurf des Prüfkonzepts zur Verwundbarkeitsanalyse der IKT-Infrastrukturen der Bundesverwaltung wurde erstellt. Dieser wurde im August dem Steuerungsausschuss (STA NCS) zur Konsultation vorgelegt. Dabei ergaben sich Differenzen. Die hauptsächliche Differenz lag darin, dass das Konzept eine Methodik zur Risikoanalyse vorschlägt. Die Massnahme 3 der Strategie bezweckt jedoch, eine Methodik zur Verwundbarkeitsanalyse darzulegen. Auch sehen verschiedene Mitglieder des STA NCS die Umsetzung einerseits mit einem grossen Aufwand verbunden und zweifeln, dass eine Umsetzung des vorgelegten Konzepts die erhoffte Wirkung erzielen kann. Der STA NCS bestimmt in der 6. Sitzung des Steuerungsausschusses NCS im Februar 2016 über das weitere Vorgehen für die Massnahme 3.

3.1.3 Massnahme 4: Erstellung Lagebild und Lageentwicklung

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

Bei der Bewältigung von Cyber-Angriffen wird ein Lagebild benötigt, welches über die Entwicklungen im Cyber-Bereich informiert und Gefahren- und Schadenspotenziale von Cyber-Angriffen für die jeweiligen kritischen Sektoren und deren Relevanz für die Schweiz beschreibt.

Um ein möglichst umfassendes Lagebild zu erstellen, sollen alle relevanten Informationen aus technischen Analysen, sowie aus nachrichtendienstlichen und polizeilichen Quellen in das Lagebild einfliessen. Um dies zu erreichen, müssen bei und zwischen den Akteuren Prozesse definiert und Verantwortlichkeiten zugeordnet werden. Zu den Akteuren zählen das Computer Emergency Response Team von MELANI im ISB (GovCERT), das Operation Information Center von MELANI im NDB (MELANI OIC), die Abteilung Cyber beim NDB und der Militärische Nachrichtendienst (MND). Ziel der NCS ist es, in enger Zusammenarbeit mit allen relevanten Akteuren ein Lagebild zu erstellen.

Aktueller Stand:

Die Prozesse zur Erstellung eines Lagebildes, der organisatorischen Abläufe, des Führungsrhythmus sowie der Verantwortlichkeiten zwischen MELANI-ISB/GovCERT, MELANI-OIC und Cyber NDB wurden erfasst. Der Cyber NDB, zuständig für die Bearbeitung von entsprechenden nachrichtendienstlich relevanten Informationen, hat zudem seine Fähigkeiten und sein Spezialwissen ausgebaut (Ziel und Methode eines Cyber-Angriffes, Bedrohungsanalyse, Täterschaftszuordnung). Um den NDB zu unterstützen, wurden ausserdem die technischen Fähigkeiten der Führungsunterstützungsbasis der Armee (FUB) eingebunden. Die Unterzeichnung eines entsprechenden Service Level Agreement (SLA) ist erfolgt. Weiter wurden Prozesse zwischen MELANI und den zuständigen Stellen des Bundesamtes für wirtschaftliche Landesversorgung (BWL) und des Bundesamtes für Bevölkerungsschutz (BABS) definiert und eingeführt. Schliesslich stehen die Anpassungen auf operativer Stufe, welche im Rahmen der Arbeiten der Massnahme 15 Krisenmanagement erforderlich wurden, kurz vor dem Abschluss, so dass die Prozesse im Bereich Krisenmanagement auf operativer Stufe im Rahmen von internationalen Übungen getestet werden können.

3.2 Reaktion

Um bei einem Vorfall möglichst rasch zu reagieren, muss eine koordinierte Vorfall-Analyse und Nachbearbeitung erfolgen. Die NCS sieht dazu einen Ausbau der Fähigkeiten und eine Steigerung der Reaktionsfähigkeit aller beteiligten Organisationen und Akteure vor. Somit ist gewährleistet, dass Vorfälle rasch analysiert werden können, die Strafverfolgung effizient handeln und eine Täterschaft schneller identifiziert werden kann. Bei der Reaktion sind folgende Massnahmen enthalten: Vorfall-Analyse und Nachbearbeitung von Vorfällen (M5), Übersicht Straffälle und Koordination interkantonaler Fallkomplexe (M6) und aktive Massnahmen und Identifikation der Täterschaft (M14).

3.2.1 Massnahme 5: Vorfall-Analyse und Nachbearbeitung von Vorfällen

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 die Vorfall-Analyse und Nachbearbeitung weiterentwickelt werden. Die verschiedenen Computer Emergency Response Teams (CERT) (GovCERT, CISIRT-BIT, milCERT-VBS) sollen ihre Fähigkeiten im Bereich Malware-Analyse ausbauen, damit

Daten bei einem Vorfall so analysiert und aufbereitet werden können, dass technische Gegenmassnahmen ergriffen werden können. Um diesen Auftrag zu erfüllen, müssen erstens die technischen Kapazitäten und das Spezialwissen ausgebaut werden und zweitens eine umfassende Analyse und Bewertung von Bedrohungen vorgenommen werden. Dazu gehören eine Erhöhung der Durchhaltefähigkeit, die Reaktionsfähigkeit aller CERTs sowie deren Vernetzung untereinander.

Aktueller Stand:

In 2015 hat das GovCERT für den Austausch von technischen Informationen über Cyber Bedrohungen zwei Plattformen aufgebaut und in Betrieb genommen. Beide basieren auf der Open Source Software MISP (Malware Information Sharing Plattform).

Mit ausgewählten Mitgliedern des geschlossenen Kundenkreises von MELANI (Energiesektor und Finanzsektor) wurde ein Pilotprojekt realisiert. Dieses erlaubt den Organisationen und dem GovCERT, einfach und effizient über längere Zeiträume zurück nach Manipulationen (sogenannte Indicators of Compromise) von Computersystemen und Netzwerken zu suchen.

Weiter wurden verschiedene Plattformen weiterentwickelt, welche das Nachverfolgen von Phishing und Malware-Angriffen ermöglichen, um betroffene Firmen und Organisationen zu informieren und zu schützen. Besonders erwähnenswert ist die Inbetriebnahme der Webseite antiphishing.ch. Mit Hilfe dieser Website können Bürgerinnen und Bürger sowie Firmen auf einfache Weise bei Phishing verwendete URLs an MELANI melden. Die dabei gesammelten Informationen werden zusätzlich statistisch aufbereitet und dienen der Darstellung eines technischen Lagebildes.

Durch die Besetzung einer zusätzlichen Stelle im GovCERT wurden die Analysekapazität und die Durchhaltefähigkeit des GovCERT weiter erhöht.

3.2.2 Massnahme 6: Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe

Zuständigkeiten: EJPD-KOBIK; EFD-MELANI

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

Aktueller Stand:

Das Konzept wurde erarbeitet und 2015 den Strafverfolgungsbehörden von Bund und den Kantonen zur Vernehmlassung unterbreitet. Die inhaltlichen Eingaben der konsultierten Stellen konnten in den aktuellen Konzeptentwurf übernommen werden.

Neben dem Konzept wurde in Zusammenarbeit mit der Bundesanwaltschaft durch fedpol ein Cyber-Phänomene-Katalog, der aus 25 Cyber-Phänomenblättern besteht, erstellt. Diese Cyber-Phänomenblätter beschreiben die verschiedenen Arten von Cyberkriminalität, die Täterschaft, die Tatmittel und die Angriffs-Methode, die Angriffsobjekte sowie die technische Komplexität. Dieser Katalog hat massgeblichen Einfluss auf die konkrete Definition der Cyberkriminalität in der Schweiz.

Die Vernehmlassung hat einerseits bestätigt, dass die Strafverfolgungsbehörden mit Blick auf die Erstellung einer nationalen Fallübersicht eine zentrale Erfassung der Cyberkriminalität bevorzugen. Die im Rahmen von Massnahme 6 katalogisierten Cyber-Phänomene wur-

den in die aktuellen Arbeiten der Arbeitsgruppe zur Harmonisierung der Schweizerischen Polizeiinformatik aufgenommen. Dadurch ist sichergestellt, dass unabhängig der verwendeten polizeilichen Informationssysteme eine einheitliche Erfassung der Cyberkriminalität möglich ist.

Parallel zu den Konzeptarbeiten M6 NCS sind die Konferenz der Kantonalen Polizeikommandanten (KKPKS) und fedpol daran, eine nationale Gesamtstrategie zu sämtlichen Aspekten der Verfolgung der Cyberkriminalität zu erarbeiten. Diese nationale Gesamtstrategie Cybercrime soll die eigentliche Ermittlungsarbeit sowie Fragen der Organisation, der Infrastruktur und der Ausbildung umfassen. Im Rahmen dieser Gesamtstrategie sollen dereinst als Teilaspekte auch die Umsetzungsmodalitäten der Massnahmen und Bedarfsschätzungen aufgezeigt werden, die Gegenstand des Grundauftrages von KOBIK und des Konzeptberichtes zu Massnahme 6 sind.

3.2.3 Massnahme 14: Aktive Massnahmen und Identifikation der Täterschaft

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

Die Fähigkeiten des Nachrichtendienstes des Bundes (NDB) zur Identifikation der Täterschaft (Akteur- und Umfeldanalyse und die Entwicklung technischer Hilfsmittel) soll mit der NCS weiter ausgebaut werden. Auch hier ist eine enge Zusammenarbeit der relevanten Akteure (MELANI, NDB, KOBIK, Cyber NDB und subsidiär der Armee) nötig.

Aktueller Stand:

Das Spezialwissen und die Fähigkeiten rund um Cyber wurden beim NDB mit der Schaffung des neuen Bereichs Cyber NDB aufgebaut, mit der FUB und dem militärischen Nachrichtendienst (MND) als Leistungserbringer. Die Schnittstellen zwischen dem Cyber NDB und MELANI sowie der Informationsaustausch zwischen diesen Stellen wurden etabliert. Auch konnten die Cyber NDB Fähigkeiten und Kenntnisse aufgebaut und ein breites Netz an Kontakten und Informationsquellen etabliert werden. Das neu zur Verfügung stehende Wissen ermöglicht es dem Cyber NDB selbstständig, sowie im Verbund mit FUB und MND als Leistungserbringer, Cyberattacken gegen Schweizer Interessen frühzeitig festzustellen. Dieser Erkenntnisse fliessen in die Analyse der Bedrohungslage durch MELANI ein. Die FUB und der MND konnten durch die NCS ebenfalls eigene Fähigkeiten und Kenntnisse im militärisch-strategischen und im technisch-analytischen Cyberbereich aufbauen.

3.3 Kontinuitäts- und Krisenmanagement

Das Krisenmanagement setzt klar definierte Führungsabläufe und -prozesse für den Cyber-Fall voraus. Das Kontinuitätsmanagement sorgt dafür, dass die Geschäftsprozesse auch während einer Krise verfügbar sind. Bei der Kontinuität sind folgende Massnahmen enthalten: Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren (M12), Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise (M13) sowie Konzept Führungsabläufe und -prozesse mit Cyber-Ausprägung (M15).

3.3.1 Massnahme 12: Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren

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

Basierend auf den Ergebnissen der Risiko- und Verwundbarkeitsanalyse definiert das jeweilige federführende Bundesamt für Wirtschaftliche Landesversorgung (BWL) respektive das

Bundesamt für Bevölkerungsschutz (BABS) in Zusammenarbeit mit den relevanten Unternehmen und zuständigen Fachstellen die notwendigen Massnahmen zur Sicherstellung der Kontinuität. Für jeden der 28 Teilsektoren wird aufbauend auf der Risiko- und Verwundbarkeitsanalyse ein Massnahmenbericht erarbeitet.

Aktueller Stand

In der Erdgasversorgung wurde ein erster Entwurf eines Massnahmenkataloges erstellt und der NCS-Koordinationsstelle zur Überprüfung vorgelegt. Die versorgungsrelevanten Unternehmen werden einen gemeinsamen 24/7-Pikettdienst aufbauen, der bei IKT-Ereignissen schweizweit kurzfristig eingesetzt werden kann. Weiter werden die Unternehmen das Notfallkommunikationssystem «Polycom» anschaffen sowie dem geschlossenen Kundenkreis der Melde- und Analysestelle Informationssicherheit (MELANI) beitreten.

Im Strassenverkehr ist die Verwundbarkeit so gering, dass vorderhand keine Massnahmen vorgeschlagen werden. Stattdessen gilt es, die aktuellen Entwicklungen (z.B. IKT im Fahrzeug) zu beobachten, um diese im Rahmen der periodischen Wiederholung der Verwundbarkeitsanalyse neu zu beurteilen.

Im Bereich Medien ist der Aufbau einer neuen Fachgruppe innerhalb des geschlossenen Kundenkreises bei MELANI vorgesehen. Zudem prüfen einzelne Unternehmen den Aufbau von redundanten Standorten. Des Weiteren gilt es die dynamische Entwicklung (z.B. neue Verbreitungstechnologien) der Medienlandschaft zu beobachten und periodisch hinsichtlich neuer Verwundbarkeiten und Risiken zu beurteilen.

In den anderen bis Januar 2016 abzuschliessenden kritischen Teilsektoren wurden im Rahmen der Risiko- und Verwundbarkeitsanalyse ebenfalls bereits erste mögliche Massnahmen identifiziert. Diese befinden sich zurzeit bei den zuständigen Stellen und Fachbehörden im Review und werden im Rahmen der Erarbeitung von Massnahmen in den entsprechenden Berichten detaillierter beschrieben.

3.3.2 Massnahme 13: Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise

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

Die betroffenen Akteure werden in einer Krise durch MELANI subsidiär unterstützt mit der Bereitstellung von Expertenwissen. Der freiwillige Informationsaustausch von Betreibern kritischer Infrastrukturen, IKT-Leistungserbringern und Systemlieferanten wird sichergestellt, um die Kontinuität und Widerstandsfähigkeit auf der Basis der Selbsthilfe zu stärken. Dazu wurden die heute vorhandenen Dienstleistungen nicht nur sichergestellt, sondern weiter ausgebaut.

Das EDA wird informiert bei Fällen mit möglichen aussenpolitischen Implikationen und ist eingebunden bei der Erarbeitung von entsprechenden Vorsorgeplanungen

Aktueller Stand:

Um festzustellen, welche Bedürfnisse die betroffenen Akteure haben, hat MELANI eine online-Umfrage im geschlossenen Kundenkreis durchgeführt. Die Resultate werden zurzeit ausgewertet und bilden die Grundlage für die Weiterentwicklung sowie Anpassungen der MELANI Produkte und Dienstleistungen. Das Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch wurde konsolidiert, angepasst und wird nun erweitert und auf die Bedürfnisse der kritischen Teilsektoren betreffend Kontinuitätsmanagement abgestimmt.

3.3.3 Massnahme 15: Konzept Führungsabläufe und -prozesse mit Cyber-Ausprägung

Zuständigkeit: BK

Mit der Massnahme 15 soll das bestehende, allgemeine Krisenmanagement mit den Cyber-Aspekten ergänzt werden.

Aktueller Stand:

Die Massnahme wurde 2014 abgeschlossen.

Die Massnahme 15 wurde auf Stufe Bund mit einem Konzept für Führungsabläufe und -prozesse in Krisensituationen mit Cyber-Ausprägung abgeschlossen. Gleichzeitig wurde die Zusammenarbeit mit den Kantonen und den Betreibern kritischer Infrastrukturen im Rahmen der Umsetzung der NCS durch den Sicherheitsverbund Schweiz in der Arbeitsgruppe 3 - Krisenmanagement weiterentwickelt. Die Aktivitäten dieser Arbeitsgruppe sollen somit auch im Jahresbericht NCS rapportiert werden. Die Details sind in Kapitel 3.6 zusammengefasst.

3.4 Unterstützende Prozesse

Als Grundlagen und Prozesse für die Bewältigung der Cyber-Problematik sind umfassende internationale Kooperationen, der Aufbau von Kompetenzen durch Forschung und Bildung sowie gegebenenfalls eine Anpassung von gesetzlichen Grundlagen notwendig. Hierzu wurden folgende Massnahmenpakete gebildet:

- Forschung und Kompetenzbildung: (M1, M7, M8)
- Internationale Kooperationen: (M9, M10, M11)
- Gesetzliche Grundlagen: (M16)

3.4.1 Massnahme 1: Identifikation von Cyber-Risiken durch Forschung

Zuständigkeiten: SBFI; KS NCS

Mit Hilfe der Forschung sollen die relevanten Cyber-Risiken der Zukunft, wie auch die Veränderungen in der Gefährdungslandschaft aufgezeigt werden, damit Entscheidungen in Politik und Wirtschaft frühzeitig und zukunftsgerichtet getroffen werden können. Zu diesem Zweck wird die Forschung (sowohl Grundlageforschung als auch angewandte Forschung) im Bereich Schutz vor Cyber-Risiken gefördert. Verantwortlich für die Umsetzung ist das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) in Zusammenarbeit mit der Koordinationsstelle NCS (KS NCS).

Aktueller Stand:

Im Januar 2015 hat das SBFI den interdepartementalen Steuerungsausschuss Forschung und Bildung im Bereich Cyber-Risiken (Comité de Pilotage Recherche et Formation Cyber - CoPIRFCyber) eingesetzt. Der Ausschuss setzt sich zusammen aus Vertreterinnen und Vertretern aller Organe der Bundesverwaltung, welche Interesse an Fragen der Forschung und Bildung im Bereich Cyber-Risiken haben. Ziel des Ausschusses ist es, zu definieren, in welche Richtung die Forschung entwickelt werden soll und welches die wichtigsten Themen der Forschung (Grundlagenforschung und angewandte Forschung) für die nächsten 5, 10 und 20 Jahre sind.

Zur fachlichen Unterstützung hat der CoPIRFCyber eine Expertengruppe eingesetzt, bestehend aus 14 Spezialistinnen und Spezialisten aus Lehre, Forschung und Praxis, welche im Bereich Cyber-Risiken tätig sind. Die Expertengruppe nimmt im Januar 2016 ihre Arbeit auf. Zusätzlich veranstaltet das SBFI eine Tagung zur Lancierung der Forschung zu Cyber-Risiken in der Schweiz und zum Einbezug weiterer Spezialistinnen und Spezialisten in die Arbeit der Expertengruppe. Die Swiss Cyber Risk Research Conference (SCRRC) findet am 20. Mai 2016 im Swiss Tech Convention Center an der EPFL Lausanne statt.[1]

3.4.2 Massnahme 7: Übersicht Kompetenzbildungsangebote

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

Um die Cyber-Resilienz in der Schweiz zu erhöhen, müssen gezielt spezifische Fähigkeiten aus- und aufgebaut werden. Gemäss NCS ist eine Übersicht zu erstellen, die über die bestehenden Kompetenzbildungsangebote Auskunft gibt, damit Angebotslücken erkannt und geschlossen werden können. Die Umsetzung dieser Massnahme erfolgt in enger Abstimmung mit der Umsetzung der «Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz» und dem EDA.

Aktueller Stand:

Die Massnahme konnte 2015 mit der Publikation des Berichtes «Kompetenzbildungsangebote im Umgang mit Cyber-Risiken»[2] abgeschlossen werden. Der Bericht basiert auf einer Befragung von 40 Expertinnen und Experten. Er zeigt auf, welche Angebote von welchen Nutzergruppen wahrgenommen werden und wo noch Angebotslücken bestehen. Die Expertinnen und Experten wiesen insbesondere auf fehlende Angebote im Bereich der Sicherheitskultur und auf den Mangel an Angeboten an der Schnittstelle zwischen IKT-Sicherheitsfachleuten und dem Management hin. Für spezifische Bereiche wurde auch das Fehlen von Ausbildungsangeboten in Bezug auf technische Sicherheit (z.B. für den Betreib eines CERT) genannt. Im Bereich Justiz und Polizei wurde mehrfach auf das Fehlen von kombinierten Ausbildungsangeboten Forensik und Jura sowie generell auf mangelnde Sensibilisierung bzgl. Cyber-Risiken hingewiesen.
Die festgestellten Angebotslücken sollen im Rahmen der Massnahme 8 geschlossen werden.

3.4.3 Massnahme 8: Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken

Zuständigkeiten: KS NCS; SBFI, EDA-PD

Mit der Massnahme 8 sollen einerseits bestehende Kompetenzbildungsangebote im Umgang mit Cyber-Risiken ausgebaut und andererseits die Schliessung der erkannten Angebotslücken erarbeitet werden. Die Förderung der Ausbildung erfolgt in enger Abstimmung mit der Förderung der Bildung im Bereich Cyber-Risiken und baut auf den Erkenntnissen aus Massnahme 7 auf.

Aktueller Stand:

[1] Informationen zur Veranstaltung werden ab Februar 2016 auf der Seite www.scrrc.ch abrufbar sein.

[2] Der Bericht ist auf der Seite der Informationsgesellschaft Schweiz verfügbar: http://www.bakom.admin.ch//themen/infosociety/04837/index.html

Das EDA gab 2015 eine Ressortforschung zum Thema Kompetenzbildung im Bereich Cybersicherheit im Ausland in Auftrag (veröffentlicht unter http://www.diplomacy.edu/cyber-security). Diese beleuchtet die verschiedenen Massnahmen, welche zehn ausgewählte OECD-Staaten zur Förderung der Kompetenzbildung im Bereich Cyber-Sicherheit getroffen haben (z.B. im Hochschulbereich, durch berufliche Weiterbildungsprogramme etc.). Die dabei identifizierten Lösungsansätze können mögliche unter Massnahme 8 gestartete Aktivitäten in der Schweiz inspirieren.

Auf Grund der engen Verknüpfung zwischen den Themen Forschung und Bildung hat das SBFI zusammen mit der KS NCS entschieden, den Bereich Bildung ebenfalls im Rahmen des interdepartementalen Steuerungsausschusses Forschung und Bildung im Bereich Cyber-Risiken (Comité de Pilotage Recherche et Formation Cyber - CoPIRF Cyber) (vgl. Massnahme 1) zu bearbeiten. Ziel ist es, die Bildung an den Hochschulen parallel zur Forschung zu fördern.

Zusätzlich laufen Arbeiten mit dem Verband ICT-Berufsbildung Schweiz zur Förderung der Berufsbildung. Die Idee ist, einen Abschluss für eine eidgenössisch diplomierte ISC-Security Expertin resp. einen eidgenössisch diplomierten ICT-Security Experten zu schaffen. Die Gespräche mit interessierten Parteien sind angelaufen, und im Frühjahr 2016 entscheidet der Verband ICT-Berufsbildung, ob ein solcher Abschluss realisiert werden kann.

3.4.4 Massnahme 9: Internet Governance

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 Bundesamt für Kommunikation (BAKOM) nimmt aktiv an den relevanten internationalen und regionalen Arbeiten, 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) und Europarat teil.

Aktueller Stand:

Das BAKOM hat sich aktiv an den Arbeiten des ICANN-Regierungsbeirats (Government Advisory Committee, GAC) beteiligt, dessen Vorsitz die Schweiz innehält. In diesem Zusammenhang standen die Übergabe der Aufsicht über die IANA-Funktionen sowie die Steigerung der Rechenschaftspflicht (Accountability) im Zentrum der Arbeiten, an welchen sich auch das EDA beteiligte. Zudem setzte sich die Schweiz für sicherheits- und vertrauensstärkende Massnahmen bei den neuen Top-Level-Domains ein. Im Rahmen der Überprüfung der Umsetzung der Resultate des Weltgipfels zur Informationsgesellschaft (WSIS) beteiligte sich die Schweiz mit einer Delegation aus BAKOM und EDA an den Vorbereitungsarbeiten für das hochrangige Treffen der UN-Generalversammlung im Dezember 2015 in New York, mit welchem die Arbeiten abgeschlossen wurden.

Weiter unterstützt das BAKOM die Vorbereitung und Durchführung des Internet Governance Forum (IGF), als Mitinitiant und Mitorganisator des europäischen IGF-Dialogforums «EuroDIG (European Dialogue on Internet Governance)». Zusammen mit dem EDA ist das BAKOM zudem in der Steuerungsgruppe der Geneva Internet Platform vertreten und unterstützt deren Arbeiten.

Auf nationaler Ebene organisiert das BAKOM regelmässig die Diskussionsplattform «Plateforme Tripartite zum WSIS Follow-up», welche einen Informationsaustausch aller Interessengruppen (Bundesverwaltung, Zivilgesellschaft, Akademie) zu aktuellen Themen und Entwick-

lungen in Bezug auf das Internet ermöglicht und veranstaltete im Mai 2015 das Swiss Internet Governance Forum, welches die Interessengruppen zu einem interaktiven Dialog über Fragen zur Internet Governance zusammen brachte.

3.4.5 Massnahme 10: Internationale Kooperation Cyber-Sicherheit

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

Massnahme 10 umfasst die sicherheitspolitische Interessenswahrung 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:

2015 setzte sich die Schweiz weiterhin für die Schaffung eines normativen Regelwerkes ein, um die Nutzung und Grenzen des Cyber-Raumes mithilfe von politischen und rechtlichen Instrumenten zu regeln und ihre Vision eines offenen, freien und sicheren Cyber-Raumes zu fördern.

Zu den politischen Instrumenten gehört die Schaffung von gegenseitigem Vertrauen, zumal Vertrauen die Voraussetzung für Transparenz, zwischenstaatliche Kooperation und Stabilität im Cyber-Raum ist. Die Schweiz hat den OSZE-Prozess rund um Vertrauensbildung aktiv mitgestaltet. Zudem unterstützte die Schweiz den serbischen OSZE-Vorsitz bei der Organisation einer OSZE-weiten Konferenz.

Im Bereich der Schaffung von staatlichen Verhaltensnormen bildete die Global Conference on Cyberspace 2015, die am 16.-17. April 2015 in Den Haag stattfand, den Schwerpunkt der Schweizer Aktivitäten. Bundesrat Didier Burkhalter nahm an der Konferenz teil und setzte sich dafür ein, dass das zwischenstaatliche Regelwerk auf dem existierenden Völkerrecht basieren muss, welches auch im Cyber-Raum anwendbar ist.

Dank einer von der Schweiz organisierten Veranstaltung in Genf konnten als Beitrag zur Global Conference on Cyberspace 2015 regionale Ansätze verglichen und die Zusammenarbeit über regionale Grenzen hinaus gefördert werden.

Um die Teilnahme von Entwicklungsländern an internationalen Prozessen zu ermöglichen bzw. zu erleichtern, finanzierte die Schweiz konkrete Projekte zum Kapazitätsauf- bzw. -ausbau. Sie ist auch Gründungsmitglied des im Berichtsjahr ins Leben gerufenen Global Forum on Cyber Expertise (GFCE), das zum Ziel hat, den globalen Kapazitätsaufbau weiter zu fördern.

Die Schweiz beteiligte sich auch dieses Jahr aktiv am multilateralen Dialog zwischen europäischen Staaten und China, um die jeweilige Bedrohungsauffassung besser zu verstehen und um Fragestellungen zu identifizieren, deren Vertiefung von gegenseitigem Interesse sind.

3.4.6 Massnahme 11: Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit

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

Der Fokus der Massnahme 11 liegt auf der Koordination und Kooperation der Cyber Security Experten in der Schweiz, um das internationale Engagement bei Standardisierungsorganisationen und anderen zielführenden Initiativen zu optimieren.

Aktueller Stand:

2015 wurde im Austausch mit den beteiligten Akteuren die prioritären Wirkungsbereiche für die Koordination internationaler Standardisierung und Initiativen im Bereich Cyber Security festgelegt und die für die Massnahme notwendigen Prozesse abgestimmt. Die aktiven Teilnehmer der M11 streben künftig einen jährlichen öffentlichen Workshop an, Koordinations-

projekte werden bei Bedarf in Fachgruppen organisiert. Die Prozesse und die prioritären Wirkungsbereiche wurden dokumentiert und an die Koordinationsstelle NCS übergeben.

3.4.7 Massnahme 16: Handlungsbedarf rechtliche Grundlagen

Zuständigkeiten: KS NCS

Massnahme 16 sieht vor, dass das anwendbare Recht daraufhin überprüft wird, ob es die nötigen Grundlagen für den Schutz gegen Cyber-Risiken enthält, und dass die allenfalls nötigen Anpassungen vorgenommen werden. Die Verwaltungseinheiten sollen für ihr Aufgabengebiet die relevanten Rechtsgrundlagen erheben und den Revisions- bzw. Ergänzungsbedarf evaluieren.

Aktueller Stand:

Erste Abklärungen zu den rechtlichen Grundlagen wurden 2014 abgeschlossen. Auch die aktuellen Entwicklungen ergeben keinen koordinierenden Regelungsbedarf. Der Regelungsbedarf wird laufend neu beurteilt.

3.5 Umsetzungsaktivitäten der Armee

Die Armee gehört zu den kritischen Infrastrukturen des Landes, für welche der Cyber-Raum und die Cyber-Bedrohungen eine zentrale Herausforderung geworden ist. Mit der rasanten Entwicklung und der zunehmenden Wichtigkeit des Cyber-Raumes ergeben sich neue militärische operationelle Optionen, die zu berücksichtigen sind. Zu den wichtigsten unmittelbaren Aufgaben der Armee gehört aber der Schutz ihrer IKT-Systeme und -Infrastrukturen in allen Lagen, um ihre Einsatzfähigkeit und Handlungsfreiheit sicherzustellen.

Die Armee verfügt über wesentliches Wissen und Fähigkeiten, welche von den verantwortlichen Bundesämtern bei Bedarf subsidiär abgerufen werden können, sofern sie nicht gleichzeitig von der Armee selber benötigt werden.

Zu diesen Zwecken werden das Wissen und die Fähigkeiten der Armee laufend weiterentwickelt. Die Präzisierung der Aufgaben der Armee im subsidiären Bereich sowie ihre Aufgaben im Kriegs- und Konfliktfall sind in Erarbeitung. Im Bereich des Personals konnten die in 2015 geplanten Ressourcen nicht beschafft werden; es ist vorgesehen, dies in 2016 nachzuholen.

Aktueller Stand:

Die doktrinalen Eckwerte der militärischen Aktionen im Cyber-Raum und die methodischen Grundsätze des Cyber-Risiko-Managements sind definiert. Auch wurden wichtige Schritte in den Bereichen Antizipation (u.a. Schaffung einer «Kartographie» der Akteure im akademischen Sektor) und Cyber-Lagebild realisiert und ein Beirat für die Begleitung der Arbeiten geschaffen. Im Jahr 2015 fand die Übung «CYBER-PAKT 15» statt, die ein wichtiger Meilenstein im Bereich des Krisenmanagements und der Zusammenarbeit der Armee mit ihren Partnern darstellt. Zudem konnten die Prozesse für die Behandlung von Cyber-Vorfällen etabliert und überprüft werden. Somit hat der Cyber-Milizstab der Armee seine Grundbereitschaft erreicht. Es wurden auch mehrere Sensibilisierungsaktionen zugunsten der Verwaltungseinheiten und der Milizformationen durchgeführt. Sobald die Ressourcen es erlauben, kann das etablierte Ausbildungskonzept ab 2016 systematisch umgesetzt werden.

3.6 Umsetzungsaktivitäten Kantone

Der Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) ist die Schnittstelle der NCS zu den Kantonen. Die Fachgruppe Cyber (FG-C) des KKM SVS stellt in Zusammenarbeit mit den Kantonen, den Gemeinden und den erforderlichen Bundesstellen die Koordination zwischen Bund und Kantonen in der Umsetzung der NCS sicher. Sie steuert vier Teilprojekte beziehungsweise Arbeitsgruppen. Die Koordinationsstelle NCS ist Mitglied der FG-C und bildet auf Stufe Bund die Brücke zu den Projektarbeiten mit den Kantonen.

Aktueller Stand:

Anlehnend an die Massnahme 3 NCS (Prüfkonzept der IKT-Verwundbarkeiten) wurde von den beteiligten Organisationen eine Selbstüberprüfung der Cyber-Risiken durchgeführt. Diese wurde evaluiert und Massnahmen zur Reduzierung der bestehenden Risiken vorgeschlagen. Anlehnend an die Massnahmen 4 und 5 der NCS wurde der Gesamtprozess zur Bearbeitung von Cyber-Vorfällen erstellt und in fünf Teilprozesse unterteilt. Sowohl die Teilprozesse wie auch die Definition eines Cyber-Sicherheitsvorfalls wurden den Kantonen zur Verfügung gestellt.

Das Konzept zur Massnahme 15: «Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung» wurde um die Dimension der Kantone und kritischen Infrastrukturen erweitert. Zur Überprüfung des Konzeptes wurde ein strategisches Seminar mit Vertretern des Bundes, der meisten Kantone sowie den Betreibern von kritischen Infrastrukturen durchgeführt. Dazu wurde ein massgeschneidertes Szenario zu einem Cyber-Angriff auf das Schweizerische Rentensystem entwickelt. Die Hauptthemen waren Problemerfassung, Prozesse, Strukturen, Schnittstellen und Bedürfnisse.

4 Strategisches Controlling

Der Bundesrat hat den Steuerungsausschuss NCS (STA NCS) beauftragt, die Umsetzung der Strategie mit einem strategischen Controlling zu begleiten. Das Controlling soll den zielorientierten und terminlichen Fortschritt der NCS-Massnahmen der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» halbjährlich überprüfen. Gemäss Bundesratsbeschluss vom 15. Mai 2013 zum Umsetzungsplan der NCS soll dieses Geschäft jeweils via Generalsekretärenkonferenz (GSK) an den Bundesrat gehen. Die 5. Sitzung des STA NCS hat am 20. August 2015 stattgefunden.

5 Wirksamkeitsüberprüfung

2015 haben die Vorbereitungsarbeiten für die Wirksamkeitsüberprüfung der NCS begonnen. Die Überprüfung soll im Jahr 2016 durchgeführt werden, so dass im April 2017 dem Bundesrat die Ergebnisse vorgelegt werden können und dieser auf Basis der Ergebnisse über eine Weiterführung der NCS entscheiden kann.

Im Frühjahr 2015 entwickelte die KS NCS mit Hilfe externer Unterstützung ein Detailkonzept für die Umsetzung der Wirksamkeitsüberprüfung. Ziel der Arbeiten war es, eine stringente Methodik zu entwickeln, die konkreten Fragestellungen zu definieren und die zu befragenden Akteure zu identifizieren. Der STA NCS hat in der Sitzung vom 20. August 2015 dem Detailkonzept zugestimmt. Daraufhin hat die KS NCS den Auftrag im Rahmen eines Einladungsverfahrens einer geeigneten Firma erteilt. Im Dezember fand die erste Projektsitzung mit den Auftragnehmern statt.

Die Wirksamkeitsüberprüfung kann daher zeitgerecht starten und basiert bereits auf einem gut ausgearbeiteten Konzept. Es bleibt die Herausforderung, dass die Wirkung der NCS zu einem Zeitpunkt bewertet werden muss, bei welchem sich viele der Massnahmen noch in Umsetzung befinden.

6 Schlussbetrachtung

Im dritten Jahr der Umsetzung hat sich erneut gezeigt, wie umfangreich und komplex die Umsetzung der NCS ist. Die Bedrohungen von heute entsprechen nicht jenen von morgen, weshalb die NCS flexibel gestaltet und laufend den neuen Bedrohungen angepasst werden muss. Auch 2015 gab es darum noch Änderungen am Zeitplan und bei den Definitionen einiger Aufgaben. Dies geschieht jedoch immer in Hinblick auf die Sicherung der hohen Qualität der Umsetzungsarbeiten und der Produkte der NCS. Bereits heute wird für die Sicherung der Resultate über den Zeithorizont von 2017 hinaus gearbeitet. Es wurden neue Prozesse definiert, die dafür sorgen werden, dass die durch die NCS geschaffene Zusammenarbeit, Kooperation und Kommunikation der relevanten Akteure auch in der Zukunft so bleiben wird und bei Bedarf weitere Akteure eingebunden werden können. Diese Faktoren haben bei einigen Massnahmen zu leichten Verzögerungen geführt. Dennoch sind die Umsetzungsarbeiten bei der Mehrheit der Massnahmen im Zeitplan, weshalb die Bilanz auch Ende 2015 positiv ausfällt.

Der Anstieg der Cyber-Delikte des vergangenen Jahres hat wiederum verdeutlicht, wie wichtig die nationale und internationale Kooperation ist. Auf nationaler Ebene steht dabei die vertrauensvolle Zusammenarbeit mit den Betreibern von kritischen Infrastrukturen, der Wirtschaft und den Kantonen im Zentrum. Ebenso hat sich die Zusammenarbeit mit der Armee gut etabliert. Zur Stärkung der Schweiz muss der Informationsaustausch mit den Polizeiorganisationen und Staatsanwaltschaften sowie Betreibern der kritischen Infrastrukturen, IKT-Leistungserbringern, Systemlieferanten, Fachbehörden und Regulatoren weiter ausgebaut werden.

Auch ist die Zusammenarbeit und der Austausch von relevanten Informationen mit Staaten und internationalen Organisationen zentral. Das gegenseitige Vertrauen muss durch politische und rechtliche Instrumente gefördert und geregelt werden, da Vertrauen die Voraussetzung für Transparenz, zwischenstaatliche Kooperation und Stabilität im Cyber-Raum ist. So soll das gemeinsame Verständnis über Sicherheit und Vertrauen im Internet weiter vorangetrieben werden.

Das Jahr 2016 wird weitere Herausforderungen mit sich bringen, was wiederum heisst, dass wir diese Zusammenarbeit und Kooperation stärken und alle relevanten Akteure von heute und der Zukunft einbinden müssen.

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

«Jahresbericht NCS 2013»:
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=de

«Jahresbericht NCS 2014»:
https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

7.2 Zusammenstellung der Parlamentarischen Vorstösse zu Cyber-Risiken

Vorstoss Ip. = Interpellation; Mo. = Motion; Po. = Postulat; An. = Anfrage	Eingereicht am:	Stand per 31.12.2015:
08.3050 Po Schmid-Federer. Schutz vor Cyber-bulling	11.03.2008	erledigt
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	erledigt
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	29.06.2010	erledigt

der SiK-S vom 11. Januar 2011 sowie Verhandlungen des Ständerates vom 15. März 2011 (AB S 15.03.2011)		
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	erledigt
12.3417 Mo. Hodgers. Öffnung der Telekommunikationsmärkte. Strategien für die nationale digitale Sicherheit	30.05.2012	erledigt
12.4161 Mo. Schmid-Federer. Nationale Strategie gegen Cyberbullying und Cybermobbing	13.12.2012	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
13.3677 Ip. Fraktion. Schnüffeleien der NSA und anderer Nachrichtendienste auch in der Schweiz	11.09.2013	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	angenommen
13.3927 Ip. Reimann. Schutz für den Datenbunker Schweiz	27.09.2013	im Plenum noch nicht behandelt
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	05.11.2013	erledigt

umzusetzen.“)		
13.4077 Ip. Clottu. Datenspionage und Internetsicherheit	05.12.2013	erledigt
13.4086 Mo. Glättli. Nationales Forschungsprogramm Alltagstauglicher Datenschutz in der Informationsgesellschaft	05.12.2013	erledigt
13.4308 Po. Graf-Litscher. Sicherheit und Unabhängigkeit der Schweizer Informatik verbessern	13.12.2013	im Plenum noch nicht behandelt
13.5224 Fra. Reimann. Zur Präsenz von US-Geheimdiensten und ihren Cyber-Schnüffelaktivitäten in der Schweiz	10.06.2013	erledigt
13.5325 Fra. Sommaruga. Verwendet der Nachrichtendienst des Bundes illegal von der NSA beschaffte Daten?	11.09.2013	erledigt
14.1105 An. Buttet. Mittel zur Verteidigung des Cyberraums in der schweizerischen Sicherheitspolitik	10.12.2014	Eingereicht
14.3654 Ip. Derder. Digitale Sicherheit. Sind wir auf dem Holzweg?	20.06.2014	im Plenum noch nicht behandelt
14.4138 Ip. Noser. Beschaffungspraxis bei kritischen IKT-Infrastrukturen	10.12.2014	im Plenum noch nicht behandelt
14.4299 Ip. Derder. Umfassende Aufsicht über die digitale Revolution. Muss ein Staatssekretariat für die digitale Gesellschaft geschaffen werden?	12.12.2014	im Plenum noch nicht behandelt
14.5569 Frau. Leutenegger. NSA. Ein Jahr Schnüffelstaat	26.11.2014	erledigt
15.1059 Berberat. Dringende Finanzhilfe des Bundes infolge des Cyberangriffs auf TV5 Monde	10.09.2015	erledigt
15.3359 Po. Derder. Für eine innovative Armee	20.03.2015	im Plenum noch nicht behandelt
15.3375 Ip. Entwendung von SIM-Codes bei der Firma Gemalto durch die Geheimdienste NSA und GCHQ	20.03.2015	erledigt
15.3656 Ip. Munz. Gefahr für das AKW Mühleberg durch Fernwartung des Computersystems. Fragwürdige Überwachung des Ensi	18.06.2015	im Plenum noch nicht behandelt
15.4073 Ip. Derder. Ist die Armee wirklich in der Lage, den Schweizer Cyberspace zu schützen?	25.09.2015	im Plenum noch nicht behandelt
15.5299 Fra. Leutenegger. Schutz vor NSA-Spionage	09.06.2015	erledigt

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
CNO	Computer Network Operations
CSIRT	Computer Security Incident Response Team
CSTD	Commission on Science and Technology for Development
Cyber NDB	Bereich Cyber im Nachrichtendienst des Bundes
EAPC	Euro-Atlantischen Partnerschaftsrates
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDA-AIO	Eidgenössisches Departement für auswärtige Angelegenheiten – Abteilung internationale Organisationen
EDA-PD	Eidgenössisches Departament für auswärtige Angelegenheiten – Politische Direktion
EDI	Eidgenössisches Departement des Innern
ENISA	European Network and Information Security Agency
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
GAC	Government Advisory Committee
GIP	Geneva Internet Platform
GCHQ	Government Communications Headquarters
GovCERT	Swiss Governmental Computer Emergency Response Team
GSK	Generalsekretärenkonferenz
GS-VBS	Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport
ICANN	Internet Cooperation for Assigned Names and Numbers
ICT	Information and Communication Technology
IG	Internet Governance
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	Militärisches Computer Emergency Response Team
MND	Militärischer Nachrichtendienst
NATO	North Atlantic Treaty Organization
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz

NSA	National Security Agency
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SDO	Standardisierungsorganisation
SKI-Strategie	Schutz Kritischer Infrastrukturen Strategie
SLA	Service Level Agreement
STA NCS	Steuerungsausschuss Nationale Cyber Strategie
SVS	Sicherheitsverbund Schweiz
SVU	Sicherheitsverbundübung
UNO	United Nations Organization
UP NCS	Umsetzungsplan zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken
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
WiÜ	Wirksamkeitsüberprüfung
WL	Wirtschaftliche Landesversorgung
WSIS	World Summit on the Information Society