.

Jahresbericht 2016

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 2017

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

Wie wichtig und komplex die Digitalisierung und Automatisierung in allen Lebensbereichen geworden sind, hat sich auch im Jahr 2016 gezeigt. Besonders deutlich vor Augen geführt wurde und dies an der diesjährigen CeBIT, bei der die Schweiz das Partnerland war. Diese stand im Zeichen der voranschreitenden Digitalisierung und Automatisierung neuer Bereiche. Besonders eindrücklich zeigt sich dies in den Fortschritten bei der Entwicklung hin zur autonomen Mobilität oder am Beispiel von Robotern, welche viele unsere menschlichen Aufgaben übernehmen. Die Chancen der Digitalisierung sind auch für die Schweiz von grosser Bedeutung. Doch sie bringt leider auch Risiken mit sich, wie die neusten Cyber-Angriffe deutlich gezeigt haben. Spionage- und Sabotageangriffe, neue und bisher unbekannte Arten von Malware und Erpressungen mit DDoS-Angriffen gehören zum Alltag. Wir müssen wachsam bleiben und unsere Cyber-Sicherheit weiter erhöhen, damit wir auf die stetig steigende Gefährdung durch Cyber-Angriffe vorbereitet sind.

Die wichtigste Frage liegt auf der Hand: Ist die Schweiz auf dem richtigen Weg und reichen die heutigen Schutzmassnahmen aus, um nachhaltig gegen diese Cyber-Risiken gewappnet zu sein? Mit der Verabschiedung der «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» und dessen Umsetzungsplan sind wir in die richtige Richtung gegangen und haben bereits viel erreicht. Konkret wurden 15 der 16 geplanten NCS-Massnahmen bis Ende 2016 abgeschlossen. Der Umsetzungserfolg dieser Massnahmen wurde 2016 einer Wirksamkeitsüberprüfung unterzogen, die Aufschluss darüber gibt, wo die Ziele erreicht wurden und wo weiterer Handlungsbedarf besteht. Die Resultate dieser Überprüfung werden im vorliegenden Bericht kurz zusammengefasst.

Ohne die Resultate der Wirksamkeitsüberprüfung vorwegzunehmen, kann gesagt werden, dass wir mit der Umsetzung der NCS in vielen Bereichen beachtliche Fortschritte erzielen konnten. Dank der NCS haben wir den Grundstein für eine vertrauensvolle Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und der Gesellschaft gelegt, um die Schweiz besser vor Cyber-Angriffen zu schützen. Auch international hat sich die Schweiz im Rahmen ihrer Aussen- und Sicherheitspolitik weiterhin für einen offenen, freien und sicheren Cyber-Raum eingesetzt. 2016 wurde die Schweiz zum Mitglied der UNO Expertengruppe zu Cyber[1] für den Zeitraum von einem Jahr gewählt.

Die Ereignisse der letzten Jahre und die Resultate der Wirksamkeitsüberprüfung haben deutlich gemacht, dass das bereits Erreichte wichtig ist, die Arbeiten rund um die Cyber-Sicherheit jedoch noch lange nicht abgeschlossen sind. Wir werden auch 2017 alle notwendigen Schritte unternehmen, damit die Schweiz das Internet weiterhin als sicheren, offenen und freien Raum für Wirtschaft, Behörden und Bevölkerung nutzen kann. Dazu gehört insbesondere die Weiterentwicklung der NCS. Die Umsetzung der aktuellen NCS wird bis Ende dieses Jahres abgeschlossen sein und wir sind bereits daran, das weitere Vorgehen in enger Zusammenarbeit mit allen Betroffenen festzulegen.

In diesem Sinn freuen wir uns darauf, mit Ihnen zusammen den Schutz der Schweiz vor Cyber-Risiken weiter zu stärken, so dass wir die Chancen der Digitalisierung nutzen können, ohne dabei unverhältnismässige Risiken einzugehen.

Peter Fischer
Delegierter für die Informatiksteuerung des Bundes (ISB)

[1] UN Governmental Group of Experts on the Development in the field of information and telecommunications in the context of international security.

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 von 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 übertragen worden. Koordiniert werden die Arbeiten von der Koordinationsstelle (KS NCS), 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 (internationale Zusammenarbeit, Forschung und Bildung und rechtliche Grundlagen). In allen Bereichen konnten in den vergangenen Jahren, nicht zuletzt dank der engen Zusammenarbeit und guten Kommunikation aller Beteiligten, wichtige Ziele erreicht werden. So konnten bis Ende 2016 15 der 16 NCS Massnahmen abgeschlossen und der im Umsetzungsplan vorgegebene Zeitplan eingehalten werden. Auch hat die 2016 durchgeführte Wirksamkeitsüberprüfung ergeben, dass die NCS eine beachtliche Wirkung erzielt und dass der dezentrale und risikobasierte Ansatz sich bewährt hat.

Bei der **Prävention** haben das Bundesamt für Bevölkerungsschutz (BABS) und das Bundesamt für Wirtschaftliche Landesversorgung (BWL) die Risiko- und Verwundbarkeitsanalysen in den in der «Strategie zum Schutz der kritischen Infrastrukturen (SKI)» identifizierten kritischen Teilsektoren durchgeführt, und die Berichte liegen vor.

Die Darstellung der gesamtheitlichen Bedrohungslage wurde durch den Nachrichtendienst des Bundes (NDB) erstellt. Diese interaktive Darstellung, der sogenannte Bedrohungslageradar, visualisiert die verschiedenen Cyber-Bedrohungen für die Infrastrukturen der Schweiz und zeigt die Relevanz der Bedrohungen auf. Der Lageradar wird ab 2017 den Mitgliedern des geschlossenen Kundenkreises von MELANI zur Verfügung gestellt. Eine Übersicht der wichtigsten Cyber-Bedrohungen in 2016 liefern der MELANI Halbjahresbericht und der Jahresbericht des Bundesamtes für Polizei (fedpol).

Im Bereich **Reaktion** wurden im Jahr 2016 die Fachkompetenzzentren zur Analyse von Schadsoftware beim Informatiksteuerungsorgan des Bundes (ISB) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), z. B. GovCERT-ISB, CISIRT-BIT, milCERT-VBS, weiter ausgebaut und zahlreiche weitere Produkte entwickelt, die die Detektions- und Reaktionsfähigkeit erhöhen. Zudem wurden wichtige interne und externe Prozesse zur Verbesserung der Kommunikation etabliert und die internationale Zusammenarbeit gestärkt

In der Fachabteilung Cyber des Nachrichtendienstes des Bundes (NDB) konnten zudem das Spezialwissen und Fähigkeiten aufgebaut werden, die es ihm erlauben, die Ziele, Methoden und Akteure eines Angriffs zu analysieren und so mögliche Täter zu identifizieren. Das vom Volk gutgeheissene Nachrichtendienstgesetz (NDG) gibt dem NDB zudem die rechtliche Grundlage bei schwerwiegenden Cyber-Angriffen auf kritische Infrastrukturen auch offensive Gegenmassnahmen vorzunehmen, was die nachrichtendienstliche Informationsbeschaffung vereinfacht. Derzeit fehlt es aber insbesondere an zusätzlichen technischen und operativen Analysten sowie an Sprachspezialisten für eine systematischere und nachhaltigere Aufarbeitung der Cyber-Attacken beim NDB.

Im Rahmen der **Kontinuität** erarbeiten das BABS und das BWL gemeinsam mit den Betreibern der kritischen Infrastrukturen und den zuständigen Fach-, Aufsichts- und Regulierungsbehörden Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren. Diese Arbeiten bauen auf den Ergebnissen der durchgeführten Risiko- und Verwundbarkeitsanalysen auf und dienen dazu, die identifizierten Schwachstellen und Risiken zu reduzieren. Dabei ist zu berücksichtigen, dass für viele Sektoren die Einführung von Richtlinien und Mindeststandards zunehmend wichtig wird sowie die Abstimmung der Massnahmen mit bestehenden Vorgaben zu beachten ist.

Im Bereich der **unterstützenden Prozesse** stehen die Forschung und Bildung sowie die internationale Zusammenarbeit im Vordergrund. Das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) hat gemeinsam mit der KS NCS wichtige Gremien ins Leben gerufen, die in Zusammenarbeit mit der Wirtschaft und Verwaltung eine Übersicht der Kompetenzbildungsangebote sowie Vorschläge zu deren Nutzung und Schliessung der Lücken erstellt haben. So konnte in Zusammenarbeit mit dem Verband ICT-Berufsbildung Schweiz und dank der Unterstützung zahlreicher Unternehmen in Rekordzeit, ein neuer Abschluss als «ICT Security Expertin/Experte» mit eidgenössischem Diplom geschaffen werden.

Gleichzeitig werden in einem Expertenbericht die wichtigsten Forschungsthemen zu Cyber-Risiken in der Schweiz identifiziert. Ausserdem werden innerhalb der Verwaltung die entsprechenden Fachstellen mit Bezug zur Forschung (Cyberrisiken) neu in einem amts- und departementsübergreifenden Komitee koordiniert. Das Netzwerk der Forschenden wurde an der „Swiss Cyber Risk Research Conference“ gestärkt.

Die internationale Zusammenarbeit im Bereich Frieden und internationale Sicherheit wurde auf bilateraler und multilateraler Ebene unter der Führung der Abteilung für Sicherheitspolitik (ASP) des Eidgenössischen Departementes des Äussern (EDA) weiter gestärkt und ausgebaut. Für den Bereich Internet Governance war das Bundesamt für Kommunikation (BAKOM) zuständig. 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, und die Schweiz wurde 2016 für ein Jahr zum Mitglied der «UN Governmental Group of Experts zu Cyber (UNGGE)» gewählt.

Wichtigste Cyber-Bedrohungen 2016

Das Jahr 2016 war primär geprägt von ähnlichen Cyber-Bedrohungen, wie in 2015.[2] Ein wesentlicher Unterschied stellt jedoch die Intensität und Häufigkeit der Cyber-Angriffe dar: In 2016 konnte eine zunehmende Spezialisierung beobachtet werden. Auch ist ein Zuwachs von kriminellen Handlungen durch Spionageangriffe zu beobachten. Wie der MELANI Halbjahresbericht 2016/2 aufzeigt, ist Cyber-Spionage eine ernstzunehmende Gefahr, und Unternehmen müssen sich bewusst sein, dass es sich um eine reale und nicht um eine hypothetische Gefahr handelt. Zahlreiche Fälle, die MELANI bekannt sind, bestätigen dies. Eine weitere beunruhigende Tendenz ist, dass komplexe Angriffe, sogenannte Advanced Persistent Threat (APT), vermehrt auch bei Cyber-Kriminellen zu finden sind.

Die wesentlichen Gefahren für 2016 zusammengefasst sind[3]:

- **Spionage** (Angriff auf eine Rüstungsfirma)
- **Datenabflüsse** (Twitter-Zugangsdaten auf dem Schwarzmarkt, Passwörterklau)
- **DDoS und Erpressung** (Cryptolocker, Locky, Armada Collective, KeRanger, CTB-Locker)
- **Social Engineering und Phishing** (CEO-Fraud)
- **Crimeware** (E-Banking Trojaner wie Gozi, Conficker, Dyre)
- **Angriffe auf industrielle Kontrollsysteme** (Angriff auf Steuerungssysteme bei Kraftwerken in der Ukraine).

[2] MELANI Halbjahresbericht 2015 Januar-Juni: www.melani.admin.ch

[3] Für Details über diese Bedrohungen siehe MELANI Halbjahresbericht 2016 Januar-Juni: www.melani.admin.ch

2 Stand der Umsetzungsarbeiten NCS 2016

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.

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

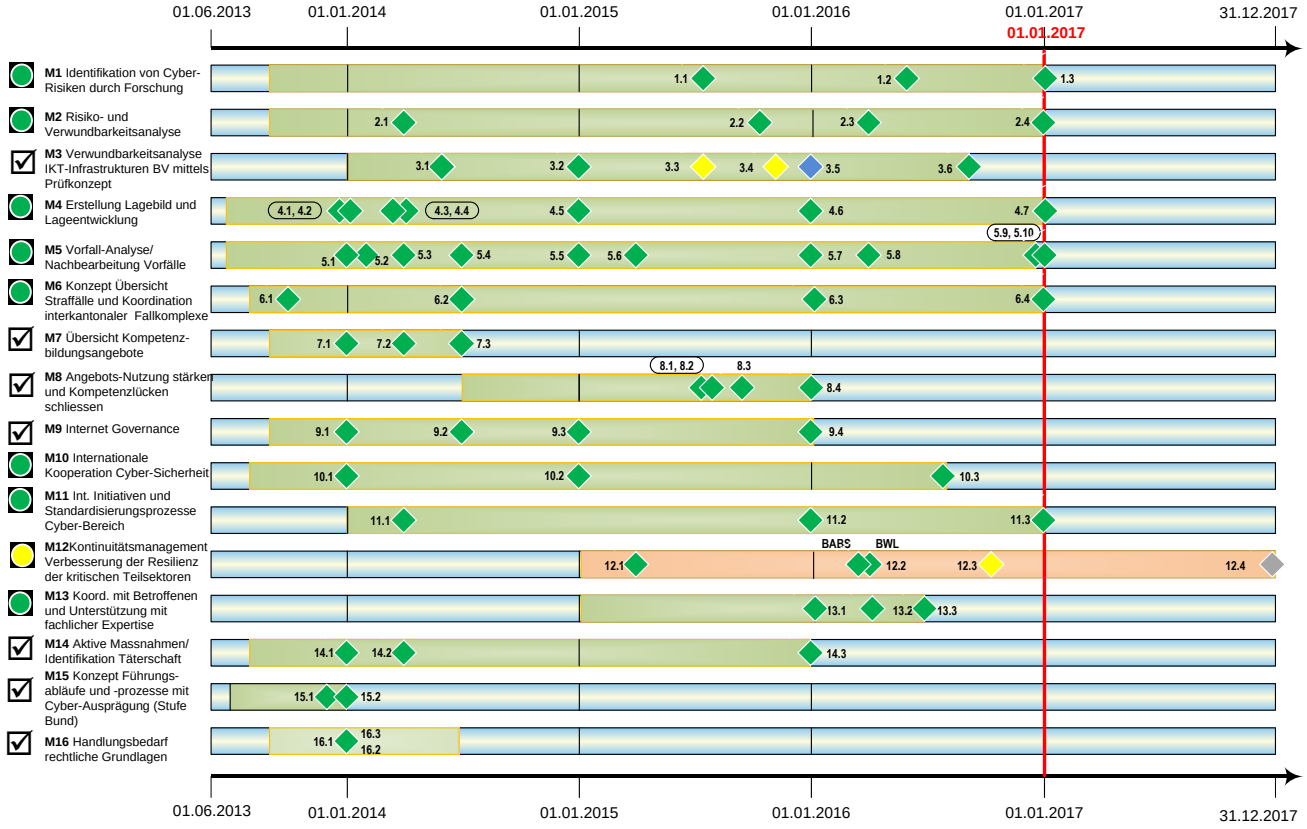

Abbildung 1: Roadmap NCS

Legende: Stand Massnahmen

- Massnahme gefährdet
- Massnahme in Verzug
- Massnahme planmässig in Umsetzung
- Sondermassnahme geplannt
- Massnahme noch nicht in Umsetzung
- Massnahme abgeschlossen

2.1 Prävention

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

2.1.1 Massnahme 2: Risiko- und Verwundbarkeitsanalyse

Zuständigkeiten: WBF-BWL, VBS-BABS, Fach-, Aufsichts- und Regulierungsbehörden; EFD-MELANI

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

Das BWL und das 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 Fach-, Aufsichts- und Regulierungsbehörden bei Bund und Kantonen beigezogen. Dadurch sind die Analysen breit abgestützt; gleichzeitig zeigt dies auch das grosse Interesse der involvierten Stellen.

Aktueller Stand:
Die Massnahme wurde weitgehend in 2016 abgeschlossen, es folgen noch Finalisierungsarbeiten. Dabei sind Verwundbarkeitsanalysen in 28 kritischen Teilsektoren durchgeführt worden. Die Analysen dienen als Grundlage zur Erarbeitung von Massnahmen zur Stärkung der IKT-Widerstandsfähigkeit (vgl. Kapitel 3.3.1 Kontinuitätsmanagement).

2.1.2 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 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:
Die Massnahme wurde 2016 abgeschlossen.

In Erfüllung seines Auftrages hat das ISB bis Ende 2015 ein Prüfkonzept für IKT-Infrastrukturen der Bundesverwaltung erstellt (im Folgenden als Prüfkonzept bezeichnet), das auf den im IKT-Sicherheitsmanagement etablierten Risiko-basierten Standards und Best Practices (z. B. ISF IRAM2) aufsetzt und in dem Sinne die aktuelle Lehrmeinung widerspiegelt. Weil die Umsetzung des Prüfkonzeptes in der Praxis sehr aufwändig wäre, hat der STA NCS am 25. Februar 2016 auf Antrag des BWL, EDA und NDB beschlossen, dass das ISB im Sinne einer Sondermassnahme zu M3 einen zum Prüfkonzept alternativen Vorschlag für das weitere Vorgehen im Bereich IKT-Verwundbarkeitsanalysen in der Bundesverwaltung ausarbeiten soll. Obwohl die befristete Stelle für M3 bereits Ende 2015 abgebaut worden ist, hat das ISB im Rahmen dieser Sondermassnahme einen solchen Ansatz ausgearbeitet und am 31. Mai 2016 dem STA NCS vorgelegt. Der STA NCS hat sich zugunsten dieses Ansatzes ausgesprochen. Im Wesentlichen basiert er darauf, dass auf einen Risiko-basierten Ansatz verzichtet wird und stattdessen eine Verwundbarkeitsanalyse durchgeführt wird.

2.1.3 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), der Bereich Cyber 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 Massnahme wurde 2016 abgeschlossen.

Die Darstellung der gesamtheitlichen Bedrohungslage wurde erstellt. Ab 2017 wird diese interaktive Darstellung (Bedrohungslageradar) den Mitgliedern des geschlossenen Kundenkreises von MELANI zur Verfügung gestellt. Eine öffentliche Version soll später folgen.

Auch wurde ein externes Gutachten erstellt, das die eingeleiteten Prozesse von MELANI zur Selbstverbesserung beurteilt.

2.2 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).

2.2.1 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) wie das GovCERT, CISIRT-BIT sowie das 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 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:

Die Massnahme wurde 2016 abgeschlossen.

Insgesamt wurde die Detektions- und Reaktionsfähigkeit bei den Fachkompetenzzentren (GovCERT, BIT-CISIRT, mil-CERT) ausgebaut.

Zudem sieht das neue Nachrichtendienstgesetz (NDG) den nachrichtendienstlichen Schutz der kritischen Infrastrukturen vor Cyber-Angriffen ausdrücklich vor und gibt neu dem NDB die rechtliche Grundlage, bei schwerwiegenden Cyber-Angriffen auf kritische Infrastrukturen auch offensive Gegenmassnahmen vornehmen zu können. Weiter sieht das NDG zur nachrichtendienstlichen Informationsbeschaffung auch das Eindringen in Computersysteme und -netzwerke vor.

Die im Rahmen der NCS geschaffene Stelle im Bereich Cyber NDB wurde 2016 besetzt und nimmt folgende Aufgaben wahr:

- Quellenrekrutierung und -führung (Anwerbung von externen Fachexpertinnen und Fachexperten)
- Informationsbeschaffung (ohne bewilligungspflichte Massnahmen gemäss NDG)
- Strategische Analysen
- Technische Analysen
- Nachrichtendienstliche Täteridentifikation (Attribution)
- Internationale Kooperation

Der Aufbau eines Quellennetzes und die weitere internationale Vernetzung mit Partnerdiensten haben zudem dazu geführt, dass der NDB immer wieder in der Lage ist, Cyber-Angriffe frühzeitig zu entdecken. Allerdings kann der NDB heute mit den verfügbaren Mittel und Fähigkeiten nur einen kleinen Teil der im Bereich beschafften Informationen verarbeiten. Zudem dauern die Cyber-Angriffe oft über Jahre an, was die wenigen Spezialistinnen und Spezialisten auf längere Zeit bindet. Das Risiko wächst, dass gleichzeitig neue Attacken nicht rechtzeitig erkannt werden, daher ist eine systematischere und nachhaltigere Aufarbeitung der Cyber-Attacken zentral. Leider fehlt es beim NDB derzeit insbesondere an zusätzlichen technischen und operativen Analysten sowie an Sprachspezialistinnen und –spezialisten, um diesen Auftrag zu erfüllen.

2.2.2 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) und dort im fedpol) angesiedelte Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) in Zusammenarbeit mit den Kantonen per Ende 2016 ein Konzept «Fallübersicht und Koordination interkantonaler Fallkomplexe» vorlegt.

Aktueller Stand:
Die Massnahme wurde 2016 abgeschlossen.

Sowohl die in Massnahme 6 der NCS vorgesehene Koordination von Ermittlungen im Bereich der Cyber-Kriminalität als auch das gesamtschweizerische Lagebild sind bereits Gegenstand der Verwaltungsvereinbarung zwischen dem EJPD und der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) über die Grundaufträge der bei fedpol angesiedelten KOBIK. Diese Grundaufträge der von Bund und Kantonen gemeinsam finanzierten KOBIK liessen sich bis anhin jedoch nur teilweise umsetzen. Das von Strafverfolgungsbehörden des Bundes und der Kantone gemeinsam erarbeitete Konzept M6 der NCS schlägt Massnahmen vor für die einheitliche Erfassung, Koordination und Verbreitung

von Lageinformationen, die für das Erstellen des umfassenden Cybercrime-Lagebildes notwendig sind. Für die angestrebte interkantonale Fallkoordination in allen Cyber-Delikten beschreibt das Konzept erste polizeiliche Massnahmen zur Bestimmung der örtlich und sachlich zuständigen Behörden für die Verfolgung der oft aus dem Ausland und über ausländische Cyber-Infrastrukturen agierenden Täterschaft. Wie sich an der Herbsttagung der KKJPD vom 18. November 2016 gezeigt hat, unterstützt die KKJPD das Konzept.

Das gesamtschweizerische Lagebild und die interkantonale Fallkoordination sind jedoch nur zwei Teilaspekte der Herausforderung Cybercrime. Deshalb erarbeitet die Konferenz der kantonalen Polizeikommandanten (KKPKS) das nationale Dispositiv «Cybercrime und IT-Forensik». Dort sollen alle mit der Bekämpfung der Cyberkriminalität verbundenen organisatorischen und infrastrukturellen Fragen in ihrer Gesamtheit angegangen werden. Auch fedpol beteiligt sich an diesen Arbeiten. Die Frage der *Umsetzung* des Konzepts zur Massnahme 6 soll deshalb im Rahmen dieses Dispositivs von der KKPKS geklärt werden.

2.2.3 Massnahme 14: Aktive Massnahmen und Identifikation der Täterschaft

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

Die Fähigkeiten des 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:
Die Massnahme wurde 2016 abgeschlossen.

Ergänzend zu den Ausführungen unter 3.2.1 konnte der NDB auch 2016 Cyber-Attacken gegen die Schweiz auf bestimmte staatliche oder staatlich unterstützte Akteure zurückführen. Diese Erkenntnisse flossen in Kurzanalysen, Berichte und Informationsnotizen zuhanden der zuständigen Behörden ein. Die Attribution ist ein nachrichtendienstlicher Prozess, der die Täteridentifikation mit einer bewerteten Wahrscheinlichkeit erlaubt und nicht als primäres Ziel die strafrechtliche Verfolgung, sondern die Wahrung der politischen Handlungsfähigkeit vorsieht. Entsprechend richten sich die Ergebnisse primär an die politischen Entscheidungsträger.

2.3 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).

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

Zuständigkeiten: WBF-BWL, VBS-BABS, Fach-, Aufsichts- und Regulierungsbehörden**;** EFD-MELANI

Basierend auf den Ergebnissen der Risiko- und Verwundbarkeitsanalyse definiert das jeweilige federführende BWL respektive das 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:
Das BABS und das BWL erarbeiten gemeinsam mit den Betreibern der kritischen Infrastrukturen und den zuständigen Fach-, Aufsichts- und Regulierungsbehörden Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren. Diese Arbeiten bauen auf den Ergebnissen der durchgeführten Risiko- und Verwundbarkeitsanalysen auf und dienen dazu, die identifizierten Schwachstellen und Risiken zu reduzieren.

Die Massnahmenberichte zur Verbesserung der IKT-Resilienz aller in der «Strategie zum Schutz kritischer Infrastrukturen (SKI)» definierten kritischen Teilsektoren werden Ende 2017 vorliegen. Diverse Massnahmen wurden bereits umgesetzt resp. befinden sich in Umsetzung. Damit kann die Widerstandsfähigkeit der für die Versorgung unseres Landes mit wichtigen Gütern und Dienstleistungen kritischen Teilsektoren gegenüber IKT-Störungen und -Angriffen gestärkt werden.

2.3.2 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 mit Expertenwissen unterstützt. 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:
Die Massnahme wurde 2016 abgeschlossen.

Die im November 2015 durchgeführte Befragung unter den Mitgliedern des geschlossenen Kundenkreises wurde 2016 ausgewertet und die wichtigsten Resultate in einem Bericht festgehalten. Die Umfrage zeigt, dass das Modell der Public-Private-Partnership von MELANI weiterhin gut funktioniert. MELANI hat auch das starke Wachstum des Geschlossenen Kundenkreises der letzten Jahre gut bewältigt. Herausforderungen liegen in der Stärkung derjenigen Sektoren, welche noch wenig etabliert sind.

Basierend auf den Erkenntnissen aus dieser Umfrage hat MELANI ein Konzept zur Stärkung ihrer Rolle als Plattform für den Informationsaustausch erstellt. Das Konzept klärt den Grundauftrag und die Ziele von MELANI und zweigt Massnahmen auf, wie sich MELANI sowohl auf der operativen als auch auf der strategischen Ebene weiterentwickeln will. Das Konzept wird ergänzt durch ein externes Gutachten über die vorgesehenen Massnahmen.

2.3.3 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 dessen Arbeitsgruppe 3 - Krisenmanagement weiterentwickelt. Die Aktivitäten dieser Arbeitsgruppe sollen somit auch im Jahresbericht NCS rapportiert werden. Die Details sind in Kapitel 3.6 zusammengefasst.

Im November 2016 wurde die Übung «Popula» durchgeführt, die einen Cyber-Angriff auf das Rentensystem der Schweiz simulierte. Sie stand unter der Federführung des Sicherheitsverbundes Schweiz (SVS) in Zusammenarbeit mit Bund, Kantonen und kritischen Infrastrukturen und hatte zum Ziel, die Bereitschaft und das Krisenmanagement in Bund und Kantonen zu üben.

2.4 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)

2.4.1 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 soll die Forschung (sowohl Grundlageforschung als auch angewandte Forschung) im Bereich Schutz vor Cyber-Risiken gezielt genutzt und verstärkt werden. Verantwortlich für die Umsetzung ist das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) in Zusammenarbeit mit der Koordinationsstelle NCS (KS NCS).

Aktueller Stand:
Die Massnahme wurde 2016 abgeschlossen.

Bei den Arbeiten zur Identifizierung zentraler Forschungsthemen konnten wichtige Fortschritte erzielt werden. Der interdepartementale Steuerungsausschuss Forschung und Bildung im Bereich Cyber-Risiken (CoPIRFCyber) hat eine Expertengruppe aus 15 Expertinnen und Experten der Schweizer Hochschulen eingesetzt und damit beauftragt, die wichtigsten Forschungsthemen zu identifizieren. Die breit aufgestellte Expertengruppe hat sich vertieft

mit den verschiedenen Disziplinen, Blickwinkeln und Herausforderungen der Forschungslandschaft auseinandergesetzt und neun Forschungsgebiete identifiziert, in denen die Forschung inskünftig verstärkt durchgeführt werden soll. Aufgrund der stark interdisziplinär angelegten Thematik wurden zudem drei hochrelevante fach- und disziplinübergreifende Schlüsselthemen als künftige Forschungsschwerpunkte empfohlen. Der von der Expertengruppe konsolidierte Bericht wird voraussichtlich im Sommer 2017 veröffentlicht.

Gestützt auf Grundlagenarbeiten 2016 des SBFI und des SECO hat der Bundesrat am 11. Januar 2017 den Bericht „Rahmenbedingungen der digitalen Wirtschaft“ verabschiedet und gleichzeitig das Eidgenössische Departement für Wirtschaft, Bildung und Forschung beauftragt, die darin hergeleiteten Herausforderungen im Bereich Bildung und Forschung vertieft zu prüfen. Gemäss Auftrag sind unter Einbezug der zuständigen Bundesstellen sowie der Kantone und der Schweizerischen Hochschulkonferenz SHK im Wesentlichen die systemischen Auswirkungen der Digitalisierung auf den Bildungsbereich zu prüfen und allfällige Lücken an den Hochschulen für die Bewältigung der digitalen Transformation zu identifizieren. Die Arbeiten zur Erstellung des Prüfberichts (Teil Forschung) werden die Erkenntnisse des Expertenberichts zur Forschung im Bereich Cyber-Risiken (s.o.) aufnehmen und gegebenenfalls weiterentwickeln.

Mit der Durchführung der «Swiss Cyber Risk Research Conference» am 20. Mai 2016 an der EPFL wurde zudem ein wichtiger Schritt zur Vernetzung und Sensibilisierung der Forschenden im Bereich Cyber-Risiken erreicht. Über 300 Teilnehmende folgten den Referaten von nationalen und internationalen Fachspezialisten. Die Konferenz setzte ein wichtiges Zeichen für die Stärkung der Forschung zu Cyber-Risiken in der Schweiz und brachte zum ersten Mal Forschende aus sämtlichen relevanten Disziplinen zusammen.

2.4.2 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 7 wurde 2015 abgeschlossen.

2.4.3 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:
Die Massnahme wurde 2016 abgeschlossen.

Die Massnahme 8 konnte 2016 plangemäss abgeschlossen werden. Der interdepartementale Steuerungsausschuss Forschung und Bildung im Bereich Cyber-Risiken hat ein Konzept verabschiedet, welches aufzeigt, wie die Bildung im Bereich Cyber-Risiken gefördert werden soll.

Das wichtigste Resultat der Massnahme ist die Schaffung eines neuen Abschlusses als «ICT Security Expertin/Experte» mit eidgenössischem Diplom durch den Verband ICT-Berufsbildung Schweiz. Dank der Unterstützung durch die NCS ist es dem Verband gelungen, eine breit abgestützte Trägerschaft aus der Privatwirtschaft für den Abschluss zu bilden und gemeinsam mit diesen Partnern das Qualifikationsprofil zu entwickeln. Dieses ist nun erstellt, so dass bereits im Herbst 2018 die ersten Prüfungen stattfinden können.

2.4.4 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 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:
Die Massnahme wurde 2016 abgeschlossen.

Als letzter Meilenstein wurde 2016 eine Wirksamkeitsanalyse der Massnahme durchgeführt. Diese kommt zum Schluss, dass das Engagement der Schweiz im Bereich der Internet Governance mit der Umsetzung der Massnahme 9 den substantiellen Zielen entspricht und insgesamt koordinierter ausfällt. Dies indem die Zusammenarbeit innerhalb der Bundesverwaltung sowie mit den verschiedenen Interessengruppen weiter institutionalisiert und strukturiert wurde sowie vermehrt Synergien genutzt werden. Die Zusammenarbeit soll auch zukünftig weiter ausgebaut werden, damit sich die Schweiz auch in Bezug auf die immer neuen Herausforderungen im Bereich der Internet Governance aktiv und koordiniert einbringen kann.

2.4.5 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:
Die Massnahme wurde 2016 abgeschlossen.

2016 engagierte sich die Schweiz im Rahmen ihrer Aussen- und Sicherheitspolitik weiter für einen offenen, freien und sicheren Cyber-Raum, damit dessen Nutzung auf klaren Regeln basiert. Schwerpunkt ihres Engagements war die Arbeit in der «UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)», die sich als einziges Gremium der UNO mit der Erarbeitung globaler Verhaltensnormen für Staaten, der Anwendbarkeit des Völkerrechts, Vertrauensbildung und Kapazitätsaufbau im Cyber-Raum befasst. Die Schweiz wurde für die Zeitperiode 2016–2017 erstmals zum Mitglied gewählt. Ihre Prioritäten sind die Konsolidierung und Konkretisierung der bereits erfolgten konzeptuellen Arbeiten der Gruppe sowie die Einbindung von Nicht-UN GGE-Mitgliedern und nichtstaatlichen Akteuren in den Prozess.

Die Schweiz beteiligte sich weiter aktiv am Prozess der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) zu vertrauensbildenden Massnahmen im Cyber-Bereich.

Der Prozess zielt darauf ab, mittels Transparenz, Kooperation und Stabilität das zwischenstaatliche Vertrauen zu erhöhen. Zwischenstaatliches Vertrauen soll dazu beitragen, das Risiko von Fehleinschätzungen und Missverständnissen zu reduzieren. In diesem Rahmen förderte die Schweiz die Umsetzung der bereits beschlossenen vertrauensbildenden Massnahmen und unterstützte parallel dazu die Entwicklung weiterer Massnahmen. Angesicht der globalen Natur der Cyber-Risiken bemühte sich die Schweiz auch um die Universalisierung des OSZE-Prozesses.

Punktuell setzte sich die Schweiz für den Aufbau von cyber-bezogenen Kapazitäten ein. Sie unterstützte Projekte des «Global Forum on Cyber Expertise (GFCE)» (z. B. Meridian-Initiative zum Schutz kritischer Informationsinfrastrukturen). Zur Weiterentwicklung der eigenen Fähigkeiten setzte die Schweiz die Zusammenarbeit mit dem «Cooperative Cyber Defence Centre of Excellence (CCDCoE)» in Tallin, Estland, fort.

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

Schliesslich führte die Schweiz auf bilateraler Ebene cyber-spezifische Konsultationen mit ausgewählten Ländern.

2.4.6 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 Expertinnen und Experten in der Schweiz, um das internationale Engagement bei Standardisierungsorganisationen und anderen zielführenden Initiativen zu optimieren.

Aktueller Stand:
Die Massnahme wurde 2016 abgeschlossen.

In der M11 wurde in 2016 ein Workshop für die beteiligten Akteure zum Informationsaustausch veranstaltet sowie eine Umfrage für die Analyse der Wirksamkeit durchgeführt. Gegen Ende 2016 werden die Umfrageergebnisse ausgewertet und mit Rückmeldungen der Akteure Anfang Dezember aufbereitet. Mit der Abgabe des Berichtes zur Wirksamkeitsanalyse zum Jahresende an die KS NCS werden alle vorgegebenen Meilensteine und Lieferobjekte voraussichtlich planmässig erreicht.

Die Massnahme gilt im Sinne der NCS-Projektplanung als abgeschlossen. Die erarbeiteten Ergebnisse und Aktivitäten werden im Jahre 2017 fortgeführt.

2.4.7 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:
Die Massnahme wurde 2014 abgeschlossen.

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

2.5 Umsetzungsaktivitäten der Armee

Die Armee hat 2016 die Umsetzung ihres Cyber-Defence-Konzepts fortgesetzt und verschiedene organisatorische Verbesserungen vorgenommen. Die ständige Zunahme von Cyber-Bedrohungen und Cyber-Vorfällen, das Volks-Ja zum Nachrichtendienstgesetz (NDG), die Genehmigung des Militärgesetzes (MG) durch das Parlament und die Folgen des Hacker-Angriffs auf die RUAG zählen zu den wichtigsten Elementen, die kontinuierlich in die Bemühungen der Armee im Bereich Cyber Defence eingebunden wurden.

Im VBS wurde in Übereinstimmung mit den Zielen 2016 die Erstellung eines Plan d'Action Cyberdéfense DDPS (PACD) angeordnet. Dieser Plan steht im Einklang mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), erfüllt konkret deren Erwartungen und behindert ihre Entwicklung nicht.

Der Plan verfolgt drei Ziele:

- Stärkung des VBS, insbesondere der Armee, um die zunehmenden Cyber-Bedrohungen im Alltag sowie in Krisen- und Konfliktsituationen zu bewältigen;
- Konkrete Unterstützung im Cyber-Bereich bei der Umsetzung des NDG und der Bestimmungen des MG, die es der Armee ermöglichen, sich ab 2018 unter bestimmten Bedingungen aktiv gegen Cyber-Angriffe zu verteidigen;
- Schaffung günstiger Bedingungen, die es dem VBS (gemäss NDG) ermöglichen, KI-Betreiber zu unterstützen, auf die Hacker-Angriffe verübt wurden.

Bereits die Erarbeitung dieses Aktionsplans führte zu einer Optimierung der bestehenden Mittel; sie gab ausserdem den Anschub zur Einführung einer Governance im VBS. Die eigentliche Implementierung des Aktionsplans jedoch wird eine signifikante Umverteilung von Ressourcen im VBS erfordern. Der angestrebte Endzustand dürfte 2020 erreicht werden.

Der Reifegrad und die Bereitschaft der Armee werden aber auch durch die Ausbildung und Sensibilisierung ihres Miliz- und Berufspersonals gesteigert. So hat die Armee 2016 an verschiedenen Übungen teilgenommen, namentlich an der internationalen Übung LOCKED SHIELD 16 sowie an der Übung des Sicherheitsverbundes Schweiz (SVS), die einen Cyber-Angriff auf das Schweizerische Rentensystem mit Auswirkung auf die AHV-Nummer zum Thema hatte. Die Stabsstelle Cyber Defence der Armee hat die Übung CYBER PAKT 16 durchgeführt, in der verschiedene hochkomplexe und intensive Szenarien durchgespielt wurden. Auf diese Weise konnten die im Rahmen des PACD entwickelten Abläufe überprüft, das Verständnis der neuen rechtlichen Grundlagen verbessert und die Subsidiaritätsgrundsätze der Armee geregelt werden. Zusätzlich zu diesen Übungen fanden 2016 auch zahlreiche Sensibilisierungsaktionen beim Personal des VBS, bei der Truppe (z.B. beim Sicherheitseinsatz der Armee beim World Economic Forum), aber auch bei der Bevölkerung im Rahmen öffentlicher Veranstaltungen der Armee in Meiringen und Thun statt.

2.6 Umsetzungsaktivitäten Kantone

Der Sicherheitsverbund Schweiz (SVS) ist die Schnittstelle der NCS zu den Kantonen. Die Fachgruppe Cyber (FG-C) des 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. Die Koordinationsstelle NCS ist Mitglied der FG-C und bildet auf Stufe Bund die Brücke zu den Projektarbeiten mit den Kantonen. Für die kantonale Umsetzung der NCS wurden vier Arbeitsgruppen gegründet, welche von der Fachgruppe Cyber gesteuert werden.

<u>Aktueller Stand:</u>
Die Erhebung des Ist-Zustands der Cyber-Risiken bei den Kantonen bildete die Basis für die Ausarbeitung eines Hilfsmittels. Mit diesem können die wichtigen Prozesse in den Kantonen erhoben werden, womit ein wichtiger Schritt Richtung verbessertes Risikomanagement im

Cyber-Bereich getan werden kann. Dieses Hilfsmittel wird zurzeit von drei Kantonen auf seine Tauglichkeit geprüft, bevor es dann allen Kantonen zur Verfügung gestellt wird.

Die von der Arbeitsgruppe «Incident Management» erstellten Prozessbeschriebe zur Bearbeitung von Cyber-Vorfällen wurden teilweise angepasst bzw. verbessert.

Mit Hilfe der zweitägigen Stabsrahmenübung «POPULA» im November 2016 sollte das Konzept für Führungsabläufe und -prozesse auf Stufe Bund bei Krisen mit Cyber-Ausprägung überprüft werden, welches um die Dimension der Kantone und Kritische Infrastrukturen ergänzt wurde. Die Übung fand unter Teilnahme von Bund, Kantonen, kritischen Infrastrukturen und vom Szenario «Cyber-Angriff auf das Rentensystem» betroffenen Dritten statt. Rund 50 Teilnehmende aus verschiedenen Organisationen, die im Alltag mehrheitlich wenig bis nichts miteinander zu tun haben, waren anwesend. Als Einführung in die Übung zeigte die RUAG live eine technische Simulation eines Cyber-Angriffs. Das Ziel der Übung war die Überprüfung der Schnittstellen zwischen den verschiedenen vom Szenario betroffenen Organisationen. Dies bedeutete, dass die Teilnehmenden ihre Partner suchen, Informationen teilen sowie den Fall eskalieren lassen mussten. Es konnten wichtige Erkenntnisse für das Konzept und das nationale Krisenmanagement bei Krisen mit Cyber-Ausprägung gewonnen werden. Jedoch war es aufgrund der Art und Weise, wie sich die Übung entwickelt hat, nicht möglich, alle Teile des Konzeptes zu überprüfen.

In der Arbeitsgruppe zur Cyber-Kriminalität wurde entschieden, dass die von KOBIK unter Mithilfe der Kantone erstellten Phänomen-Infoblätter, die die wichtigsten Phänomene im Bereich Cyber-Kriminalität beschreiben, breitflächig bei den Strafverfolgungsbehörden zu verteilen sind, damit sie diese in ihrer täglichen Arbeit anwenden können.

3 Steuerungsausschuss und Strategisches Controlling

Der Bundesrat hat den 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. Das Controlling per 31. Dezember 2016 zeigt, dass von den 16 NCS Massnahmen bereits 15 abgeschlossen sind und die letzte laufende Massnahme im Bereich Kontinuitätsmanagement planmässig bis Ende 2017 erfüllt werden kann.

Der STA NCS hat sich dieses Jahr intensiv mit der Weiterentwicklung der NCS ab 2018 auseinandergesetzt. Er hat am 30. Juni 2016 in einer Sondersitzung, in der ordentlichen 7. Sitzung des STA NCS am 17. August 2016 und einem Workshop am 26. Oktober 2016 mit einem erweiterten Teilnehmerkreis das weitere Vorgehen diskutiert. Aufgrund der Resultate der Wirksamkeitsüberprüfung waren sich der STA NCS und der erweiterte Teilnehmerkreis einig, dass die NCS eine beachtliche Wirkung erzielt hat, dass der dezentrale und risikobasierte Ansatz richtig ist und die NCS weitergeführt werden muss.

4 Wirksamkeitsüberprüfung

Im Beschluss zum Umsetzungsplan der NCS hat der Bundesrat dem ISB den Auftrag erteilt, im April 2017 eine Wirksamkeitsüberprüfung der NCS vorzulegen. Um diesen Auftrag fristgerecht zu erfüllen, fand die Überprüfung bereits 2016 statt. Eine externe Firma führte zwischen März und Juli insgesamt 14 Interviews und 15 schriftliche Befragungen durch und analysierte insgesamt 130 Dokumente, welche im Rahmen der NCS erstellt worden sind.

Die NCS wurde dabei auf drei Ebenen evaluiert: der Umsetzungserfolg bei den 16 Massnahmen, die massnahmenübergreifenden Aspekte (Ressourcenplanung, Inhalte, Organisationsstruktur und Kommunikation) sowie die Schnittstellen zu den Arbeiten der Kantone und der Armee. Die Überprüfung führte zu folgenden Ergebnissen:

- **Massnahmen:** die Umsetzung der 16 Massnahmen der NCS war insgesamt erfolgreich, und die vorgegeben Ziele wurden grösstenteils erreicht. Dies hat nachweislich zu gestärkten Kapazitäten, aufgebautem Spezialwissen und verbesserter Koordination geführt. Der Nachweis einer unmittelbaren kausalen Wirkung der Massnahmen auf die strategischen Ziele ist auf Grund des frühen Zeitpunkts der Überprüfung schwierig. Mit Hilfe von Wirkungsmodellen kann aber plausibel aufgezeigt werden, welche Effekte zu erwarten sind. Bei vier Massnahmen wurden nicht alle gesetzten Ziele erreicht. Bei ihnen wird der weitere Handlungsbedarf ausgewiesen.
- **Inhalte, Ressourcen, Organisationstruktur und Kommunikation**: auf der übergeordneten Ebene stellt die Wirksamkeitsüberprüfung fest, dass sich die strategischen Ziele des Bundesrates von 2012 grundsätzlich bewährt haben. Die Ressourcen für die Umsetzung der Massnahmen waren knapp ausreichend und die dezentrale Organisationsstruktur hat insgesamt gut funktioniert. Bemängelt wird die Kommunikation gegen aussen auf der nationalen Ebene. Die NCS wird in der Öffentlichkeit zu wenig wahrgenommen, und es ist nicht genügend bekannt, was der Bund im Bereich der Cyber-Risiken unternimmt und wo er die Grenzen seiner Zuständigkeit sieht.
- **Schnittstellen zu den Arbeiten der Kantone und der Armee:** die Arbeiten der NCS wurden über den SVS mit jenen der Kantone koordiniert. Die Überprüfung hat gezeigt, dass die Zusammenarbeit gut funktioniert und eine gewisse Sensibilisierung in den Kantonen stattgefunden hat. Hingegen bleiben an der Schnittstelle zu den Arbeiten der Armee noch wichtige Fragen offen. Die Abgrenzung zwischen den zivilen Aufgaben der NCS und den Zuständigkeiten der Armee im Krisenfall sind nicht abschliessend geklärt, und die Erwartungen an die und die Möglichkeiten der Armee in Bezug auf die subsidiäre Unterstützung müssen präzisiert werden.

Die Resultate der Wirksamkeitsüberprüfung zeigen, dass die strategische Ausrichtung richtig gewählt wurde und die dezentrale aber eng koordinierte Umsetzung der NCS insgesamt gut funktioniert. In allen Bereichen ist es gelungen, funktionierende Prozesse und Strukturen zu etablieren und nötiges Spezialwissen aufzubauen, so dass die Schweiz heute besser auf Cyber-Risiken vorbereitet ist, als dies 2012 der Fall war. Gleichzeitig wird deutlich, dass mit der NCS erst ein Fundament gelegt worden ist und der Schutz vor Cyber-Risiken weiter ausgebaut werden muss.

5 Konferenzen und Anlässe

In diesem Kapitel werden einige wichtige Veranstaltungen aufgeführt, die 2016 auf nationaler und internationaler Ebene im Zusammenhang mit der NCS abgehalten wurden.

5.1 Nationale Ebene

Am 6. April 2016 wurde die vierte «Cyber-Landsgemeinde» durchgeführt. Rund 100 Cyber-Verantwortliche von Bund und allen Kantonen sowie enge Partner des Sicherheitsverbundes Schweiz (SVS) nahmen auch dieses Jahr am Vernetzungsanlass teil. Wie schon in den vergangenen Jahren standen der Umsetzungsstand der Projekte auf Kantonsebene und jener der NCS im Fokus sowie die Wirksamkeitsüberprüfung der NCS.

Vom 7. bis 8. April 2016 wurde die «Cyber 9/12 Student Challenge» in Genf durchgeführt. Wie im letzten Jahr waren der Atlantic Council zusammen mit dem Geneva Centre for Security Policy (GCSP) Gastgeber dieser Veranstaltung. Auch in diesem Jahr trafen sich 28

Teams aus 13 Ländern aus Europa und der Schweiz, dem Mittleren Osten und den USA, um sich auf einen grossen Cyber-Angriff vorzubereiten und adäquate Handlungsempfehlungen zu entwickeln. Das Sieger-Team kam diesmal aus Großbritannien. Seitens Bund wurde dieser Anlass durch die Teilnahme der KS NCS und weiterer Vertreter als Juroren unterstützt.

Am 20. Mai 2016 fand die erste «Swiss Cyber Risk Research Conference» an der Eidgenössische Technische Hochschule Lausanne (EPFL) in Lausanne statt, welche vom SBFI organisiert wurde. Zweck der Konferenz war, der Forschung zum Thema Cyber-Risiken Schub zu verleihen und das Netzwerk von Forschenden in der Schweiz zu stärken.

Am 18. September 2016 tagte in Luzern der dritte «Europäische Cyber Security Challenge». 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 EFD. Der diesjährige Sieger war Spanien.

Am 26. Oktober wurde die dritte «NCS-Tagung» veranstaltet, dies jedoch in einem anderen Format als in den Vorjahren: Am Morgen fand ein interner Workshop mit den Verantwortlichen der jeweiligen NCS-Massnahmen statt, um das weitere Vorgehen ab 1. Januar 2018 zu eruieren. Ziel war es, mit den Verantwortlichen der verschiedenen NCS-Massnahmen den weiteren Handlungsbedarf für eine mögliche Nachfolgestrategie der NCS festzustellen. Am Nachmittag folgte dann der offizielle Teil der NCS Tagung mit dem Ziel, Vertretungen aus Wirtschaft und Politik einen detaillierten Überblick über den aktuellen Umsetzungsstand der NCS-Massnahmen zu geben sowie die ersten Resultate der Wirksamkeitsüberprüfung zu präsentieren.

Vom 23. bis 24. November 2016 wurde die Krisenmanagementübung «Popula» durchgeführt, die einen Cyber-Angriff auf das Rentensystem der Schweiz simulierte. Sie stand unter der Federführung des SVS in Zusammenarbeit mit Bund, Kantonen und kritischen Infrastrukturen und hatte zum Ziel, die Bereitschaft und das Krisenmanagement in Bund und Kantonen zu üben.

5.2 Internationale Ebene

Vom 14. bis 18. März 2016 fand die jährliche IT-Messe «CeBIT» in Hannover statt, an der diesmal die Schweiz das Partnerland war. Schwerpunkt bildeten die Prozesse in Unternehmen und die Vernetzung des Alltags, das Internet der Dinge sowie die Industrie 4.0.

Vom 10. bis 11. Mai und vom 14. bis 15. November 2016 beteiligte sich die Schweiz erneut am fünften und sechsten «Sino-European Cyber Dialogue» und gestaltete diesen massgebend mit. 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.

Vom 8. bis 10. Juni 2016 wurde in Brüssel der «Europäische Dialog zur Internet Governance (EuroDIG)» durchgeführt. Die Veranstaltung hat das Internet Governance Forum der Vereinten Nationen zum Vorbild und ist Vorreiterin, wenn es um innovative Diskussionsformate und die Einbindung der verschiedenen Interessengruppen in die Diskussion rund um Themen mit Bezug zum Internet geht. Das BAKOM gehört zu den Gründungsmitgliedern des EuroDIG, und auch dieses Jahr konnte sich die Schweiz aktiv in die Diskussionen vor Ort einbringen.

Vom 29. August bis 2. September und vom 28. November bis 2. Dezember 2016 tagte die «UN Group of Governmental Experts» zu Cyber in New York und Genf. Die Schweiz ist 2016 neu Mitglied für 1 Jahr und entwickelt entlang der fünf Themenbereiche (d.h. Bedrohungslage, Normen für staatliches Verhalten, Völkerrecht, Vertrauensbildung und Kapazitätsaufbau) Empfehlungen zur Nutzung des Cyber-Raums.

Am 18. September 2016 traf sich im Vorfeld der Generalversammlung der Vereinten Nationen die «ITU/UNESCO Broadband Commission for Sustainable Development (BBCOM)» zu ihrem jährlichen Treffen in New York. Die BBCOM und ihre Arbeitsgruppen setzen sich insbesondere für die Ausweitung des Zugangs zu Breitbandinternet ein.

Am 28. bis 30. September 2016 fand in New Delhi die indische Konferenz «CyFy» statt, an welcher die Schweiz als Partnerstaat vertreten war. Dies ist die grösste asiatische Konferenz zu Cyber-Sicherheit und Internet Governance, an welcher neben Regierungen auch Vertretungen der Privatwirtschaft und Forschung teilnehmen.

Am 30. September 2016 endete die Aufsichtsrolle der USA über die «Internet Corporation for Assigned Names and Numbers (ICANN)», der Verwaltungsstelle von Internetadressen. Die weltweite Internetadressverwaltung wird seither von einer globalen Gemeinschaft geleitet, in der alle Interessensgruppen vertreten sind. Damit ist man dem von der Schweiz verfolgten Ziel einer internationalen Verwaltung des Domain-Namen-Systems (DNS) einen wichtigen Schritt nähergekommen.

Am 4. November 2016 fand der «OSZE Cyber Showcase Event» unter dem Vorsitz von Deutschland in Wien statt. Schwerpunkt bildete das Thema Attribution, die Identifikation der Täterschaft. Die Teilnehmerstaaten waren sich einig, dass die Attribution von Cyber-Vorfällen eine Herausforderung darstellt und gemeinsame Lösungen erarbeitet werden müssen. Die OSZE könnte einen geeigneten Rahmen für vertiefe Diskussionen zu diesem Thema bieten.

Vom 3. bis 9. November 2016 wurde in Hyderabad (Indien) das Treffen der «ICANN57» veranstaltet. Nach Marrakech (5. bis 10. März) und Helsinki (27. bis 30. Juni) war dies das dritte ICANN-Treffen im Berichtsjahr. Nach der Übergabe der Aufsichtsrolle der USA an die globale Community gilt es nun die Details umzusetzen und die Reformen innerhalb ICANN weiter voranzutreiben. Die Schweiz wurde per Akklamation für weitere zwei Jahre zum Vorsitz des Regierungsbeirates von ICANN gewählt.

Vom 16. bis 18. November 2016 organisierte die chinesische Regierung in Wuzhen – einer Kleinstadt nahe Shanghai - die dritte «World Internet Conference (WIC)». Die WIC ist der chinesische Gegenentwurf zum «Internet Governance Forum (IGF)» und stellt in erster Linie ein Sprachrohr der Kommunistischen Partei dar. Mit diesen Initiativen und den damit verbundenen Investitionen will China seinen Anspruch untermauern, in den Diskussionen zur Internet Governance eine immer wichtigere Rolle einzunehmen. Das Thema wurde von Staatspräsident Xi Jinping weit oben auf der politischen Agenda seines Landes positioniert, und dementsprechend scheut China keine Aufwände, diesen Ansprüchen gerecht zu werden.

Vom 6. bis 9. Dezember 2016 fand in Guadalajara (Mexiko) das erste Internet Governance Forum (IGF) der Vereinten Nationen nach der Mandatsverlängerung durch die UNO-Mitgliedstaaten im Dezember 2015 statt. Das IGF ist eine der grössten, jährlich stattfindenden Konferenzen im Bereich der Internet Governance und bietet allen Interessengruppen eine Diskussionsplattform für den Austausch zu Themen rund um das Internet. Die Schweiz hat in Mexiko angekündigt, die Durchführung des IGF 2017 am UN-Sitz in Genf als Gastgeberland unterstützen zu wollen.

Im August 2016 verabschiedete die Europäische Kommission die Netz- und Informationssicherheit Direktive der EU (NIS-Direktive), die für die EU Mitgliedstaaten verpflichtend ist. Die Weiterentwicklungen dieser Direktive müssen von der Schweiz beobachtet werden, da die Meldepflicht auch Auswirkungen für die Schweiz und Schweizer Unternehmen haben könnte, die in der EU tätig sind. Die Koordinationsstelle NCS ist Mitglied der ENISA Cyber-Expertengruppe und Teil der regelmässigen Konferenzen und Aktivitäten.

6 Schlussbetrachtung

Die Umsetzung der NCS neigt sich dem Ende zu. Von den 16 NCS-Massnahmen sind Ende

2016 15 Massnahmen abgeschlossen, und 1 Massnahme wird planmässig bis Ende 2017 umgesetzt sein. Auch liegen die ersten Resultate der Wirksamkeitsüberprüfung vor, die ergeben haben, dass mit der NCS eine grosse Wirkung erzielt wurde, die strategischen Ziele des Bundesrates sich bewährt haben und die Schweiz besser auf Cyber-Risiken vorbereitet ist als 2012. Durch die NCS wurden die bestehenden Strukturen und Prozesse weiter ausgebaut, weiterentwickelt und neue dazu definiert, damit die Zusammenarbeit, Kooperation und Kommunikation der relevanten Akteure gestärkt werden konnte und bei Bedarf weitere Akteure in der Zukunft eingebunden werden können.

Der Anstieg der Cyber-Angriffe 2016 hat wiederum verdeutlicht, dass wir weiterhin wachsam bleiben müssen und die gut etablierte Kooperation mit unseren nationalen und internationalen Partnern weiter vertieft werden muss. Es gilt auch in Zukunft, die wertvolle Zusammenarbeit mit den Betreibern von kritischen Infrastrukturen, der Wirtschaft und den Kantonen zu intensivieren und den Informationsaustausch mit den Polizeiorganisationen und Staatsanwaltschaften sowie IKT-Leistungserbringern, Systemlieferanten, Fachbehörden und Regulatoren stetig weiter zu stärken, damit die Resilienz der Schweiz erhöht werden kann.

Auch auf der internationalen Ebene war die Schweiz erneut aktiv. Die Schweiz hat sich für die Schaffung eines normativen Regelwerkes eingesetzt, 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.

Die Zukunft wird weitere Herausforderungen mit sich bringen. Die Bedrohungen haben sich in den letzten Jahren deutlich verschärft, wandeln sich stetig und haben auch im letzten Jahr gezeigt, dass die Bedrohungen von heute nicht denjenigen von morgen entsprechen. Deshalb muss die Schweiz auch für die kommenden Cyber-Bedrohungen gut vorbereitet sein. Die Massnahmenverantwortlichen und die Akteure aus Bund und Kantonen sind sich einig, dass die Resultate der NCS auch über den Zeithorizont von 2017 hinaus gewährleistet sein müssen. Daher erarbeitet der STA NCS eine Auslegeordnung zur Weiterentwicklung der Strategie, die dem Bundesrat unterbreitet wird.

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

Vorstoss Ip. = Interpellation; Mo. = Motion; Po. = Postulat; An. = Anfrage	Eingereicht am:	Stand per 31.12.2015:
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	erledigt
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. Cyber-Krieg und Cyber-Kriminalität. Wie gross sind die Bedrohungen, und mit welchen Massnahmen können sie bekämpft werden?	22.03.2013	erledigt
13.5224 Fra. Reimann. Zur Präsenz von US-Geheimdiensten und ihren Cyber-Schnüffelaktivitäten in der Schweiz	10.06.2013	erledigt
13.3558 Ip. Eichenberger. Cyber-Spionage: 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
13.5325 Fra. Sommaruga. Verwendet der Nachrichtendienst des Bundes illegal von der NSA beschaffte Daten?	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 Cyber-Raum-Strategie	17.09.2013	im Plenum noch nicht behandelt
13.3773 Ip. FDP-Liberale Fraktion. Zukunftstaugliches Fernmeldegesetz. Für eine übergreifende Cyber-Raum-Strategie	24.09.2013	im Plenum noch nicht behandelt

Vorstoss Ip. = Interpellation; Mo. = Motion; Po. = Postulat; An. = Anfrage	Eingereicht am:	Stand per 31.12.2015:
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 umzusetzen.“)	05.11.2013	erledigt
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
14.3654 Ip. Derder. Digitale Sicherheit. Sind wir auf dem Holzweg?	20.06.2014	im Plenum noch nicht behandelt
14.5569 Frau. Leutenegger. NSA. Ein Jahr Schnüffelstaat	26.11.2014	erledigt
14.4138 Ip. Noser. Beschaffungspraxis bei kritischen IKT-Infrastrukturen	10.12.2014	im Plenum noch nicht behandelt
14.1105 An. Buttet. Mittel zur Verteidigung des Cyber-Raums in der schweizerischen Sicherheitspolitik	10.12.2014	eingereicht
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
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
15.5299 Fra. Leutenegger. Schutz vor NSA-Spionage	09.06.2015	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
15.1059 Berberat. Dringende Finanzhilfe des Bundes infolge des Cyber-Angriffs auf TV5 Monde	10.09.2015	erledigt
15.4073 Ip. Derder. Ist die Armee wirklich in der Lage, den Schweizer Cyberspace zu schützen?	25.09.2015	im Plenum noch nicht behandelt
16.3186 Mo. Eichenberger. Cyberrisiken. Austausch technischer Informationen	17.03.2016	erledigt

Vorstoss Ip. = Interpellation; Mo. = Motion; Po. = Postulat; An. = Anfrage	Eingereicht am:	Stand per 31.12.2015:
16.3348 Po. Béglé. Schaffung eines Rates für Cyberverteidigung. Vordringlich für unsere Souveränität und unsere Sicherheit	27.04.2016	im Plenum noch nicht behandelt
16.3353 IP. Salzmann. Zweck des Sicherheitsverbundes Schweiz	30.05.2016	im Plenum noch nicht behandelt
16.3356 Ip. Nordmann. Endlich Finanzen und Personal auf den Kampf für Cybersicherheit umverteilen	31.05.2016	im Plenum noch nicht behandelt
16.3363 Ip. Glättli. Cyber-Attacke auf Ruag und VBS. Die notwendigen Konsequenzen ziehen!	31.05.2016	erledigt
16.3364 Ip. Glanzmann-Hunkeler. Aufklärung des Cyber-Angriffs auf die Ruag	31.05.2016	erledigt
16.1020 Dringliche Anfrage Fraktion BD. Kontrollsystem und Kompetenzzentrum als zukunftsweisende Instrumente im Kampf gegen Cyberrisiken	02.06.2016	erledigt
16.1021 Dringliche Anfrage Grüne-Fraktion	02.06.2016	erledigt
16.1022 Dringliche Anfrage CVP-Fraktion. Aufklärung des Cyberangriffs auf die Ruag	02.06.2016	erledigt
16.1024 Anfrage Knecht. Interpol, Cyberrisiken und Cyberkriminalität	07.06.2016	erledigt
16.3413 Ip. Heim. Cyberrisiken und Nuklearanlagen	09.06.2016	erledigt
16.3528 Mo. Glanzmann-Hunkeler. Kompetenzen bei der Cyberdefence	16.06.2016	im Plenum noch nicht behandelt
16.3561 Ip. Dittli. Erklärung der NATO. Hackerangriffe können einen Bündnisfall auslösen	17.06.2016	erledigt
16.061 Geschäft des Bundesrates. Sicherheitspolitik der Schweiz. Bericht	24.08.2016	im Plenum noch nicht behandelt
16.3706 Po. Vonlanthen. Digitale Wirtschaft und Arbeitsmarkt	27.09.2016	angenommen
16.4073 Po. Golay. Cyber-Risiken: für einen umfassenden, unabhängigen und wirksamen Schutz	15.12.2016	im Plenum noch nicht behandelt
16.4115 Ip. Quadranti. E-ID. Elektronische Identität	16.12.2016	im Plenum noch nicht behandelt.
16.5418 Fragestunde Glättli. Angriffe von Terroristen. Sicherheit der Atomkraftwerke?	21.09.2016	erledigt
16.1059 An. Glättli. Angriffe von Terroristen. Sicherheit der Atomkraftwerke?	28.09.2016	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