Juni 2015 / www.isb.admin.ch

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

Jahresbericht 2014 des Steuerungsausschusses NCS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Publikation: 5. Juni 2015

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 unter: http//www.isb.admin.ch/themen/01709/01891/index.html?lang=de

Inhaltsverzeichnis

Vorwort

Im Jahr 2014 wurden wieder Vorfälle und Attacken mit hochentwickelten Mitteln bekannt, die Staaten zugeordnet werden. Auch die ausgeklügelten Fähigkeiten der Cyberkriminellen mussten zur Kenntnis genommen werden. Zudem spielten hochverbreitete Lücken eine wichtige Rolle. Demzufolge wurde der Welt neben den Chancen der fortschreitenden Digitalisierung noch mehr bewusst, wie verletzlich das Internet und damit die eigenen Daten, die Privatsphäre und das Vertrauen in die Internettechnologie sind. Um dem gegenüberzutreten und den Schutz vor Cyber-Risiken sowie die Anforderungen an eine vertrauenswürdige Infrastruktur zu stärken, geht die Schweiz konsequent ihren Weg: Die Umsetzung der «Nationalen Strategie der Schweiz vor Cyber-Risiken (NCS)» wurde deshalb weiter vorangetrieben und dabei sind erste wichtige Ziele erreicht worden. Der vorliegende zweite Jahresbericht zur Umsetzung der NCS gibt ihnen einen detaillierten Überblick über die aktuelle Bedrohungslage, die eingeleiteten Massnahmen aus der NCS-Strategie und deren Umsetzungsstand.

Die Schweiz steht mit den Herausforderungen zum Schutze des Internets nicht alleine da, die Bedrohungen sind grenzüberschreitend. Daher sind internationale Kooperationen wichtiger denn je. Im Rahmen des Schweizer Vorsitzes der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) wurden vertrauensbildende Massnahmen entwickelt, die für das gemeinsame Verständnis über Sicherheit im Internet enorme Wichtigkeit haben. Mit verschiedenen Staaten wurden Abkommen zum Austausch über Sicherheitslücken und Vorfälle getroffen sowie bereits bestehende Partnerschaften ausgebaut. Dadurch konnte die gegenseitige Information zu Cybervorfällen weiter optimiert werden.

Auch innerhalb der Schweiz muss der Kampf gemeinsam angegangen, das Wissen miteinander geteilt werden. Daher wurde im Schulterschluss von MELANI mit der IKT-Industrie und Forschungspartnern das Kompetenznetzwerk «Swiss Cyber Experts» gegründet.

Das bereits Erreichte ist wichtig, die Arbeiten bei der NCS-Umsetzung sind aber noch lange nicht abgeschlossen. Auch in 2015 werden wir alle notwendigen Schritte einleiten, damit die Schweiz das Internet weiterhin als sicheren und zensurfreien Raum für Wirtschaft, Behörden und Bürger nutzen kann. Das ist und bleibt unser aller Anspruch im digitalen Lebensraum.

Peter Fischer
Delegierter für die Informatiksteuerung des Bundes (ISB)

1 Management Summary

Der Bundesrat hat am 27. Juni 2012 die «Nationalen Strategie der Schweiz vor Cyber-Risiken (NCS)» und am 15. Mai 2013 deren Umsetzungsplan (UP NCS) verabschiedet. Die NCS mit ihren sechszehn Massnahmen fokussiert insbesondere auf die frühzeitige Erkennung vor Cyber-Risiken und Bedrohungen sowie auf eine Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen. Ebenfalls bezweckt sie eine generelle Reduktion von Cyber-Bedrohungen, insbesondere Cyber-Spionage, Cyber-Sabotage und Cyber-Kriminalität.

Für die Umsetzung der einzelnen Massnahmen ist jeweils einem Bundesamt die Federführung übertragen worden. Um die 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. Der Bundesrat hat zudem einen Steuerungsausschuss NCS (STA NCS) beauftragt, die Umsetzung mit einem strategischen Controlling zu begleiten.

Die 16 Massnahmen betreffen vier Bereiche: Prävention, Reaktion, Kontinuität und unterstützende Prozesse. In allen Bereichen konnten im vergangenen Jahr nicht zuletzt dank einer engen Zusammenarbeit und guten Kommunikation wichtige Ziele erreicht werden.

Bei der Prävention wurden in sechs kritischen Teilsektoren Verwundbarkeitsanalysen durchgeführt oder begonnen (Informationstechnik, Strassenverkehr, Erdgasversorgung, Behörden, Blaulichtorganisationen, Zivilschutz) sowie ein Konzept zum Erfassen von Verwundbarkeiten der Informations- und Kommunikationstechnik (IKT) auf Bundesebene erstellt. Um Risiken zu erkennen, ist es zwingend notwendig, die aktuelle Bedrohungslage zu kennen und ein vollständiges Lagebild zu haben. Für Letzteres wurde ein technisches Lagebild aufgebaut, das eine Übersicht über die kritischen Infrastrukturen in der Schweiz liefert und den Betreibern dadurch ermöglicht, infizierte Geräte im eigenen Netz rasch zu erkennen. Die wichtigsten Cyber-Bedrohungen in 2014 werden durch den MELANI Halbjahresbericht und den KOBIK Jahresbericht erfasst und aufgezeigt.[1]

Im Bereich Reaktion wurden im vergangenen Jahr die Kompetenzzentren zur Analyse von Schadsoftware (z. B. GovCERT.ch, CISIRT-BIT, milCERT-VBS) ausgebaut. Dadurch kann eine dauernde Bereitschaft gewährleistet werden. Im Falle von komplizierten und technisch anspruchsvollen Cyber-Vorfällen kann künftig zudem auf das Fachwissen des Vereins der «Swiss Cyber Experts», zurückgegriffen werden. Dies dank der zwischen dem Verein und MELANI in 2014 geschlossenen Kooperationsvereinbarung.

Bei der Kontinuität wurden auf der Basis einer der abgeschlossenen Verwundbarkeitsanalysen der kritischen Teilsektoren Schritte zur Etablierung eines Kontinuitäts- und Krisenmanagements eingeleitet. Ziel ist eine Branchenvereinbarung, in der sich die versorgungsrelevanten Unternehmen zur gegenseitigen Unterstützung im Falle von Cyber-Vorfällen verpflichten.

Im Bereich der unterstützenden Prozesse wurde die internationale Zusammenarbeit auf bilateraler und multilateraler Ebene gestärkt. Auf multilateraler Ebene beteiligte sich die Schweiz, die den OSZE-Vorsitz im vergangenen Jahr innehatte, an deren vertrauensbildenden Massnahmen. Auf bilateraler Ebene wurden zudem bestehende Kontakte intensiviert und neue geknüpft.

Um die Wirksamkeit der 16 Massnahmen zu überprüfen, wird ab 2015 eine Wirksamkeitsüberprüfung vorbereitet, deren Ergebnisse als Basis für die Entscheide des Bundesrates zum weiteren Vorgehen nach 2017 dienen.

[1] Das Jahr 2014 war primär geprägt vom Erkennen und Aufdecken von Trojanern und Sicherheitslücken, die die NCS-Umsetzung beeinflusst haben und in Zukunft noch weiter beeinflussen werden. Diese waren: «Heartbleed» - Sicherheitslücke in einer der wichtigsten Verschlüsselungsbibliotheken, «Cryptolocker» – Tückische Erpressersoftware auf dem Vormarsch, «Regin» – Hoch komplexe Spionagesoftware.

2 Zusammenarbeit

In diesem Kapitel werden einige wichtige Eckdaten der nationalen und internationalen Zusammenarbeit aufgeführt.

2.1 Nationale Ebene

Am 20. März 2014 konnte mit der zweiten Cyber-Landsgemeinde des Sicherheitsverbundes Schweiz (SVS) die Zusammenarbeit und Vernetzung zwischen Bund und den Kantonen weiter gestärkt werden. Rund 70 Interessierte aus Bund und Kantonen nahmen an der Veranstaltung teil. Im Fokus standen die laufenden Projekte auf Kantonsebene sowie Information über den aktuellen Stand der Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)».

Am 26. März 2014 wurde der Verein der «Swiss Cyber Experts» unter Beteiligung von MELANI gegründet und am 17. Dezember die Kooperationsvereinbarung zwischen dem Verein und MELANI unterzeichnet. Auf dieser Basis wird im Falle von schweren Cyber-Vorfällen der Zugang zu weiteren Fachressourcen koordiniert.

Ziel der ersten Tagung NCS vom 20. November 2014 war der Informationsaustausch über die Aktivitäten von Verwaltung und Wirtschaft zur Minimierung von Cyber-Risiken in der Schweiz, insbesondere bei den kritischen Infrastrukturen sowie über den aktuellen Stand der Umsetzung der NCS. Rund 150 Vertreterinnen aus Bund, Kantonen und der Wirtschaft haben an der Veranstaltung teilgenommen.

Vom 3. bis zum 21. November 2014 fand die Sicherheitsverbundsübung 2014 (SVU 14) statt. Sie untersuchte mit dem Szenario «Pandemie und Strommangellage» die Zusammenarbeit der Partner im Sicherheitsverbund Schweiz. An der Übung haben 26 Kantone, Bundesstellen aller sieben Departemente, Armee, Krisenorganisationen und Privatwirtschaft teilgenommen. Der Schwerpunkt der Übung lag auf der politisch-strategischen Ebene, vom Krisenmanagement bis zur politischen Entscheidungsfindung. Die SVU 14 hat für alle Beteiligten bereits jetzt wertvolle Erkenntnisse gebracht, die weiter ausgewertet werden.

In periodischen Koordinationssitzungen unter der Leitung MELANI OIC (NDB) werden sich die einzelnen Akteure in Zukunft gemeinsam austauschen, um eine gesamtheitliche Analyse der Bedrohungslage sicherzustellen. Diese wird dann in einer grafischen Übersicht (Lageradar gesamtheitliche Bedrohung im Cyber-Bereich) dargestellt.

2.2 Internationale Ebene

Mit der Wahl von Thomas Schneider (Bundesamt für Kommunikation, BAKOM) zum Vorsitzenden des Government Advisory Committee (GAC) der Internet Corporation for Assigned Names and Numbers (ICANN) im Oktober 2014 erhält die Schweiz direkten Einfluss auf die Führung einer zentralen Ressource des Internet. Er war bislang Schweizer Regierungsvertreter im GAC und Vizepräsident sowie Umsetzungsverantwortlicher für die NCS-Massnahme 9. Das GAC ist das Beratende Gremium der Regierungen für die ICANN.

Vom 3. bis 6. November 2014 fand in Linz der zweite European Cyber Security Alpen Cup statt. Dies ist ein Länderübergreifender Wettkampf mit Schülern und Studenten aus der Schweiz, Österreich und Deutschland unter der Federführung von Cyber Security Austria unter Beteiligung des Verein Swiss Cyber Storm unter dem Patronat der Melde- und Analysestelle Informationssicherung (MELANI) des Bundes und dem Verein Swiss Police ICT. Das Ziel des Wettkampfes ist Auffinden, Ausnutzen und Beheben von Schwachstellen in IT Systemen.

An der OSZE-Konferenz vom 7. November 2014 in Wien unter dem Vorsitz der Schweiz reflektierten Vertreter der Privatwirtschaft, Zivilgesellschaft und Wissenschaft mit Regierungsvertretern den Stand der Implementierung des ersten Pakets von vertrauensbildenden Massnahmen (VBM). Sie identifizierten zudem weitere Bedürfnisse und Ideen für den zweiten Massnahmenkatalog. Die Schweizer NCS konnte im Rahmen der VBM 7 (Nationale Cyber-Programme und Strategien) eingebracht werden.

Vom 18. Bis 20. November 2014 wollten die NATO Staaten mit einer gross angelegten Übung ihre Fähigkeiten zur Abwehr von Cyber-Attacken testen. Erprobt wurden die Zusammenarbeit beim Umgang mit Angriffen aus dem Internet und die Koordination. Sieben nicht-NATO Mitgliedstaaten, darunter auch die Schweiz wurde dazu eingeladen.

Im Dezember 2014 veröffentlichte die ENISA die Studie: «Framework for Evaluating National Cyber Security Strategies».[2] Die Schweiz beteiligt sich an der ENISA «Cyber Expert Working Group», die zum Ziel hat, Nationale Cyber-Strategien zu vergleichen und dabei «best practices» und «guidance» zu identifizieren. In dieser Arbeitsgruppe sind neben der Schweiz achtzehn EU-Mitgliedsstaaten und 7 nicht EU - Mitgliedsstaaten vertreten.

Auf multilateraler Ebene hat die Schweiz den Sino-European Cyber-Dialog mitgestaltet. Dieser fand einmal in Genf und einmal in Peking statt. Die Schweiz hat den OSZE-Prozess erläutert und vorgeschlagen, vertrauensbildende Massnahmen zwischen den teilnehmenden europäischen Staaten und China zu entwickeln. Im Rahmen der UNO- engagierte sich die Schweiz insbesondere für den Schutz der Menschenrechte im Cyber-Raum, unter anderem als Mitglied der Kerngruppe zur Initiative «The Right to Privacy in the Digital Age», welche den Schutz der Privatsphäre im Cyber-Raum zu stärken sucht.

3 Stand der Umsetzungsarbeiten NCS 2014

Die NCS ist eine integrale Strategie, die mit ihren 16 Massnahmen einen umfassenden Ansatz verfolgt, um die Schweiz vor Cyber-Bedrohungen zu schützen. Die 16 Massnahmen gruppieren sich entsprechend ihrer zeitlichen Entfaltung und Abhängigkeiten in 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 zweiten Jahr der Umsetzung und die Arbeiten für die meisten Massnahmen sind weit fortgeschritten. In diesem Kapitel wird die Gesamtübersicht der Umsetzung erläutert. Mit allen verantwortlichen Stellen hat die Koordinationsstelle NCS die Ziele und Meilensteine für die jeweiligen Massnahmen konkret definiert und in einer Roadmap dargestellt (siehe Abbildung 1). Jede Stelle mit Umsetzungsverantwortung präsentiert in einem kurzen Bericht den aktuellen Umsetzungsstand der jeweiligen Massnahme(n). Die Umsetzungsarbeiten einiger NCS-Massnahmen erfolgen in Zusammenarbeit mit den Verantwortlichen für die «Strategie des Bundesrates für die Informationsgesellschaft in der Schweiz» und der «Nationalen Strategie zum Schutz kritischer Infrastrukturen».

[2] https://www.enisa.europa.eu/media/enisa-auf-deutsch/

Roadmap NCS

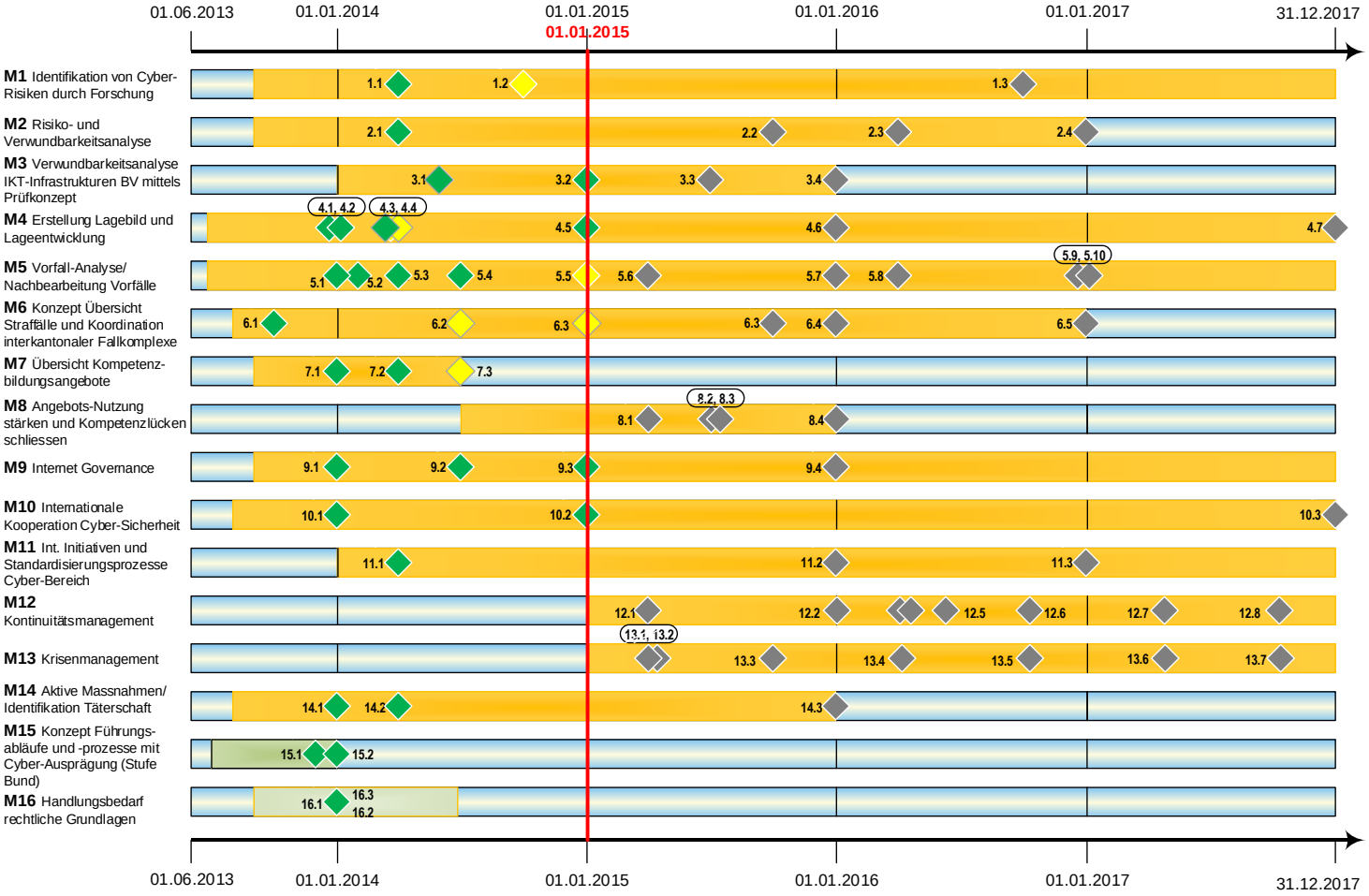

Abbildung 1: Roadmap NCS

Legende: Stand Meilensteine

- Meilenstein gefährdet
- Meilenstein verzögert
- Meilenstein planmässig in Umsetzung
- Meilenstein Umsetzung noch nicht begonnen

3.1 Prävention

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

3.1.1 Massnahme 2: Risiko- und Verwundbarkeitsanalyse

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

Ziel der Risiko- und Verwundbarkeitsanalyse 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.

Aktueller Stand:

Für die erste Gruppe von Teilsektoren wurden im Bundesamt für wirtschaftliche Landesversorgung (BWL) und im Bundesamt für Bevölkerungsschutz (BABS) Verwundbarkeitsanalysen durchgeführt. Abgeschlossen wurde die Erdgasversorgung (BWL, Oktober 2014). Die Arbeiten in den Teilsektoren Informationstechnologien und Strassenverkehr (BWL) sind weit fortgeschritten. Die Analysen zu den Teilsektoren Parlament, Regierung, Justiz und Verwaltung, Zivilschutz und Blaulichtorganisationen (BABS) wurden begonnen und sind gemäss Umsetzungsplan auf Kurs.

Der Prozess zur Durchführung der Analysen und damit die Koordination zwischen den beteiligten Akteuren aus Wirtschaft und Verwaltung wurde aufeinander abgestimmt.

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 Prüfkonzept zur periodischen Überprüfung der IKT-Infrastrukturen der Bundesverwaltung auf systemische, organisatorische und technische Schwächen zu erstellen.

Aktueller Stand:

Im ersten Schritt wurde die Aufgabenstellung analysiert und eine Eingrenzung des Einsatzfeldes des Prüfkonzepts M3 vorgenommen. Im zweiten Schritt wurden die bisherigen Verwundbarkeitsanalysen in der Bundesverwaltung, Schnittstellen zu ähnlichen Vorhaben sowie die Verantwortlichkeiten identifiziert. Eine Risikoanalyse für die Umsetzung des Prüfkonzepts M3 sowie die Identifizierung der wichtigsten Fragestellungen wurde erarbeitet. Auf dieser Basis konnte der erste Entwurf des Prüfkonzepts erstellt werden.

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 Entwicklungen im Cyber-Bereich informiert und Gefahren- und Schadenspotenziale von Cyber-Angriffen für die jeweiligen kritischen Sektoren und deren Relevanz für die Schweiz beschreibt.

Ziel der NCS ist es, in enger Zusammenarbeit mit allen Akteuren ein einheitliches Lagebild zu erstellen. Alle relevanten Informationen aus technischen Analysen, sowie aus nachrichtendienstlichen und polizeilichen Quellen fliessen dazu in das Lagebild ein.

Aktueller Stand:

Die Umsetzungsarbeiten zur Erstellung eines einheitlichen Lagebildes haben begonnen und ein Prototyp zur Darstellung der Bedrohungslage wurde erstellt. Auch wurden die Bestandsaufnahme und die Überprüfung der bestehenden Prozesse zur Erstellung der Bedrohungslage, der organisatorischen Abläufe sowie der Verantwortlichkeiten erfasst. Der daraus abgeleitete Bedarf an Prozessen und Regulierung ist unter Berücksichtigung der Prioritäten ebenfalls erhoben worden.

Ein wichtiger Meilenstein wurde bei der Erstellung des Lagebildes erreicht, indem ein Bericht über den aktuellen Stand des technischen Lagebildes erstellt wurde. Somit kann einerseits eine Zuordnung von infizierten Geräten und anderseits ein technisches Lagebild über die Infektionen erstellt werden.

Per Ende 2014 übernimmt das OIC MELANI gemäss der Umsetzung M4 den Lead bei der Koordination der einzelnen, operativen und technischen Akteure (GovCERT, FUB-ZEO CNO, Cyber NDB, BIT-CSIRT, MilCERT und Cyber MND) zwecks gesamtheitlicher Analyse der Bedrohungslage und Koordination bei der Behandlung von Vorfällen.

3.2 Reaktion

Im Bereich Reaktion muss eine koordinierte Vorfall-Analyse und Nachbearbeitung erfolgen, um einen Vorfall so rasch wie möglich zu beheben. Die NCS sieht 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 kann und eine Täterschaft schneller identifiziert werden kann (M5, M6, M14).

3.2.1 Massnahme 5: Vorfall-Analyse und Nachbearbeitung von Vorfällen

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

Das bei MELANI angesiedelte GovCERT ist schon seit Jahren im Bereich Malware-Analyse aktiv. Diese technischen Kapazitäten und das Spezialwissen sollen nun mit der NCS ausgebaut werden. Dazu gehören eine Erhöhung der Bereitschaftszeit und Steigerung der Reaktionsfähigkeit aller CERTs sowie deren Vernetzung untereinander. Zur besseren Kontextualisierung von Vorfällen und der Einschätzung ihrer Relevanz, wurde das OIC MELANI weiter ausgebaut. Im Bereich staatschutzrelevanter Vorfälle, verfügt der NDB mit dem Aufbau des Cyber NDB nun über die nötigen Ressourcen und Fähigkeiten.

Aktueller Stand:

Die Bereitschaft im GovCERT konnte gesteigert werden und die optimale Verfügbarkeit im Normalbetrieb sichergestellt werden. Durch die engen Kontakte und Vernetzung zu verwandten Stellen (weitere CERTs in der Bundesverwaltung) können im Falle einer Krise weitere Fachpersonen aus der Bundesverwaltung hinzugezogen werden, um die Krise zu bewältigen. Zusätzlich können nun auch Experten aus dem neu gegründeten Verein «Swiss Cyber Experts» beigezogen werden. Im Bereich der Bearbeitung staatschutzrelevanter Vorfälle, wurde im NDB eine neue Einheit aufgebaut und mit den von der NCS gesprochenen Ressourcen versehen.

Zwischen der FUB (MilCERT und Computer Network Operations (CNO)), dem NDB (Cyber NDB), dem MND (Cyber Defence), dem BIT (CSIRT) ist die operative Zusammenarbeit bei der Bewältigung von Cyber-Vorfällen in der Bundesverwaltung weiter systematisiert und die Instrumentierung für den Informationsaustausch mit einem periodischem Koordinationsmeeting unter der Leitung von MELANI weiter ausgebaut worden. Die Armee hat die eigenen Detektions- und Analysemittel verstärkt.

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 zur Bekämpfung der Cyber-Kriminalität. Zu diesem Zweck wurde in M6 der NCS festgehalten, dass die im eidgenössischen Justiz- und Polizeidepartement (EJPD) angesiedelte KOBIK in Zusammenarbeit mit den Kantonen per Ende 2016 ein Konzept «Fallübersicht und Koordination interkantonaler Fallkomplexe» vorlegt.

Aktueller Stand:

Die Bestandsaufnahme zur Bekämpfung der Cyber-Kriminalität in der Schweiz konnte Ende Juni 2014 durch einen Fragebogen für Polizei und Staatsanwaltschaften im Bund und den Kantonen geklärt werden. Auch wurde eine Überprüfung der bestehenden Prozesse, der organisatorischen Abläufe sowie der Verantwortlichkeiten der Strafverfolgungsbehörden von Bund und Kantonen durchgeführt. Rechtliche Aspekte konnten geklärt werden. Somit wurde eine solide Basis des Konzeptentwurfes geschaffen. Ein erster Entwurf des Konzeptes zur Übersicht der Straffälle liegt vor.

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) sollen 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:

Der am 1. Januar 2014 neu gegründete Bereich Cyber im NDB ist für die Bearbeitung von entsprechenden nachrichtendienstlich relevanten Informationen zuständig. Er hat seine Arbeiten begonnen, ist voll funktionsfähig und hat 80% der Stellen bereits besetzt. Somit verläuft die Umsetzung der Meilensteine der NCS beim Cyber NDB planmässig. Die Schnittstellen mit dem OIC MELANI sind etabliert und der Informationsaustausch wurde etabliert. Die Anbindung der technischen Fähigkeiten der FUB zur Unterstützung des Cyber NDB ist mit der Unterzeichnung des Service Level Agreements (SLA) erfolgt. Es regelt die entsprechende Zusammenarbeit.

3.3 Kontinuitäts- und Krisenmanagement

Die gezielte Durchführung eines Krisenmanagements setzt klar definierte Führungsabläufe und -prozesse für den Cyber-Fall voraus. Das Kontinuitätsmanagement sorgt dafür, dass die Geschäftsprozesse auch während einer Krise verfügbar sind (M12, M13, M15).

3.3.1 Kontinuitätsmanagement (M12)

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

Auf Grundlage der Ergebnisse der Risiko- und Verwundbarkeitsanalyse (Massnahme 2) definieren das federführende BWL und das BABS mit den relevanten Unternehmen und zuständigen Fachstellen die notwendigen Massnahmen zur Sicherstellung der Kontinuität.

Aktueller Stand:

Die Meilensteine für das weitere Vorgehen bei der Massnahme 12 wurden bis 2017 festgelegt und in der Roadmap visualisiert. Die Bearbeitung der beiden Massnahmen M12 und M13 erfolgt gleichzeitig. Das Vorgehen wird dabei in einer ersten Phase mit den ersten Teilsektoren erprobt und ein dazugehöriges methodisches Vorgehen durch das BABS und das BWL definiert und abgesprochen.

Das BWL konnte mit Vertretern der Gaswirtschaft konkrete Schritte zur Etablierung eines Kontinuitätsmanagements einleiten. Ziel ist die Unterzeichnung einer Branchenvereinbarung, in der sich die versorgungsrelevanten Unternehmen zur gegenseitigen Unterstützung im

Falle eingetretener Cyber-Risiken verpflichten. Insbesondere sollen mit der Vereinbarung die in der Verwundbarkeitsanalyse erkannten Abhängigkeiten von Kommunikationsmitteln und qualifizierten Arbeitskräften adressiert werden. Ein Entwurf einer Vereinbarung befindet sich in der Vernehmlassung bei der Gaswirtschaft (Oktober 2014).

3.3.2 Massnahme 13: Krisenmanagement

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

Mit Massnahme 13 sollen die kritischen Infrastrukturen und der Bund die notwendigen Prozesse zur Bewältigung einer durch Cyber-Risiken verursachten ausserordentlichen Lage definieren. Die Arbeiten stützen sich dabei auf die Erkenntnisse der Risiko- und Verwundbarkeitsanalysen (Massnahme 2). Im Krisenmanagement ist zwischen einer strategischen- und einer operativen Ebene zu unterscheiden. Für die Definition der Prozesse auf strategischer Ebene sind das BWL und das BABS zuständig, für diejenigen der operativen Ebene MELANI. Weiter ist zu beachten, dass die Massnahme 13 komplementär zur Massnahme 12 ist und im Sinne des „Business Continuity Management (BCM)“ zu verstehen ist und nicht im klassischen Krisenmanagement.

Aktueller Stand:

Die Meilensteine für das weitere Vorgehen der Massnahme 13 wurden bis 2017 festgelegt und in der Roadmap visualisiert. Die Bearbeitung der beiden Massnahmen 12 und 13 erfolgt gleichzeitig. Das BWL konnte in Zusammenarbeit mit Vertretern der Schweizer Erdgasversorger bereits konkrete Schritte zur Etablierung eines Kontinuitäts- und Krisenmanagements einleiten (siehe oben).

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

Zuständigkeit: BK

Mit der Massnahme 15 soll das allgemeine Krisenmanagement mit den Cyberaspekten ergänzt werden.

Aktueller Stand:

Das Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung ist erstellt und in Umsetzung und wurde vom Steuerungsausschuss NCS (STA NCS) im Februar 2014 abgenommen.

Das Konzept zur Massnahme 15 ist erstellt. In der Arbeitsgruppe 3 des KKM SVS: *Krisenmanagement* wurde das Konzept erweitert und schliesst nun die Kantone ein. Anhand eines geeigneten Szenarios soll nun die Effektivität dieses Konzeptes evaluiert und gegeben falls angepasst werden (siehe Kapitel 3.6).

3.4 Unterstützende Prozesse

Als Grundlagen und Prozesse für die Bewältigung der Cyber-Problematik sind umfassende internationale Kooperationen, der Austausch von Erfahrungen im Bereich Bildung und Forschung sowie gegebenenfalls eine Anpassung von gesetzlichen Grundlagen notwendig (M1, M7, M8, M9, M10, M11, M16). Hierzu wurden folgende Massnahmenpakete gebildet:

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

Zudem erlaubt es die neu gegründete Fachgruppe Cyber-International, eine Übersicht über

die einzelnen Aktivitäten, Prozesse und Initiativen mit internationalem Geltungsbereich zu schaffen und den interdepartementalen Informationsfluss zu fördern.

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 Forschung (sowohl Grundlageforschung als auch angewandte Forschung) im Bereich Schutz vor Cyber-Risiken gefördert. Verantwortlich für die Umsetzung ist das SBFI in Zusammenarbeit mit der KS NCS.

Aktueller Stand:

Das SBFI hat einen Steuerungsausschuss „Forschung im Bereich Schutz vor Cyber-Risiken“ etabliert. Der Steuerungsausschuss gibt die generelle Stossrichtung für die Forschung vor, definiert Kriterien zur Vergabe von Forschungsprojekten und führt eine Datenbank von Forschenden zu den Themen Cyber-Risiken.

Um das benötigte Fachwissen zur Forschung im Bereich Cyber-Risiken zu gewinnen, wird der Forschungsausschuss einen Cyber-Expertenpool (aus Vertretern der Forschung und ausgewählten Wirtschaftsvertretern) ernennen. Der Expertenpool berät den Steuerungsausschuss in fachlichen Fragen und trägt insbesondere zur Identifizierung und Priorisierung der Forschungsthemen bei.

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:

Im ersten Schritt wurde eine Übersicht der bestehenden Kompetenzbildungsangebote zum Schutz vor Cyber-Risiken erstellt. Das Ziel der Übersicht ist es, eine Basis für die Identifikation der Best Practice Beispiele für die definierten Zielgruppen aus Wirtschaft, Verwaltung und Bevölkerung zu haben. Weiter wurde ein Kurzbericht zur Identifizierung qualitativ hochstehender Kompetenzbildungsangebote durch Expertenempfehlungen erstellt Möglichkeiten zur Publikation der identifizierten Angebote (evt. in Zusammenarbeit mit Dritten) werden überprüft. Lücken in der Angebotslandschaft im Hinblick auf den Umgang mit Cyber-Risiken identifizierte das international institute for management in technology der Universität Fribourg (iimt) im Auftrag des Bundes. Der Bericht wird im 2015 publiziert.

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

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

Mit der Massnahme 8 sollen einerseits bestehende Kompetenzbildungsangebote im Umgang mit Cyber-Risiken ausgebaut und andererseits die Schliessung der erkannten Angebotslücken erarbeitet werden. Der Fokus liegt auf Kompetenzbildungsangeboten die für die Betreiber kritischer Infrastrukturen relevant sind. Die Umsetzungsarbeiten erfolgen jedoch in enger Abstimmung mit den Verantwortlichen der «Strategie des Bundesrates für eine Informationsgesellschaft» in der Schweiz. Verantwortlich für die Umsetzung ist die KS NCS in Zusammenarbeit mit dem SBFI, dem BAKOM, dem EDA und dem BSV.

Aktueller Stand:

Massnahme 8 basiert auf den Ergebnissen von Massnahme 7. Mit dem Abschluss von Massnahme 7 wurden nun die Meilensteine zur Schliessung von erkannten Angebotslücken bis Dezember 2015 definiert und in der Roadmap visualisiert. Der Steuerungsausschuss „Forschung im Bereich Cyber-Risiken“ unter der Leitung des SBFI (vgl. 3.4.1) hilft mit den von ihm ernannten Expertenpool mit, weitere Lücken zu identifizieren und Angebote zu schaffen, um die vorhandenen Lücken zu schliessen.

3.4.4 Massnahme 9: Internet Governance

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

Mit der Massnahme 9 der NCS soll sich die Schweiz (Wirtschaft, Gesellschaft, Behörden) aktiv und soweit wie 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 an den relevanten nationalen und internationalen Prozessen teil.

Aktueller Stand:

Das BAKOM hat eine Übersicht zu den prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet Governance.[3] sowie einen Bericht zu den Prioritäten der Schweiz in der Internet Governance und der Einbindung von relevanten Akteuren erstellt.

Die Schweiz beteiligt sich aktiv an den Arbeiten der der Internet Cooperation for Assigned Names and Numbers (ICANN). Seit Ende Oktober präsidiert ein Schweizer[4] den ICANN-Regierungsbeirat.

Weiter unterstützt das BAKOM die Vorbereitung und Durchführung des «Internet Governance Forum (IGF)», ist Mitinitiator und Mitorganisator des europäischen IGF-Dialogforums «EuroDIG (European Dialog on Internet Governance)» und arbeitet aktiv in den Expertengruppen des Europarats sowie der «Commission on Science and Technology for Development (CSTD)» mit.

Auf nationaler Ebene organisiert das BAKOM regelmässig die Diskussionsplattform «Plateforme Tripartite zum WSIS[5] Follow-up», welche einen Informationsaustausch aller Interessengruppen (Bundesverwaltung, Zivilgesellschaft, Akademie) zu aktuellen Themen und Entwicklungen in Bezug auf das Internet ermöglicht. In Zusammenarbeit mit dem EDA und der DiploFoundation wurde zudem die Geneva Internet Platform (GIP) ins Leben gerufen.[6]

3.4.5 Massnahme 10: Internationale Kooperation Cyber-Sicherheit

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

[3] Diese Übersicht wurde auf CH@World veröffentlicht und wird regelmässig aktualisiert.

[4] Thomas Schneider, BAKOM

[5] World Summit on the Information Society

[6] http://www.giplatform.org/about-gip

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:

Im Kern der Aktivitäten 2014 stand die Förderung von vertrauensbildenden Massnahmen (Confidence Building Measures) im Cyber-Raum, um die Sicherheit, Transparenz und die Vorhersehbarkeit von Cyber-Bedrohungen zu erhöhen. Als OSZE Vorsitzende konnte die Schweiz die Implementierung des ersten Massnahmenpakets und dessen Bekanntmachung in anderen Foren fördern. So hat die Schweiz unter anderem die eigene nationale Strategie präsentiert und eine Auslegeordnung existierender Cyber-Terminologien in Auftrag gegeben. Die Weiterentwicklung des Massnahmenkataloges wurde vorangetrieben, indem neue Vorschläge, die auf eine Stärkung der Kooperation abzielen, mit Deutschland erarbeitet wurden.

Im UNO-Rahmen engagierte sich die Schweiz insbesondere für den Schutz der Privatsphäre im Cyber-Raum. Im Bereich des Kapazitätsaufbaus setzte sich die Schweiz dahingehend ein, dass Entwicklungsländer an internationalen Prozessen bezüglich Cybersicherheit teilnehmen können.

Weiter wird der Austausch im Rahmen von bilateralen Konsultationen vorangetrieben, um die Schweizer Interesse zu fördern.

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 (SDOs) und anderen zielführenden Initiativen zu optimieren.

Aktueller Stand:

Im Rahmen der Umsetzung der Massnahme 11 zur NCS hat das BAKOM zwei Übersichtstabellen erstellt. Eine erste Tabelle listet die Akteure der Massnahme11 auf, die das Geschehen in internationalen Organisationen und Initiativen in Fragen der Cyber Security verfolgen und beeinflussen. Die zweite Tabelle enthält die internationalen Organisationen und Initiativen, die den Akteuren der Massnahme 11 als wichtig erscheinen. Im ersten Erarbeitungsprozess wurden 34 Behörden, Fachämter und Regulatoren eingeladen und aufgrund derer Rückmeldungen weitere 90 privatwirtschaftliche Unternehmen, Verbände und Bildungseinrichtungen. Die daraus resultierende Auflistung ist allerdings nicht abgeschlossen. Entsprechend sind alle Teilnehmer jederzeit aufgerufen, weitere nationale Experten und internationale Organisationen zu nennen, die im Sinne der Massnahme11 jeweils relevant erscheinen.

3.4.7 Massnahme 16: Handlungsbedarf rechtliche Grundlagen

Zuständigkeiten: KS NCS

Die 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 relevanten Rechtsgrundlagen wurden erhoben und die Massnahme wurde vom Steuerungsausschuss NCS (STA NCS) im August 2014 abgenommen. Die Koordinationsstelle NCS hat mit allen zuständigen Bundesstellen eine Übersicht der relevanten Rechtsgrundlagen in Bereichen mit Cyber-Ausprägung erfasst und dabei auch abgeklärt, ob ein vordringlicher Gesetzgebungs- und Revisionsbedarf besteht. Der aktuell bekannte Rechtssetzungsbedarf wird in laufenden ordentlichen Gesetzgebungsverfahren behandelt. Ein darüber hinausgehender, dringender Rechtsetzungsbedarf besteht nicht. Es ist aber festzuhalten, dass dies nur eine Momentaufnahme ist und die sich verändernde Risikolandschaft in Zukunft zu neuem rechtlichem Handlungsbedarf führen kann.

3.5 Umsetzungsaktivitäten der Armee

Die Armee gehört zu den kritischen Infrastrukturen des Landes, für welche der Cyber-Raum und die Cyber-Bedrohungen zentrale Themen geworden sind. Mit der rasanten Entwicklung und der zunehmenden Wichtigkeit des Cyber-Raumes ergeben sich neue operationelle Optionen, die in den militärischen Operationen zur 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.

Aufgrund der obengenannten Bedürfnisse verfügt die Armee 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. Von hoher Bedeutung für die Armee bleibt die Ausklammerung des Kriegs- und Konfliktfalles aus der NCS (s. Kapitel 3.4) und ihre Beauftragung, sich für diesen Spezialfall vorzubereiten.

Aktueller Stand:

Basierend auf der Konzeptionsstudie Cyber-Defence (KS CYD) von 2013 wurde eine doktrinale Grundlage geschaffen, die es erlaubt, die Definition eines in der Armee und mit ihren Partnern einheitlichen Verständnisses ihrer Aufgaben im Cyber-Raum zu schaffen. Die methodischen Grundsätze für ein modernes Cyber-Risiko-Management und ein wirksames Krisen-Management wurden geschaffen und werden laufend weiterentwickelt. Die Zusammenarbeit der Armee mit ihren kritischen Partnern und Leistungserbringern hat sich weiterentwickelt und hat dazu geführt, dass im Bereich der Antizipation und des Cyber-Lagebildes wichtige Meilensteine realisiert werden konnten.

2015 sind die Weiterentwicklung der dedizierten Ressourcen und die Konkretisierung des Umsetzungsplanes der NCS vorgesehen. Die genaue sicherheitspolitische Definition der zur erbringenden Leistungen der Armee zu Gunsten der zivilen Behörden und der Betreiber kritischen Infrastrukturen, sowie ihre Verantwortung im Konflikt- und Kriegsfall konnte noch nicht präzisiert 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 NCS-Massnahme 3 wurde ein Fragebogen zur Selbstüberprüfung von Cyber-Risiken erarbeitet.

Eine Prozessbeschreibung zur Bearbeitung von Cybervorfällen wurde erarbeitet. Einer von fünf Teilprozessen ist erstellt worden. In den Prozessbeschreibungen wird ein fachtechnischer Expertenpool in Form eines Public-Private-Partnerships eingebunden (Swiss Cyber Experts, vgl. Ziff. 2.1). Darüber hinaus hat die Arbeitsgruppe eine Definition eines Cybersicherheitsvorfalls ausgearbeitet.

Das Konzept zur NCS-Massnahme 15: *Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung* wurde um die Dimension der Kantone erweitert. Mittels Ausbildungs- und Übungssequenzen soll dieses Konzept überprüft werden. Es wurden mögliche Szenarien für eine Krise mit Cyberausprägung ausgearbeitet, die im Rahmen eines Strategischen Seminars bearbeitet werden sollen.

Weiter wurde ein Entwurf eines Konzeptes zur Führung einer nationalen Fallübersicht (Straffälle) und zur Koordination von interkantonalen Fallkomplexen erarbeitet und ein Konzept für die Ausbildung der Polizeikorps zum Thema Cyberkriminalität erstellt.

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 und ist über Generalsekretärenkonferenz (GSK) an den Bundesrat zu rapportieren. Die Koordinationsstelle NCS (KS NCS) hat mit den verantwortlichen Bundesämtern Ziele, Meilensteine und den zeitlichen Ablauf für die sechzehn NCS Massnahmen definiert.

5 Wirksamkeitsüberprüfung

Der Bundesrat hat den Steuerungsausschuss NCS (STA NCS) beauftragt, ihm bis im Frühjahr 2017 eine Wirksamkeitsüberprüfung (WiÜ) vorzulegen (S. 10 des Umsetzungsplans). Eine externe Firma wurde beauftragt, diese WiÜ durchzuführen. Die WiÜ soll aufzeigen:

- inwieweit die Massnahmen der Strategie inhaltlich und organisatorisch umgesetzt worden sind und welcher Beitrag zur Erreichung der Ziele der NCS von ihnen erwartet werden kann.
- ob seitens der Bundesverwaltung die für die Umsetzung der Strategie gesprochenen personellen und finanziellen Ressourcen genutzt worden sind und ob sich insbesondere mit Blick auf die Zukunft ein weiterer Ressourcenbedarf ergibt.
- ob sich aufgrund der Ergebnisse der Überprüfung ein Handlungsbedarf ergibt, die NCS anzupassen.

Mit Blick auf die Erarbeitung dieser WiÜ wurden zwei zeitliche Phasen mit folgenden Inhalten erarbeitet: Im Vorkonzept wurde unter Einbezug der relevanten Akteure ein gemeinsames Verständnis bezüglich der Eckpunkte (z. B. inhaltliche Schwerpunkte, Umfang, Organisation, usw.) der WiÜ entwickelt. Im Detailkonzept wird das Konzept operationalisiert. Die Arbeiten zum Detailkonzept haben begonnen.

6 Schlussbetrachtung

Seit der Verabschiedung des Umsetzungsplans NCS im Mai 2013 sind fast zwei Jahre vergangen. Die Umsetzung einiger Massnahmen ist ein umfangreiches und zeitaufwendiges Verfahren. Die Konsolidierung der Vorhaben sowie die Bestandsaufnahmen mit den relevanten Akteuren haben teilweise viel Zeit in Anspruch genommen. Die begrenzten Ressourcen

bzw. deren Priorisierung durch die betreffenden Stellen sowie umfangreiche Abklärungen von Rechtsgrundlagen haben die Umsetzungsarbeiten zum Teil verzögert. Zudem lassen sich mehrere sequentielle Arbeiten nicht parallelisieren. Dennoch sind die Umsetzungsarbeiten mit wenigen Ausnahmen im Zeitplan, weshalb die Bilanz per Ende 2014 durchaus positiv ausfällt.

Die NCS hat dazu geführt, dass eine zukunftsgerichtete vertrauensvolle Zusammenarbeit mit den Kantonen entstanden ist. Dadurch wird der kontinuierliche Wissens- und Erfahrungsaustausch zwischen Bund und Kantonen gefördert sowie eine bessere Zusammenarbeit mit weiteren Stellen, was dem Grundgedanken des dezentralen Ansatzes der NCS-Umsetzung entspricht. Durch diese Zusammenarbeit ist auch ein Austausch von Best-Practices entstanden, welcher für die jeweiligen Kantone den Aufwand reduzieren und die Wirksamkeit ihrer Massnahmen erhöhen kann. Die Ausgestaltung der Zusammenarbeit mit der Armee mit Blick auf deren subsidiäre Unterstützung konnte angegangen werden. Der Informationsaustausch zwischen KI-Betreibern, IKT-Leistungserbringern, Systemlieferanten, Verbänden, nationalen Standardisierungsorganisationen, Fachbehörden und Regulatoren wurde gestärkt. Die Interessen des Wirtschaftsstandortes Schweiz können auch koordiniert in die internationalen privaten und staatlichen Gremien im Bereich Sicherheit, Sicherung und Standardisierung eingebracht und vertreten werden.

Die NCS hat einen Prozess ausgelöst und muss sich stetig den neuen Bedrohungen anpassen. Es ist daher wichtig, dass die Zusammenarbeit, Kooperation und Kommunikation der relevanten Akteure auch in der Zukunft so bleiben wird und bei Bedarf weitere Akteure eingebunden werden können.

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

7.2 Zusammenstellung der Parlamentarischen Vorstösse zu Cyber-Risiken

Vorstoss Ip. = Interpellation; Mo. = Motion; Po. = Postulat; An. = Anfrage	Eingereicht am:	Stand per 31.12.2014:
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 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
13.3228 Ip Recordon. Abhöreinrichtungen und allgemeine Mängel der Informatik- und Telekommunikationseinrichtungen des Bundes	22.03.2013	erledigt
13.3229 Ip Recordon. Cyberkrieg und Cyberkriminalität. Wie gross sind die Bedrohungen, und mit welchen Massnahmen können sie bekämpft werden?	22.03.2013	erledigt
13.3558 Ip. Eichenberger. Cyberspionage: Einschätzung und Strategie	20.06.2013	erledigt
13.3692 Ip. Hurter. Telekommunikationsmarkt. Sind aktuelle Gesetzgebung und Regulierungsmassnahmen noch zeitgemäss?	12.09.2013	im Plenum noch nicht behandelt
13.3696 Mo. Müller-Altermatt. Echter Datenschutz statt Schutzschild für Steuerpreller	12.09.2013	im Plenum noch nicht behandelt
13.3707 Po. Fraktion BD. Ganzheitliche und zukunftstaugliche Cyberraumstrategie	17.09.2013	im Plenum noch nicht behandelt
13.3773 Ip. FDP-Liberale Fraktion. Zukunftstaugliches Fernmeldegesetz. Für eine übergreifende Cyberraum-Strategie	24.09.2013	im Plenum noch nicht behandelt
13.3841 Mo. Rechsteiner. Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit	26.09.2013	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	im Plenum noch nicht behandelt
13.4308 Po. Graf-Litscher. Sicherheit und Unabhängigkeit der Schweizer Informatik verbessern	13.12.2013	im Plenum noch nicht behandelt

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

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