AWK GROUP

Consulting
Engineering
Project Management

Bericht

Wirksamkeitsüberprüfung NCS

Informatiksteuerungsorgan Bund ISB
Schwarztorstrasse 59
3003 Bern

30. November 2016, Projekt-Nr. 12.415.14.01

Dokumentinformationen

Titel:	Wirksamkeitsüberprüfung NCS	
Projektnummer:	12.415.14.01	
Anzahl Seiten:	83 exkl. Beilagen	
Dateiname:	_Ber_161201_WiÜ_NCS_V1.0.docx	
Dokumentverantwortlicher:	Markus Meier, AWK	
Geprüft durch:	Korreferent /Projektbegleiter: Adrian Marti, AWK	Datum: 18.11.2016

Versionen

Version	Datum	Wichtigste Änderungen	Verantwortlich
V0.8	31.08.2016	Erster vollständiger Entwurf Begleitgruppe	Mem, Sep
V0.15	20.09.2016	Entwurf zum Review STA NCS	Mem
V0.25	16.11.2016	Version nach Feedback WS NCS II	Mem
V1.0	30.11.2016	Endgültige Version	Mem

Abkürzungen und Begriffe

Abkürzung	Beschreibung
ASP	Abteilung Sicherheitspolitik
ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAKOM	Bundesamt für Kommunikation
BFE	Bundesamt für Energie
BIT	Bundesamt für Informatik und Telekommunikation
BK	Bundeskanzlei
BR	Bundesrat
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BWL	Bundesamt für wirtschaftliche Landesversorgung
CDA	Chef der Armee
CERT	Computer Emergency Response Team
CNO	Computer Network Operations
CoPIRFC	Comité de Pilotage Recherche et Formation Cyber
CYD	Cyberdefence
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDK	Erziehungsdirektorenkonferenz
EJPD	EJPD Eidgenössisches Justiz- und Polizeidepartement
FUB	Führungsunterstützungsbasis
GCSP	Geneva Centre for Security Policy
ICANN	Internet Cooperation for Assigned Names and Numbers
IOC	Indicator of Compromise
IRB	Informatikrat des Bundes
ISB	Informatiksteuerungsorgan des Bundes
KFS	Kantonaler Führungsstab
KI	Kritische Infrastrukturen
KKM	KKM Konsultations- und Koordinationsmechanismus
KOBIK	Koordinationsstelle zur Bekämpfung der Internetkriminalität
KS NCS	Koordinationsstelle NCS
KTI	Kommission für Technologie und Innovation
MELANI	Melde- und Analysestelle Informationssicherung
MISP	Malware Information Sharing Platform
MND	Militärischer Nachrichtendienst
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes
OIC	Operation Information Center
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SCE	Swiss Cyber Experts

Abkürzung	Beschreibung
SFU	Strategische Führungsübung
SIEM	Security Information and Event Management
SIGF	Swiss Internet Governance Forum
SOC	Security Operation Center
SPOC	Single Point of Contact
SSK	Schweizerische Staatsanwälte-Konferenz
STA NCS	Steuerungsausschuss NCS
SVS	Sicherheitsverbund Schweiz
UCC	Unified Collaboration and Communication
ZEO	Zentrum elektronische Operationen
PPP	Public Private Partnership
PW	Privatwirtschaft
AG	Arbeitsgruppe
WiÜ	Wirksamkeitsüberprüfung
WSIS	World Summit of the Information Society
GK	Geschlossener Kundenkreis

Inhaltsverzeichnis

Zusammenfassung

Ausgangslage und Auftrag
Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) beschlossen und am 15. Mai 2013 verabschiedete er deren Umsetzungsplan. Darin enthalten ist der Auftrag, bis im Frühjahr 2017 eine Wirksamkeitsüberprüfung (WiÜ) zur NCS vorzulegen. Der vorliegende Bericht erfüllt diesen Auftrag.

Die NCS definiert drei strategische Ziele:

- Frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich
- Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- Wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage

Diese Ziele sollen über 16 Massnahmen in den Bereichen Prävention und Kontinuität, Reaktion, Krisenmanagement, internationale Zusammenarbeit, Forschung und Bildung und rechtliche Grundlagen erreicht werden.

Fragestellung
Um die Wirkung der NCS umfassend beurteilen zu können, braucht es Wirksamkeitsanalysen auf drei Ebenen:

1) Die NCS-Massnahmen: wurden die 16 Massnahmen planmässig umgesetzt? Was wurde dadurch erreicht? Inwiefern haben sie zur Erreichung der strategischen Ziele beigetragen?
2) Schnittstellen: sind die Kantone und die Armee genügend in die Arbeiten der NCS einbezogen worden?
3) Massnahmenübergreifende Aspekte: war die Ressourcenplanung der NCS zutreffend? Haben sich die Inhalte und die Organisationsstruktur der NCS bewährt? Hat die Kommunikation intern und extern funktioniert?

Evaluationsmethodik
Die Wirksamkeitsüberprüfung wendet einen umfassenden Evaluationsansatz an, der die Wirkung auf den drei Stufen Output, Outcome und Impact analysiert. Dabei werden die Stufen wie folgt verstanden:

- Output: Ergebnisse der effektiven Umsetzung der Strategie.
- Outcome: Erreichte Zielgruppen, ausgelöster Wissensaufbau, erreichte Sensibilisierungen und Verhaltensänderungen.
- Impact: Effektive Wirkung auf die strategischen Ziele der NCS..

Die Bewertung des Output und des Outcome erfolgt nach den im Umsetzungsplan vorgegebenen Zielen mit Hilfe einer vierstufigen Skala (Ziele nicht erreicht, Ziele nur teilweise erreicht, Ziele grösstenteils erreicht, Ziele erreicht). Beim Impact wird aufgezeigt, ob nachweislich ein Impact erzielt werden konnte oder nicht.

Datenerhebung
Die Resultate der WiÜ basieren in erster Linie auf einer Befragung der Massnahmenverantwortlichen und der Vertreter der Schnittstellen sowie einer umfangreichen Dokumentenanalyse. Wo nötig und sinnvoll wurden zusätzliche Befragungen durchgeführt. Die Interviewpartner wurden in Zusammenarbeit mit der Koordinationsstelle NCS festgelegt. Die Erhebung fand von März 2016 bis Ende Juni 2016 statt. Zu diesem Zeitpunkt, waren noch verschiedene Massnahmen nicht abgeschlossen. Die Wirksamkeitsüberprüfung spiegelt den Status zum Zeitpunkt der Erhebung wieder.

Bewertung der Massnahmenumsetzung

Tabelle 1 fasst die Resultate der WiÜ pro Massnahme zusammen.

Legende			
✗✗	Ziele nicht erreicht	✗	Ziele nur teilweise erreicht
✓✓	Ziele erreicht	✓	Ziele grösstenteils erreicht
◎	Impact erzielt	☐	Zurzeit nicht messbar, nicht beurteilbar

Massnahmen	Zust. Amt, OE	Output	Outcome	Impact
M2/M12 Prävention & Kontinuität: Risiko- und Verwundbarkeitsanalysen sowie Kontinuität	BABS, BWL	✓✓	✓✓	☐
M3 Prävention & Kontinuität: Verwundbarkeitsanalyse IKT-Infrastruktur	ISB	✗	☐	☐
M4 Prävention & Kontinuität: Erstellung Lagebild und Lageentwicklung	MELANI, NDB	✓	✓	◎
M5 Reaktion: Vorfall-Analyse und Nachbearbeitung von Vorfällen	MELANI, NDB	✓	✓	◎
M6 Reaktion: Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	KOBIK	✓	✗	☐
M14 Reaktion: Aktive Massnahmen und Identifikation der Täterschaft	MELANI, NDB, ISB	✓	✓	◎
M13 Krisenmanagement: Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise	MELANI und NDB	✓	☐	☐
M15 Krisenmanagement: Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung	BK	✓	✗	☐
M9 Internationale Zusammenarbeit: Internet Governance	BAKOM	✓✓	✓	☐
M10 Internationale Zusammenarbeit: Kooperation auf der Ebene der internationalen Sicherheitspolitik	EDA	✓✓	✓✓	☐
M11 Internationale Zusammenarbeit: Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit	BAKOM	✓	✗	☐
M1 Bildung und Forschung: Identifikation von Cyber-Risiken durch die Forschung	SBFI	✓✓	✓	☐
M7/M8 Bildung und Forschung: Übersicht Kompetenzbildungsangebote sowie vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotsnutzen	KS NCS	✓	✓✓	☐
M16 Gesetzliche Grundlagen: Handlungsbedarf rechtlicher Grundlage	KS NCS	✓✓	☐	☐

Tabelle 1 Beurteilung Zielerreichung der Massnahmen

Es kann festgestellt werden, dass die Umsetzung der Massnahmen gut vorangekommen ist. Die vorgesehenen Strukturen und Prozesse sind grösstenteils implementiert und verschiedene Produkte (Berichte und Konzepte) wurden termingerecht geliefert. Der geleistete Output führte auch bereits zu einem beachtlichen Outcome, indem nachweislich Kapazitäten ausgebaut, der Wissensstand vergrössert und die Koordination verbessert wurde.

Am schwierigsten messbar ist die direkte Wirkung (Impact) der Arbeiten auf die strategischen Ziele. Im komplexen und dynamischen Kontext der Cyber-Risiken ist es kaum möglich kausale Zusammenhänge zwischen den ergriffenen Massnahmen und ihrer Wirkung auf die Ziele der NCS nachzuweisen. Zudem ist der Zeitpunkt der Wirksamkeitsüberprüfung für eine solche Messung zu früh. Typischerweise entfalten die getroffenen Massnahmen ihre Wirkung erst nach einem gewissen Zeitraum. Darum kann erst für drei der 16 Massnahmen ein Impact nachgewiesen werden. In den im Rahmen der Überprüfung entwickelten Wirkungsmodellen für alle Massnahmen wird aber aufgezeigt, welche konkrete Wirkung auf Grund der bisher erzielten Resultate zu erwarten ist.

Bewertung der Schnittstellen
Für die Umsetzung der NCS sind zwei Schnittstellen von zentraler Bedeutung: die Schnittstelle zu Aktivitäten der Kantone und die Schnittstelle zur Cyber-Defence der Armee. Die WiÜ hat untersucht, wie gut diese Schnittstellen wahrgenommen wurden.

Schnittstelle zu den Kantonen:

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome			✓	
Impact	☐ aktuell nicht beurteilbar			

Tabelle 2 Beurteilung Zielerreichung Schnittstellen mit den Kantonen – SVS

Schnittstelle zur Armee:

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output		✗		
Outcome		✗		
Impact CYD-Umgebung	☐ aktuell nicht beurteilbar			

Tabelle 3 Beurteilung Zielerreichung Schnittstellen mit der Armee

Bewertung der massnahmenübergreifenden Aspekte
In Bezug auf die massnahmenübergeordneten Aspekte wird beurteilt, ob die Ressourcenplanung der NCS zutreffend war, ob die Inhalte und die Organisationsstruktur der NCS sich insgesamt bewährt haben und ob die Kommunikation intern und extern funktioniert hat. Dabei wird beurteilt, ob die Erwartungen erfüllt, grösstenteils erfüllt, nur teilweise erfüllt oder nicht erfüllt wurden. Die Resultate dieser Beurteilung sind in Tabelle 5 dargestellt:

Ebene	Erwartungen nicht erfüllt	Erwartungen nur teilweise erfüllt	Erwartungen grösstenteils erfüllt	Erwartungen erfüllt
Ressourcenplanung			✓	
Inhalte				✓✓
Organisation			✓	
Kommunikation		✗		

Tabelle 4 Beurteilung der massnahmenübergreifenden Aspekte

Generell lässt sich auch zu den massnahmenübergeordneten Fragen ein positives Fazit ziehen. Die Inhalte haben sich grundsätzlich bewährt, die Ressourcen waren knapp aus-

reichend und die dezentrale Organisationsstruktur wird begrüsst. Bemängelt wurde jedoch die Kommunikation gegen aussen, die nach Ansicht verschiedener Interviewpartner gestärkt werden muss.

1. Ausgangslage und Auftrag

Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) beschlossen. Er will damit in Zusammenarbeit mit Behörden, Wirtschaft und Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, denen diese täglich ausgesetzt sind. Am 15. Mai 2013 hat der Bundesrat den Umsetzungsplan zur NCS verabschiedet. Er definiert darin die personellen Ressourcen für die Umsetzung der NCS und setzt einen interdepartementalen Steuerungsausschuss NCS (STA NCS) ein, der die Arbeiten beaufsichtigt und koordiniert

Der STA NCS ist beauftragt, dem Bundesrat bis im Frühjahr 2017 eine Wirksamkeitsüberprüfung vorzulegen (S. 10 des Umsetzungsplans). Die Überprüfung soll darüber Aufschluss geben, ob die beschlossenen Massnahmen die gewünschten Wirkungen erzielen konnten und ob die Ressourcen zielführend eingesetzt wurden.

Aus diesem Auftrag besteht die Ausgangslage für die Durchführung der Wirksamkeitsüberprüfung. Darum soll zunächst kurz dargestellt werden, welche Ziele und Massnahmen in der NCS vorgegeben werden und wer die Umsetzung verantwortet. Danach werden die Ziele und die Projektorganisation der Wirksamkeitsüberprüfung beschrieben.

1.1. Ausgangslage: Inhalt und Organisation der NCS

1.1.1. Ziele und Massnahmen der NCS

Der Bundesrat hat in der NCS drei strategische Ziele gesetzt:

- Frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich
- Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- Wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage

Um diese Ziele zu erreichen, wurden 16 Massnahmen definiert. Da Cyber-Risiken die verschiedensten Aspekte der Gesellschaft, Wirtschaft und Politik betreffen, sind die Massnahmen entsprechend unterschiedlich. Sie reichen von der Durchführung von Risikoanalysen, über die Stärkung der Vorfallbekämpfung bis zur Förderung der Forschung und der Ausgestaltung der Cyber-Aussenpolitik.

Bei der Erstellung des Umsetzungsplans wurden die 16 Massnahmen gruppiert und in folgende sechs Bereiche unterteilt:

- <u>Prävention und Kontinuität:</u>
  - M2: Risiko- und Verwundbarkeitsanalysen in den kritischen Teilsektoren
  - M3: Verwundbarkeitsanalyse IKT-Infrastruktur
  - M4: Erstellung des Lagebilds und Lageentwicklung
  - M12: Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren
- <u>Reaktion</u>
  - M5: Vorfallanalyse und Nachbearbeitung von Vorfällen
  - M6: Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe
  - M14: Aktive Massnahmen und Identifikation der Täterschaft
- <u>Krisenmanagement</u>

- M13: Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise
- M15: Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung

- Bildung und Forschung:
  - M1: Identifikation von Cyber-Risiken durch die Forschung
  - M7: Übersicht Kompetenzbildungsangebote
  - M8: Schliessung von Angebotslücken und Förderung der Nutzung bestehender Angebote
- Internationale Zusammenarbeit:
  - M9: Internet Governance
  - M10: Internationale Kooperation Cyber-Sicherheit
  - M11: Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit
- Rechtliche Grundlagen
  - M16: Handlungsbedarf rechtliche Grundlagen

1.1.2. Organisation und Umsetzungsverantwortung der NCS

Die strategische Verantwortung für die Umsetzung der NCS trägt der Steuerungsausschuss NCS (STA NCS). Als operatives Organ des STA NCS übernimmt die Koordinationsstelle NCS (KS NCS) das strategische Controlling der Massnahmen und die Koordination zwischen den Massnahmenverantwortlichen. Die KS NCS ist im Informatiksteuerungsorgan des Bundes (ISB) und der Melde- und Analyse Informationssicherung (MELANI) angegliedert.

Für die Umsetzung der Massnahmen sind folgende Organisationseinheiten zuständig:

- Koordinationsstelle NCS (M7, M8, M16)
- MELANI (M4, M5, M13, M14)
- ISB (M3)
- NDB (M4, M5, M14)
- BABS und BWL (M2, M12)
- BAKOM (M7, M9, M11)
- EDA (M10)
- BK (M15)
- SBFI (M1)

1.2. Zielsetzungen der Wirksamkeitsüberprüfung (WiÜ)

Wie im Bundesratsbeschluss über den Umsetzungsplan der NCS festgehalten, soll die WiÜ in erster Linie untersuchen, welche Arbeiten unter welchem Aufwand geleistet wurden und welche Resultate damit erzielt werden konnten. Daraus ergeben sich die drei wichtigsten Ziele der Wirksamkeitsüberprüfung:

- Beurteilung der Massnahmenumsetzung: Es soll überprüft werden, welche Arbeiten unter welchem Aufwand geleistet wurden und welche Resultate und Wirkungen damit erzielt werden konnten.
- Beurteilung der Schnittstellen: Es soll untersucht werden, ob bei der Umsetzung der NCS die Kantone genügend berücksichtigt werden und ob die Schnittstelle zur Cyber-Defence der Armee gepflegt wird.
- Beurteilung der massnahmenübergreifenden Aspekte: Es wird evaluiert, ob die Ressourcenplanung der NCS zutreffend war, ob die Inhalte und die gewählten Struktur der NCS sich bewährt haben und ob ausreichend intern und extern kommuniziert wurde.

2. Vorgehen

Grundlage für die Umsetzung der Wirksamkeitsüberprüfung war das im Herbst 2015 erstellte Detailkonzept [3], in welchem die Vorgehensweise zur WiÜ festgelegt worden ist. Basierend auf diesem Dokument wurde ein dreistufiges Vorgehen definiert:

- Konzeption
- Durchführung
- Berichterstattung

2.1. Konzeption

Das bereits erwähnte Detailkonzept gliedert die Evaluation in drei Teile:

1) Evaluation der Massnahmen (Kapitel 3)
2) Überprüfung der Schnittstellen (Kapitel 4)
3) Untersuchung der massnahmenübergreifenden Aspekte (Kapitel 5)

Diese Struktur wird auch in diesem Bericht verwendet.

Die Massnahmen und die Schnittstellen werden mit Hilfe von Wirkungsmodellen überprüft. In diesen Modellen wird dargestellt, welche Wirkung die Massnahmen auf welche Weise erzielen sollen. Unterschieden werden dabei die Ebenen Konzept, Input, Output, Outcome sowie Impact, wie dies schematisch in Abbildung 1 dargestellt ist:

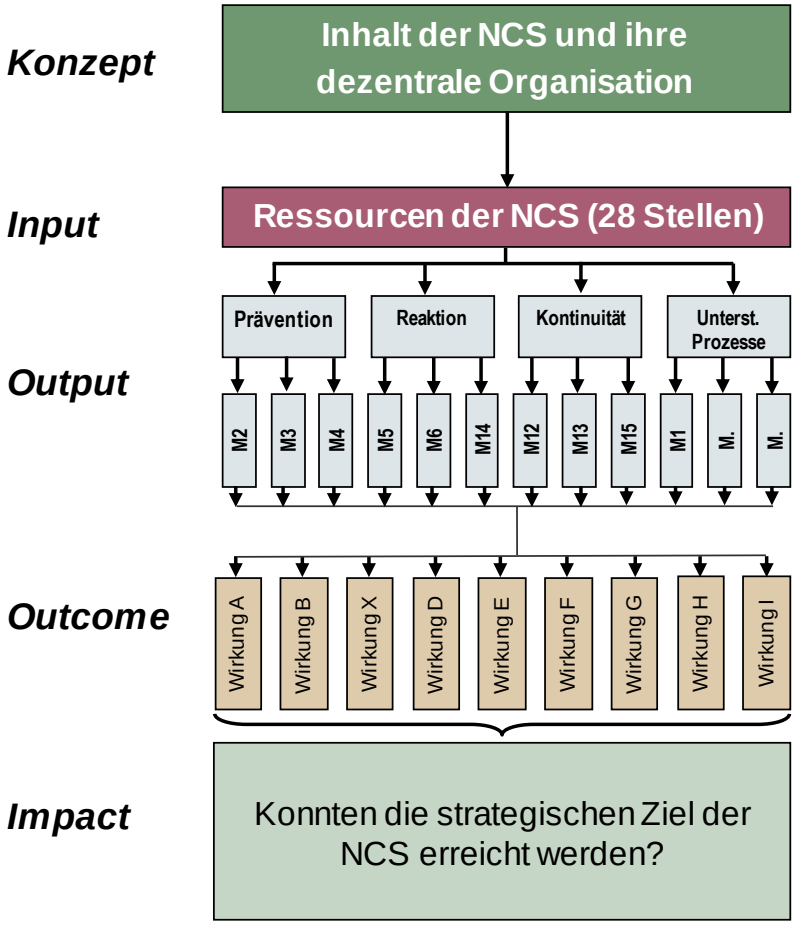

Abbildung 1 Ebenen der Wirksamkeitsüberprüfung

- **Konzept:** Die Konzept-Ebene ist vor allem für die massnahmenübergreifenden Fragen und die Schnittstellen relevant. Es wird evaluiert, ob die NCS inhaltlich und organisatorisch gut aufgestellt ist und ob die Zusammenarbeit mit Dritten funktioniert hat. Bei den 16 Massnahmen werden die Ebenen Input, Output, Outcome und Impact untersucht.
- **Input:** Finanzieller und personeller Ressourceneinsatz zur Umsetzung der Strategie. Beurteilt wird der Einsatz der gesprochenen Ressourcen und ob sie nachhaltig die Aufgaben der NCS unterstützen.
- **Output:** Ergebnisse der effektiven Umsetzung der Strategie, also etablierte Organisationsstrukturen, implementierte Prozesse, erstellte Produkte und Dienstleistungsangebote, etc. Es geht um die Beurteilung zum Stand der Umsetzung der Massnahmen in den verschiedenen Gebieten (Erreichung von Meilensteinen).
- **Outcome:** Erreichte Zielgruppen, ausgelöster Wissensaufbau, erreichte Sensibilisierungen und Verhaltensänderungen. Im Fokus steht auch die Beurteilung des Wirkungspotentials der einzelnen Massnahmen, z. B. in Bezug auf Sensibilisierung oder Verhaltensänderung bezüglich Cyber-Risiken.
- **Impact:** Können die strategische Ziel der NCS durch die Umsetzung der Massnahme erreicht werden, d. h. welche effektive Wirkung wurde durch die Umsetzung der Massnahmen erzielt? Auch soll beurteilt werden, inwieweit ein Beitrag zur Resilienz und zur Reduktion von Cyberrisiken erreicht wurde.

Für jede Massnahme (und auch für die Schnittstellen) wurde in Absprache mit den Massnahmenverantwortlichen ein Wirkungsmodell entwickelt. So kann nachvollzogen werden, was die Idee, das Vorgehen und die Resultate jeder Massnahme waren. Wichtig für die Überprüfung der Massnahmen sind vor allem die Ebenen Output, Outcome und Impact – weil auf diesen Ebenen direkt der Fortschritt und der Erfolg der Arbeiten der Umsetzungsverantwortlichen gemessen werden kann.

2.2. Durchführung

2.2.1. Vorgehen bei der Befragung

Als Basis für die Evaluation diente ein Masterfragebogen, der aus dem Detailkonzept [3] abgeleitet wurde.

Für jedes Interview bzw. für die Adressaten der schriftlichen Befragungen wurden individuelle Fragebogen erstellt, die aus diesem Fragebogen abgeleitet wurden.

Die spezifischen Fragebogen wurden dann mit Hilfe der zur Verfügung gestellten Unterlagen bereits vorausgefüllt und in der Regel mindestens 5 Arbeitstage vor den Interviews an die Interviewteilnehmer verschickt, damit sich diese vorbereiten konnten. Für die Beantwortung der nur schriftlich verteilten Fragebogen wurde den Adressaten ein Termin von ca. 10 Arbeitstagen gesetzt. Nach den Interviews wurden die vollständig ausgefüllten Fragebogen den Interviewpartnern zum Review abgegeben, damit diese ihre Antworten verifizieren konnten.

2.2.2. Auswahl der Befragten

Die Auswahl der Befragten erfolgte nach Absprache mit der Koordinationsstelle NCS:

- **Persönliche Interviews:** Insgesamt wurden 14 Interviews mit Vertretern von SBFI, EDA-ASP, ISB-SEC, ISB-MELANI, MELANI-OIC, NDB, fedpol, BAKOM, BK, SVS, BABS, BWL, MND, FUB und BFE durchgeführt.

- **Schriftliche Befragungen:** Vertreter aus sechs kritischen Teilsektoren wurden schriftlich befragt: Erdgasversorgung, Stromversorgung, Luftverkehr, Banken, Medien, Gesundheitswesen.

Die detaillierte Interviewliste befindet sich im Anhang A.1.

Zu jedem Themengebiet wurde von der KS NCS die notwendigen und verfügbaren Unterlagen/Dokumente AWK zur Verfügung gestellt. Diese Unterlagen wurden teilweise durch eigene AWK Recherchen ergänzt (siehe referenzierte Dokumente im Anhang B).

2.2.3. Eindrücke bei der Erhebung

Eine besondere Herausforderung war die Mächtigkeit der nach Vorgabe des Detailkonzepts [3] zu stellenden Fragen (insgesamt über 280). Je nach betroffenem Interviewpartner resultierten oft an die 100 Fragen, z. B. wenn die Verantwortlichen für mehre Massnahmen zuständig waren. Die Interviewpartner waren sehr motiviert und haben sich gut auf die Interviews vorbereitet. Das gewählte Vorgehen wurde verstanden und die Teilnehmenden unterstützten aktiv die Beantwortung der Fragen. Die Befragten machten z. T. auch intensiv von der Möglichkeit Gebrauch, die Antworten nach dem Interview während des Reviews noch schriftlich zu präzisieren.

Auch das Einholen der schriftlich durchgeführten Erhebung bei den Teilsektoren funktionierte tadellos. Die Fragebogen wurden rasch ausgefüllt, so dass sie für die Auswertung bereitstanden.

2.3. Berichterstattung

In der letzten Phase wurden die Resultate konsolidiert und in diesem Bericht zuhanden des Bundesrats zusammengefasst. Dies geschah in enger Abstimmung mit der KS NCS und den Umsetzungsverantwortlichen, um Unklarheiten, Lücken und Widersprüche zu klären.

Anmerkung: Die im Bericht gemachten Aussagen basieren auf den Antworten der Interviews mit den Interviewpartnern. Die AWK hat diese Antworten ohne Sinnveränderung in diesen Bericht eingearbeitet.

2.4. Grundsätzliche Herausforderungen bei der Bewertung

Die Bewertung der erhobenen Daten ist der eigentliche Kern der Wirksamkeitsüberprüfung. Gleichzeitig ist es im gesamten Prozess auch derjenige Schritt, dessen Umsetzung die grösste Herausforderung darstellt. Im Sinne der Transparenz beschreibt AWK hier einige der wichtigsten Fragestellungen, mit denen das Bewertungsteam konfrontiert war und stellt dar, welche Lösungen aus welchen Gründen gewählt wurden.

2.4.1. Inhaltliche Heterogenität der Massnahmen

Wie bereits beschrieben, decken die 16 Massnahmen inhaltlich ein sehr breites Spektrum ab. Für die Wirksamkeitsüberprüfung stellt sich vor allem die Herausforderung, dass einzelne Massnahmen klar definierte Endprodukte haben, während andere Massnahmen das Ziel haben, neue Prozesse zu initiieren oder laufende Prozesse zu stärken. Für den Prüfer sind Produkte einfacher messbar als Prozesse. Es besteht daher die Gefahr, dass Massnahmen mit Produkten im Vergleich anders bewertet werden, als eher prozessorientierte Massnahmen.

Um diese Problematik zu entschärfen, misst AWK die Massnahmen strikt an den definierten Massnahmenzielen (Meilensteine) gemäss Roadmap NCS [6]. Nur so ist eine faire Bewertung möglich, da die gesprochenen Ressourcen sich auf die definierten Massnahmen beziehen. Diese Lösung hat zur Folge, dass AWK bei der Bewertung der Massnahmen keine Quervergleiche zwischen den Massnahmen anstrebt. Die Wirksamkeitsüberprüfung beschränkt sich darauf, für jede Massnahme individuell aufzeigen, wie gut die entsprechenden Ziele erreicht wurden.

2.4.2. Wirksamkeitsüberprüfung bei laufenden Massnahmen

Eine grosse Herausforderung der Wirksamkeitsprüfung ist der Zeitpunkt ihrer Durchführung. Üblicherweise finden solche Überprüfungen nach Abschluss eines Programms statt. Bei einer Überprüfung während des laufenden Projekts bestehen zwei grundsätzliche Schwierigkeiten:

- Unterschiedlicher Umsetzungsstand der Massnahmen: Da verschiedenen Massnahmen noch laufen, wird oft nicht ein Schlusszustand, sondern ein Zwischenergebnis bewertet.
- Messung des Impacts: Bei vielen Massnahmen ist es zum aktuellen Zeitpunkt unrealistisch, bereits Wirkungen auf der Ebene des Impacts zu messen, weil die Massnahmen erst später greifen werden.

AWK war sich dieser beiden Probleme von Anfang an bewusst. Das Problem des unterschiedlichen Umsetzungsstands kann gelöst werden, indem die Massnahmen ausschliesslich aufgrund der im Frühling 2016 bereits erreichten Ziele gemäss der Roadmap NCS [6] beurteilt werden. Ziele, die gemäss dieser Roadmap erst nach diesem Zeitpunkt erreicht werden müssen, werden in der Beurteilung nicht berücksichtigt.

Der Impact von Massnahmen wird nur dann beurteilt, wenn nachgewiesen werden kann, dass eine direkte Wirkung erzielt wurde oder mit Sicherheit festgestellt werden muss, dass dies nicht der Fall sein wird.. Bei allen anderen Massnahmen wird darauf verwiesen, dass eine Messung noch nicht durchführbar ist und die Massnahme ausschliesslich über den Output und den Outcome beurteilt wird.

3. Wirksamkeitsüberprüfung Massnahmen

Massgeblich für die Bewertung der Massnahmen ist die Zielsetzung jeder Massnahme, wie sie in der Roadmap NCS [6] definiert ist und durch die Massnahmenverantwortlichen selbst präzisiert wurde.

Die in Kapitel 1.1.1 eingeführten 16 Massnahmen werden auf den Ebenen Input, Output, Outcome, Impact sowie Konzept-Ebene betrachtet. Es wird nach dem in Kapitel 2.1 eingeführten Konzept vorgegangen.

Die Berichtskapitel zu den einzelnen Massnahmen sind für alle 16 Massnahmen identisch aufgebaut:

- Tabelle mit Beschreibung der Massnahme bestehend aus
  - Beschreibung der Ziele
  - Verantwortliches Amt
  - Quellen (Konsultierte Unterlagen)
  - Interviewverweis
- Erwartete Wirkung mit Wirkungsmodel aus dem Detailkonzept [3]
- Input (eingesetzte Ressourcen)
- Tabelle mit Zielerreichung und Wirkung
- Begründung der Beurteilung gegliedert in Output, Outcome und Impact

Aspekte zu Schnittstellen befinden sich in Kapitel 4, massnahmenübergreifende Aspekte sind in Kapitel 5 zusammengefasst.

3.1. M2/M12 Prävention & Kontinuität: Risiko- und Verwundbarkeitsanalysen sowie Kontinuität

Titel Massnahme	Risiko- und Verwundbarkeitsanalysen sowie Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren
Ziele	Ziele der Massnahme M2 Risiko und Verwundbarkeit: • In den 28 kritischen Teilsektoren sind in Zusammenarbeit mit den entsprechenden Fachbehörden und Verbänden sowie unter Einbezug der IKT-Leistungserbringer und Betreiber kritischer Infrastrukturen Risiko- und Verwundbarkeitsanalysen durchgeführt. Diese erfolgten nach einem möglichst einheitlichen Ansatz. – Die Ergebnisse der Risiko- und Verwundbarkeitsanalysen werden in Zusammenarbeit mit MELANI zu einer gesamtheitlichen Analyse der Bedrohungslage konsolidiert. – Die Ergebnisse dienen insbesondere als Grundlage der Arbeiten zur Erfüllung der Massnahme 12. Ziele der Massnahme M12 Kontinuitätsmanagement: • Verbesserung der Resilienz der kritischen Teilsektoren: In den 28 kritischen Teilsektoren sind basierend auf den Ergebnissen der Risiko- und Verwundbarkeitsanalysen entsprechende Konzepte mit möglichen Massnahmen zur Verbesserung der Resilienz erarbeitet. – Dies geschieht in Zusammenarbeit mit der Branche und, wo sinnvoll, unter Einbezug der Verbände sowie den entsprechenden Fach- und Regulationsbehörden. – Das Konzept kann u. a. Vorschläge betreffend Massnahmen für die Prävention, den Aufbau eines unternehmensübergreifenden Kontinuitäts- und Krisenmanagements oder für die Verbesserung der Resilienz der Unternehmen des jeweiligen kritischen Teilsektors umfassen.

Verantwortliches Amt / Organisationseinheit	BABS, BWL
Konsultierte Unterlagen für die WiÜ	Quellen: [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64]
Interviews, Fragebogen	Siehe Anhang A.1, Interviews I 3, I 8 und Fragen an die Teilsektoren A.2

Anmerkungen:

- Das BABS und das BWL haben sich die 28 Teilsektoren wie folgt aufgeteilt:
  - Zuständigkeit BABS: Diplomatische Vertretungen und Sitze internationaler Organisationen, Forschung und Lehre, Kulturgüter, Parlament, Regierung, Justiz und Verwaltung, Abfälle, Banken, Versicherungen, ärztliche Betreuung und Spitäler, Labors, Medien, Postverkehr, Armee, Blaulichtorganisationen, Zivilschutz.
  - Zuständigkeit BWL: Erdgasversorgung, Erdölversorgung, Stromversorgung, Chemie- und Heilmittelindustrie, MEM-Industrie, Informationstechnologien, Telekommunikation, Lebensmittelversorgung, Strassenverkehr, Schiffsverkehr, Schienenverkehr, Luftverkehr, Wasserversorgung, Abwasser.
- Zur Beurteilung der Arbeiten zu den Massnahmen 2 und 12 wurden insgesamt 13 beteiligte Vertreter aus folgenden Teilsektoren befragt: Ärztliche Betreuung und Spitäler; Labors; Banken; Medien; Stromversorgung; Gas; Luftverkehr.

3.1.1. *Erwartete Wirkung: Wirkungsmodell M2 / M12*

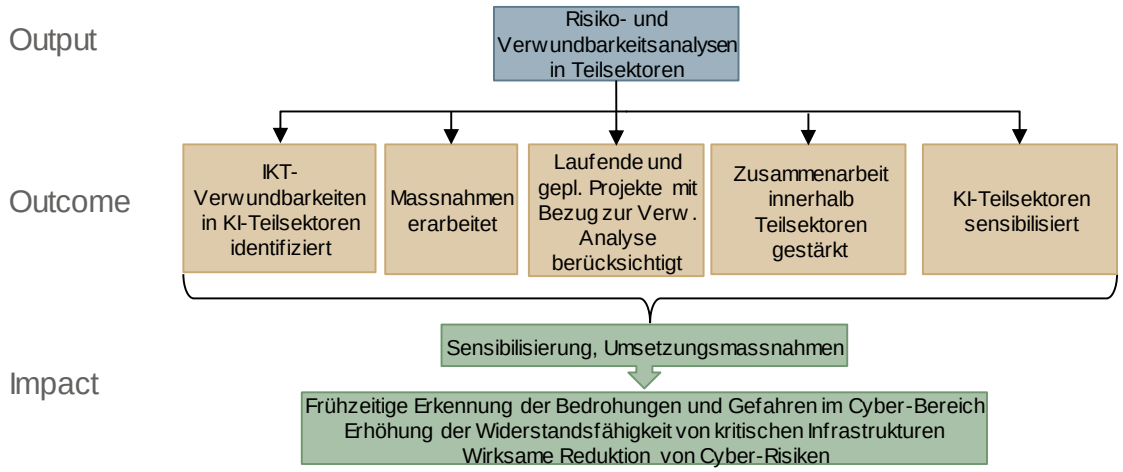

Abbildung 2 Wirkungsmodell M2 / M12

3.1.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	2 BABS 2 BWL 1 BFE
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	Fachbehörden/Regulatoren, MELANI, Konsultationen bei BIT und FUB, Fachverbände sowie Vertreter kritischer Infrastrukturen und weiterer relevanter Akteure der jeweiligen Teilsektoren

Dem BABS und dem BWL wurden jeweils zwei FTEs für die Projektleitung und Durchführung der Risiko- und Verwundbarkeitsanalysen zugesprochen. Das BFE erhielt eine Stelle, um die spezifischen Cyber-Risiken im Energiebereich zu analysieren, Resilienzmassnahmen der Energiewirtschaft zu unterstützen und bei Bedarf die Anpassung rechtlicher Rahmenbedingungen vorzubereiten. Ohne die geschaffenen Stellen wären die Arbeiten nicht möglich gewesen.

3.1.3. Beurteilung der Zielerreichung und Wirkung

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome				✓✓
Impact	☐ aktuell nicht beurteilbar			

Anmerkung: Die Erstellung der Risiko- und Verwundbarkeitsanalysen der kritischen Teilsektoren war zum Zeitpunkt der Wirksamkeitsüberprüfung noch nicht vollständig abgeschlossen. Die Arbeiten laufen plangemäss noch bis 2017 und sind auf Kurs. Zum Zeitpunkt der Überprüfung lagen für folgende Teilsektoren Schlussberichte der Risiko- und Verwundbarkeitsanalysen vor:

- BABS: Zivilschutz, Labors, Medien, Banken sowie ärztliche Betreuung und Spitäler. Zusätzlich stellte das BABS Berichtsentwürfe zu den Sektoren Blaulichtorganisationen und Parlament, Regierung, Justiz und Verwaltung zur Verfügung.
- BWL: Stromversorgung, Erdgasversorgung, Luftverkehr, Strassenverkehr, Lebensmittel.

Zusätzlich zu den Risiko- und Verwundbarkeitsanalysen lag auch bereits ein Entwurf eines Massnahmenberichtes (M12) des BWL für den Sektor Erdgas vor.

Die Beurteilung basiert auf diesen Berichten.

3.1.4. Begründung der Beurteilung

<u>Output: Ziele sind erreicht:</u>

Die Risiko- und Verwundbarkeitsanalysen in verschiedenen Teilsektoren waren z.T. bereits erstellt, andere waren zum Zeitpunkt der Wirksamkeitsüberprüfung noch in Arbeit. Die Qualität der Berichte und die gewählte Methodik werden von den befragten Experten als gut eingeschätzt. BABS und BWL verwenden für ihre Analysen jeweils leicht andere Ansätze, was die Kohärenz und Transparenz des Gesamtprojekts etwas beeinträchtigt. Es wird aber nach Abschluss der Arbeiten dennoch möglich sein, ein Gesamtbild über die IKT-Risiken und Verwundbarkeiten in den kritischen Teilsektoren zu gewinnen.

- **Beurteilung der Risiko- und Verwundbarkeitsanalysen in den KI-Teilsektoren:** Die Risiko- und Verwundbarkeitsanalysen und Marktanalysen der kritischen Teilsektoren sind in Arbeit oder wurden schon erstellt. Die Erarbeitung der Berichte erfolgte in Expertengruppen, geleitet durch das BABS, respektive durch das BWL. Die Expertengruppen wurden unterstützt durch Branchenvertreter (Fachverbände und/oder wichtige Unternehmen), Vertretern der Fachbehörden, Regulatoren und weiteren IKT-Spezialisten. Die Berichte durchliefen einen mehrstufigen Feedbackprozess, so dass sie gut mit den Experten aus den Branchen abgestimmt sind. Alle Berichte werden abschliessend jeweils vom BABS bzw. vom BWL und vom ISB freigegeben.

Anhand der zum Zeitpunkt der Wirksamkeitsüberprüfung fertiggestellten Berichte ergibt sich folgende Einschätzung:

- Vorgehen und Struktur: die enge Zusammenarbeit mit den Experten aus den Branchen wird von diesen sehr begrüsst. Deren Einbezug ermöglicht eine vollständige Darstellung der Marktstrukturen in den jeweiligen Sektoren, eine realistische Einschätzung der Risiken und Verwundbarkeiten und erleichtert die Definition von Massnahmen.
- Methodik: Für jeden Teilsektor wird zuerst der Teilsektor generell beschrieben, dann die kritischen Prozesse identifiziert und schliesslich eine Verwundbarkeits- und Risikoanalyse durchgeführt. Bei der Beurteilung der Risiken und Verwundbarkeiten wählten BABS und BWL unterschiedliche Ansätze (mehr dazu in der Anmerkung unten).
- Transparenz und Darstellung der Resultate: es ist vorgesehen, auf der Grundlage der Berichte Factsheets zu erstellen, die der Öffentlichkeit zugänglich gemacht werden können. Dies ermöglicht dann auch eine Gesamtschau über die Risiko- und Verwundbarkeitsanalysen und wird so Transparenz schaffen.

Anmerkung zu den Unterschieden beim Vorgehen zwischen BABS und BWL: Bei der Beurteilung der Risiken und Verwundbarkeiten wählten das BABS und das BWL jeweils einen unterschiedlichen Ansatz: das BABS führt auf der Grundlage der Ergebnisse der Verwundbarkeitsanalysen szenarienbasierte Risikoanalysen durch mit einer Einschätzung des Risikos als Resultat aus der Eintrittswahrscheinlichkeit multipliziert mit dem Schadenspotential. Das BWL beurteilt die IKT-Verwundbarkeiten aufgrund der Kritikalität und der Gefährdung der Teilprozesse und verzichtet auf eine szenarienbasierte Risikoanalyse. Grund für dieses unterschiedliche Vorgehen sind einerseits die unterschiedlichen Eigenschaften der jeweiligen Teilsektoren und andererseits die jeweilige Anknüpfung an bestehende Arbeiten in den beiden Ämtern (beim BABS die Strategie zum Schutz kritischer Infrastrukturen und die nationale Risikoanalyse „Katastrophen und Notlagen Schweiz“, beim BWL die strategische Ausrichtung der wirtschaftlichen Landesversorgung). Die Unterschiede führen dazu, dass das BABS Cyber-Risiken im Kontext anderer möglichen Gefährdungen analysiert, während das BWL die spezifischen IKT-Verwundbarkeiten ausführlich untersucht. Insgesamt ist es jedoch trotz den Unterschieden möglich, mit Hilfe der Analysen aus beiden Ämtern einen generellen Eindruck über die Risiken und Verwundbarkeiten in den verschiedenen Teilsektoren zu gewinnen. Zudem soll die Herleitung von IKT-spezifischen Massnahmen für die Teilsektoren wieder ähnlich erfolgen. Das unterschiedliche Vorgehen beeinträchtigt deshalb die Erfüllung der Massnahmenziele nicht.

<u>Outcome: Ziele sind erreicht:</u>

Die IKT-Verwundbarkeiten in den bearbeiteten Teilsektoren sind identifiziert und nachvollziehbar bewertet. Erste Massnahmenvorschläge werden bereits in den Schlussberichten der M2 gemacht, werden aber in separaten Massnahmenberichten im Rahmen der M12 weiter ausgearbeitet. Aus den vorliegenden Dokumenten ist erkennbar, dass konkrete und in den Sektoren gut abgestützte Vorschläge ausgearbeitet werden.
Die Herausforderung liegt in der Begleitung der Massnahmenumsetzung und in der Aktualisierung der vorgelegten Analysen. Diesbezüglich muss das weitere Vorgehen noch ausgearbeitet werden.

- **IKT-Verwundbarkeiten in kritischen Teilsektoren identifiziert:** In den zum Zeitpunkt der Wirksamkeitsüberprüfung vorliegenden Berichten wurden die IKT-Verwundbarkeiten systematisch analysiert und nachvollziehbar bewertet. Da die IKT-

Verwundbarkeiten nicht in jedem Teilsektor gleich wichtig sind, sind die Berichte entsprechend unterschiedlich detailliert.

- **Erarbeitung von Massnahmen:** In den Analysen sind bereits Massnahmenvorschläge beschrieben. Die Ausarbeitung der Massnahmen erfolgt wiederum in enger Zusammenarbeit mit den Experten aus den Branchen sowie verantwortlichen Behörden und Verbänden und wird in den Berichten der Massnahme 12 festgehalten. Zum Zeitpunkt der Wirksamkeitsüberprüfung lagen erst ein solcher Bericht (Teilsektor Erdgasversorgung) sowie ein generelles Konzept zur Erstellung der Berichte vor. Es ist erkennbar, dass auf der Grundlage der Risiko- und Verwundbarkeitsanalysen und in Zusammenarbeit mit den Branchenvertretern und den Regulatoren konkrete Massnahmen formuliert werden können (beispielsweise das Ausrollen von Polycom zur Sicherung der Kommunikation bei Betreibern kritischer Infrastrukturen). In einigen Teilsektoren erfolgte als Resultat der Arbeiten die Aufnahme von wichtigen Betreibern kritischer Infrastrukturen in den geschlossenen Kundenkreis von MELANI.
- **Berücksichtigung laufender Projekte:** Die Digitalisierung führt dazu, dass in vielen Sektoren neue IKT-Verwundbarkeiten entstehen. Die Risiko- und Verwundbarkeitsanalysen bieten darum auch jeweils einen Ausblick auf mögliche kommende Herausforderungen. Es ist klar, dass die Analysen aufgrund des technologischen Wandels einer regelmässigen Aktualisierung bedürfen. Es wird jedoch kein Turnus für die Aktualisierung definiert.
- **Zusammenarbeit innerhalb Teilsektoren gestärkt:** Die Zusammenarbeit in den Teilsektoren hat bereits vor der NCS funktioniert (auch dank den Arbeiten des BABS im Rahmen der SKI-Strategie und des BWL im Rahmen ihrer Kaderorganisation) und funktioniert heute noch besser. Die Arbeiten haben insbesondere dazu beigetragen, dass die verschiedenen Akteure der jeweiligen Teilsektoren besser in die Risiko- und Verwundbarkeitsanalysen miteinbezogen werden.
- **Sensibilisierung der KI-Teilsektoren:** Einige Teilsektoren (z. B. Banken) sind schon stark gegenüber Cyber-Risiken sensibilisiert, andere Teilsektoren waren dies noch kaum (z. B. Strassenverkehr oder Medien). In diesen Sektoren konnte ein wichtiger Beitrag zur Sensibilisierung geleistet werden. Diverse Anfragen an das BABS und das BWL bestätigen, dass seitens der Betreiber kritischer Infrastrukturen die Sensibilität für die Themen stark gestiegen ist.

<u>Impact: kann aktuell nicht beurteil werden</u>

Einen Impact haben die Massnahmen M2 und M12 dann erreicht, wenn die Teilsektoren konkrete Massnahmen zur Minderung der IKT-Risiken und Verwundbarkeiten umsetzen und so ihre Cyber-Risiken reduzieren. Vereinzelt ist dies schon geschehen (z. B. im Sektor Erdgas). Es ist jedoch zu früh, um den Effekt dieser Bemühungen und damit den Impact der Massnahmen insgesamt zu beurteilen.

3.2. M3 Prävention & Kontinuität: Verwundbarkeitsanalyse IKT-Infrastruktur

Titel Massnahme	M3: Verwundbarkeitsanalyse IKT-Infrastruktur
Bereich	Prävention
Ziele	Die Verantwortlichen der Generalsekretariate und die zuständigen Leistungserbringer erhalten ein Prüfkonzept, womit sie die IKT-Landschaft der Bundesverwaltung auf systemische, organisatorische und technische Verwundbarkeiten hin untersuchen und die IT-Risiken erkennen können. Die Erarbeitung des Prüfkonzepts ist mit Unterstützung der Leistungserbringer BIT und FUB erfolgt und wurde mit laufenden Projekten koordiniert. Die Ergebnisse sind in Zusammenarbeit mit MELANI zu einer gesamtheitlichen Analyse der Bedrohungslage konsolidiert. Das Prüfkonzept identifiziert die IT-Risiken für jeden kritischen Prozess und definiert die jeweils systemrelevanten Mindeststandards. Die Kantone, die Wirtschaft und die KI-Betreiber erhalten bei Interesse dieses Prüfkonzept der IKT-Infrastrukturen der Bundesverwaltung zur Verwendung für die eigenen Verwundbarkeits-Überprüfungen
Verantwortliches Amt / Organisationseinheit	ISB
Konsultierte Unterlagen für die WiÜ	Quellen: [65], [66], [67], [68], [69], [70]
Interviews	Siehe Anhang A.1, Interview I 7

3.2.1. *Erwartete Wirkung: Wirkungsmodell M3*

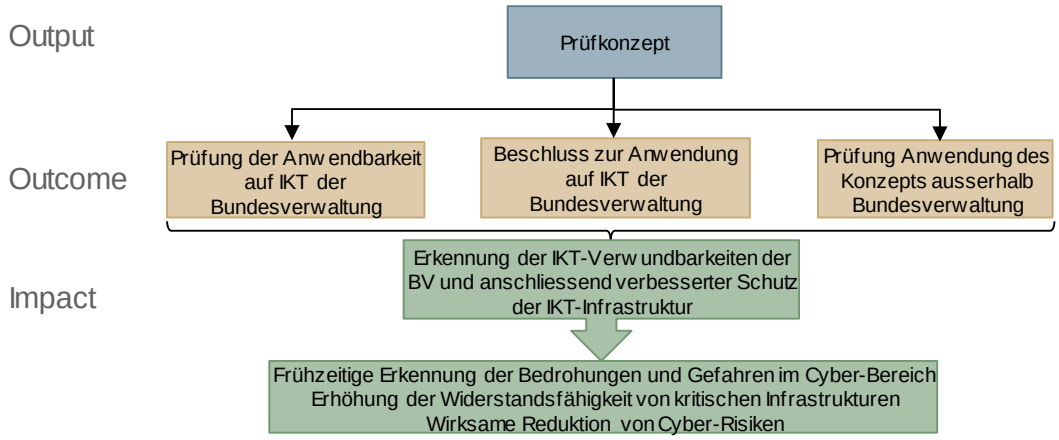

Abbildung 3 Wirkungsmodell M3

3.2.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Eine befristete Stelle (100%) am ISB bis 31.12.2015
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	Konsultationen bei BIT, FUB und im Informatikrat des Bundes (IRB)

Bemerkungen:

Für die Erarbeitung des Prüfkonzepts wurde eine zusätzliche befristete Stelle bis Ende 2015 mit einer dafür geeigneten Person besetzt. Für die Erstellung des Prüfkonzepts wurden die Leistungserbringer BIT und FUB sowie der Informatikrat des Bundes IRB miteinbezogen. Generell wurde der Ressourcenbedarf, insbesondere die Mittel für die Überprüfung der Umsetzbarkeit, deutlich unterschätzt.

3.2.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output		✖		
Outcome	☐ aktuell nicht beurteilbar			
Impact	☐ aktuell nicht beurteilbar			

3.2.4. *Begründung der Beurteilung*

Output: Ziele nur teilweise erreicht:

> Zwar wurde ein Konzept zur Analyse der IKT-Verwundbarkeiten in der Bundesverwaltung erstellt, dieses wurde aber vom STA NCS nicht abgenommen, da er die Umsetzung des Konzepts angesichts des hohen Aufwandes für unrealistisch hielt. In der daraufhin vom STA NCS beschlossenen Sondermassnahme ist eine Alternative entwickelt worden. Insgesamt sind die Arbeiten nicht so weit fortgeschritten wie ursprünglich geplant.

Im Rahmen der M3 wurde ein Prüfkonzept zur vollständigen Erfassung und systematischen Bewertung der IKT-Verwundbarkeiten in der Bundesverwaltung erarbeitet. Das Konzept basiert auf der international anerkannten „Information Risk Assessment Methodology“ (IRAM) und auf vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Standards zur IKT-Risikoanalyse.

Bereits im Grobkonzept wurde festgestellt, dass bei einer strikten Einhaltung der Standards der ursprüngliche Auftrag der IKT-Verwundbarkeitsanalyse erweitert werden muss, da dieser keine systematische Berücksichtigung der Geschäftsprozesse, der Gefahren und Bedrohungen verlangte, sondern nur die Verwundbarkeiten berücksichtigte. Bei der weiteren Ausarbeitung des Prüfkonzepts hat sich aber gezeigt, dass die Umsetzung einer ausführlichen Analyse der IKT-Risiken zu grossen personellen und finanziellen Aufwänden führen würde. Dieser Befund wurde auch in den auftragsgemäss durchgeführten Konsultationen der Leistungserbringern BIT und FUB bestätigt, welche das Konzept zwar als zielführend aber sehr ressourcenintensiv bewertet haben. Vor dem Hintergrund unveränderbarer Ressourcenmittel bewerteten die Mitglieder des IRB das Konzept als theoretisch richtig, stellten aber auf dem Prüfstand der Realität die Verhältnismässigkeit und den effektiven Mehrwert in Frage.

Innerhalb des STA NCS stiess das Konzept auf Kritik [65]. Die wichtigsten Kritikpunkt waren der fehlende Fokus auf das Erkennen von IKT-Verwundbarkeiten, der Mangel an klaren Handlungsanweisungen und der fragliche Mehrwert einer umfassenden und stark standardisierten Analyse von IKT-Risiken. Der STA NCS hat aus diesen Gründen eine Sondermassnahme zu M3 beschlossen. Es soll eine Alternative zum erarbeiteten Prüfkonzept entwickelt werden, die ein pragmatisches und einfach umsetzbares Vorgehen zur Erfassung von IKT-Verwundbarkeiten skizziert. Das ISB hat ein solches Konzept erstellt, das mit deutlich weniger Ressourcen umgesetzt werden kann. Das Konzept war

zum Zeitpunkt der WiÜ noch nicht vom STA NCS abgenommen, stiess aber in den Vorkonsultationen auf breite Zustimmung. Da es sich erst um eine Vorgehensskizze handelt, werden weitere Arbeiten nötig sein, um die IKT-Verwundbarkeitsanalyse in der Bundesverwaltung systematisch einzuführen. Insgesamt muss darum festgehalten werden, dass die Arbeiten nicht so weit fortgeschritten sind, wie ursprünglich beabsichtigt.

Outcome: aktuell nicht beurteilbar

Die Alternative lag zum Zeitpunkt der WiÜ als Skizze vor und wird in ersten Stellungsnahmen als umsetzbar eingestuft. Vor einem allfälligen Beschluss zur Anwendung dieses Ansatzes, muss die Alternative noch weiter konkretisiert werden. Es fand noch keine Überprüfung zur Anwendbarkeit des Konzepts ausserhalb der Bundesverwaltung statt.

- Anwendbarkeit des Prüfkonzepts auf die Bundesverwaltung: Die vorbereitete systematische Überprüfung fand nicht statt, da deren Durchführung angesichts knapper Mittel und im Rahmen der eingestellten Budgets als zu ressourcenintensiv eingestuft wurde. Erst mit der erarbeiteten Alternative wird es möglich sein, die Anwendbarkeit einer IKT-Verwundbarkeitsanalyse in der Bundesverwaltung detailliert zu prüfen.
- Beschluss zur Anwendung auf IKT der Bundesverwaltung: Es gab keinen Beschluss, weil zuerst das alternative Konzept geprüft wird.
- Prüfung zur Anwendung des Konzepts ausserhalb der Bundesverwaltung: eine Prüfung ist nicht sinnvoll, bevor nicht über die Anwendung innerhalb der Bundesverwaltung entschieden wurde.

Impact: aktuell nicht beurteilbar

Da kein Entscheid zur Anwendung des Prüfkonzepts getroffen wurde und eine Alternative noch in Arbeit ist, kann der Impact nicht beurteilt werden. Bisher beschränkt sich die Wirkung der Massnahme darauf, dass eine Sensibilisierung der verantwortlichen Stellen in den Departementen für die Wichtigkeit von Verwundbarkeitsanalysen stattgefunden hat.

3.3. M4 Prävention & Kontinuität: Erstellung Lagebild und Lageentwicklung

Titel Massnahme	M4: Erstellung Lagebild und Lageentwicklung
Bereich	Prävention
Ziele	Die relevanten und verantwortlichen Akteure aus Politik, Wirtschaft und Gesellschaft können sich über Cyber-Vorfälle von nationaler Bedeutung informieren. Es werden ihnen dazu stufengerecht für die jeweiligen Verantwortungsbereiche aufgearbeitete Analysen zur Verfügung gestellt, die über das Lagebild und die Lageentwicklung Auskunft geben. Diese Erkenntnisse werden im Rahmen des Public Private Partnership-Modells von MELANI gesammelt, bewertet, analysiert und in einer Lagedarstellung fusioniert. Das notwendige Cyber-Spezialwissen und die technischen Kapazitäten werden dazu ausgebaut, wie auch die Plattform für den freiwilligen Informationsaustausch mit ausgewählten KI-Betreibern und der Wirtschaft gestärkt.
Verantwortliches Amt / Organisationseinheit	MELANI, NDB
Konsultierte Unterlagen für die WiÜ	Quellen: [71], [72], [73], [74], [75], [76], [77], [78], [79]
Interviews	Siehe Anhang A.1, Interview I 2

3.3.1. *Erwartete Wirkung: Wirkungsmodell*

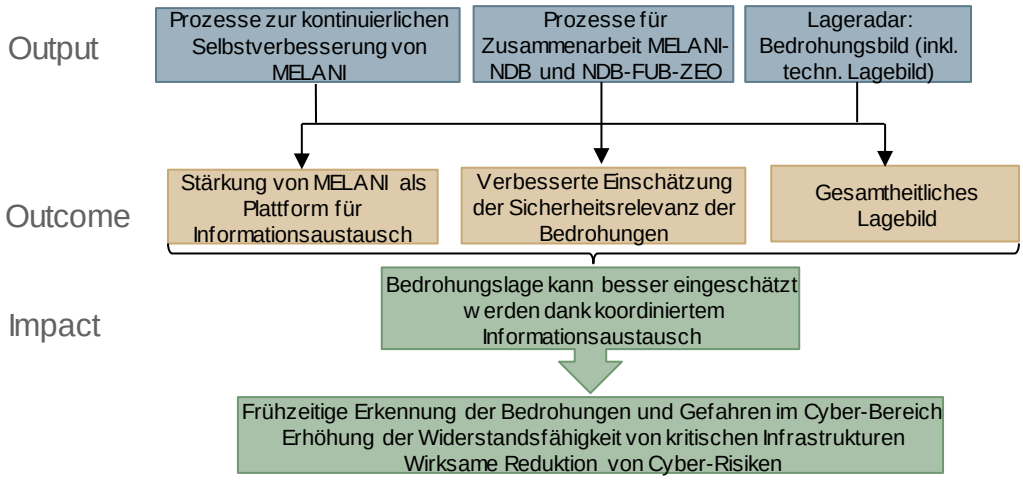

Abbildung 4 Wirkungsmodell M4

3.3.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen [Ressourcenpool für M4, M5, M14]	3 MELANI-ISB 3 MELANI-OIC (NDB) 7 NDB 1 MND 4 FUB
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	Beteiligte Stellen neben MELANI, NDB, MND und FUB: BIT, KOBIK

<u>Bemerkungen zu den Stellen des NDB:</u> Die geschaffenen Stellen im Cyber-Bereich werden (mit Ausnahme der Beschaffungsstellen) in einer neue Organisationseinheit (Cyber NDB) zusammengefasst. Daneben wurde noch das Fachkommissariat Cyber geschaffen.

Die eingestellten Mitarbeitenden haben eine für die Fachaufgabe notwendige Qualifikation. Insbesondere verfügen sie nicht nur über die technischen Fähigkeiten sondern auch über die notwendigen Soft-Skills. Wenig hilfreich für die Rekrutierung war die Befristung der Verträge.

Der Umfang der benötigten personellen Ressourcen wurde richtig eingestuft (die gleichen Ressourcen werden auch für M5 und M14 genutzt, vgl. Kapitel 3.4.2. und 3.6.2). Allerdings wird aktuell neuer Bedarf identifiziert, z. B. zur Erarbeitung von neuen Produkten oder für eine schärfere und vertiefte Analyse.

3.3.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome			✓	
Impact	◎ wurde erzielt			

3.3.4. *Begründung der Beurteilung*

<u>Output: Ziele grösstenteils erreicht:</u>

> Die Prozesse zur Selbstverbesserung von MELANI und zur Stärkung der Zusammenarbeit MELANI-NDB und NDB-FUB-ZEO sind erstellt oder die Arbeiten dazu weit fortgeschritten. Ein Prototyp des Lageradars besteht. Der Lageradar wird aber weiter ausgebaut werden müssen, damit er ein gesamtheitliches Lagebild vermitteln kann.

Die im Wirkungsmodell definierten Outputs konnten grösstenteils erzielt werden:

- **Prozesse zur kontinuierlichen Selbstverbesserung von MELANI:** Das Konzept zur kontinuierlichen Selbstverbesserung von MELANI ist in Erarbeitung. Es soll bis Ende 2016 vorliegen und von einer externen Firma separat begutachtet werden. Es basiert auf den in Massnahme 13 erhobenen Kundenbedürfnissen und auf dem Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch, das bereits vorliegt. Die im Konzept zur Selbstverbesserung definierten Prozesse sollen in periodischen Sitzungen überprüft und bei Bedarf an die neue Bedrohungslage angepasst werden.
- **Prozesse für die Zusammenarbeit MELANI-NDB und NDB-FUB-ZEO:** Die Prozesse für die Zusammenarbeit zwischen MELANI und NDB, dem NDB und der FUB-ZEO sowie für den Einbezug von internationalen Partnern sind in einem Leitfaden definiert und werden auch gelebt. Die Zusammenarbeit zwischen MELANI und dem NDB ist sehr gut, eng und hat sich seit mehreren Jahren bewährt. Die Zusammenarbeit zwischen dem NDB und FUB-ZEO wurde durch entsprechenden Leistungsvereinbarungen gestärkt.

  Aus Sicht der Massnahmenverantwortlichen ist die Zusammenarbeit auch deshalb so gut, weil man sich im Cyber-Bereich untereinander gut kennt und sich auf bilateralem Weg austauschen kann. Die Leistungsvereinbarung wird als ausreichend eingestuft, muss aber stetig überprüft und bei Bedarf angepasst werden. Bundesintern sind alle relevanten Akteure identifiziert und involviert und auch hier wird die Zusammenarbeit als grundsätzlich sehr kooperativ und sachorientiert bewertet. Wichtig ist auch, dass unter der Federführung des OIC MELANI regelmässige Koordinationssitzungen zwischen den wichtigsten operativen und technischen Akteuren (GovCERT, FUB-ZEO CNO, Cyber NDB, BIT-CSIRT, MilCERT und Cyber MND) zwecks gesamtheitlicher Analyse der Bedrohungslage und Koordination bei der Behandlung von Vorfällen, stattfinden.
- **Gesamtheitliches Lagebild** (inkl. technisches Lagebild): Ein Prototyp zur Darstellung der Bedrohungslage, der sogenannte Lageradar, wurde erstellt und im Herbst 2016 in seiner Endversion vorliegen. Dieses Produkt wird den kritischen Infrastrukturen als Monitoring Instrument mit sektorspezifischen Informationen zur Verfügung gestellt. Informationsquellen für den Radar sind die Erkenntnisse des NDB, techni-

sche Analysen des GovCERT und Informationen der polizeilichen Ermittler, welche über KOBIK einfliessen.

Der Lageradar wird aber noch weiterentwickelt werden müssen, damit er effektiv ein gesamtheitliches Lagebild vermitteln kann. Es können aktuell noch keine Fallkomplexe mit allen Zusammenhängen dargestellt werden. Zudem hängt die Qualität des Lageradars davon ab, dass MELANI genügend Ressourcen zur Verarbeitung und Einspeisung von relevanten Informationen zur Verfügung hat und den Informationsaustausch mit den kritischen Infrastrukturen weiter stärken kann.

Outcome: Ziele sind grösstenteils erreicht:

Mit dem Lageradar wurde ein wichtiges Instrument für die Darstellung eines gesamtheitlichen Lagebilds geschaffen. Damit die im Lageradar gezeigte Lageeinschätzung akkurat und zeitgemäss ist, muss der Informationsaustausch zwischen den Beteiligten und den Betreibern von KI weiter gestärkt werden.
Ein erster Schritt dazu ist der weitere Ausbau des geschlossenen Kundenkreises (GK) von MELANI. Es fehlt jedoch bisher eine klare strategische Ausrichtung für das weitere Wachstum des GK.

- **Stärkung MELANI als Plattform für den Informationsaustausch:** MELANI ist seit seiner Gründung im Jahr 2004 stark gewachsen und konnte den „geschlossenen Kundenkreis“ (GK), der sich aus den Vertretern von kritischen Infrastrukturen zusammensetzt, weiter ausbauen. Heute sind über 190 Schweizer Grossunternehmen und Verwaltungseinheiten in zehn Sektoren vertreten und können sicherheitsrelevante Informationen beziehen und teilen. Für die Stärkung des Informationsaustausches ist ein weiterer Ausbau des GK nötig. Es gibt jedoch noch keine definierte Strategie, wie dieser Ausbau weitergetrieben werden soll. Die Frage nach der Beteiligung am Informationsaustausch von Firmen, die nicht zu den kritischen Infrastrukturen gehören, ist nicht geklärt. Ideen für ein „Kreismodell“ mit verschiedenen Kundenkreisen (und entsprechenden Rechten/Pflichten) müssen weiter ausgearbeitet werden.
- **Verbesserte Einschätzung der Sicherheitsrelevanz der Bedrohungen:** Durch den erfolgten Ausbau des GK kann die Einschätzung der Sicherheitsrelevanz der Bedrohungen verbessert werden. Je mehr Akteure sich am Informationsaustausch beteiligen, desto genauer wird das Bild zur Bedrohungslage. Die gesammelten Informationen müssen aber auch mit der notwendigen Sorgfalt interpretiert werden, was nur mit einem zusätzlichen Aufwand erfolgen kann. Der Umfang und die Schärfe der Analyse sind durch die verfügbaren Ressourcen limitiert [73] Mit den heutigen Ressourcen ist ein weiterer Ausbau nur schwer realisierbar.
- **Gesamtheitliches Lagebild und Lageentwicklung:** Mit dem Lageradar wurde ein Instrument entwickelt, das einen aktuellen Überblick zur Lage ermöglicht, da der Lageradar eine Echtzeitdarstellung ist. Zusätzlich können betroffene Akteure zeitnah angesprochen werden, da ein 24*7 Pikettdienst (inkl. SMS-Dienst) bei MELANI OIC existiert. Die Informationen führten bereits zu einer höheren Handlungsfähigkeit. Folgende Beispiele haben dies gezeigt:
  - DDoS Angriffe: Durch die internationale Zusammenarbeit konnten Unternehmen rechtzeitig vorinformiert und entsprechende Gegenmassnahmen eingeleitet werden.
  - Heartblead: Das Lagebild hat dazu geführt, dass die Bedrohungen besser eingeschätzt werden konnte.

– Bedrohung in der Presse für das WEF: Die klaren Aussagen aufgrund des Lagebildes haben zur richtigen Einschätzung geführt, dass keine akute Bedrohung für das WEF besteht.

Das hohe Ziel eines gesamtheitlichen Lagebildes kann aber nur erreicht werden, wenn der Informationsaustausch und die Zusammenarbeit mit allen Beteiligten Partnern weiter gestärkt wird. Um den Auftrag zur Massnahme 4 vollumfänglich zu erfüllen, müssten zusätzliche Ressourcen gesprochen werden.

Impact: wurde erzielt:

Die Bedrohungslage kann heute besser eingeschätzt werden, da der Informationsaustausch zwischen den Akteuren NDB, MELANI, MND, Leistungserbringer und Betreiber kritischer Infrastrukturen koordiniert ist. Der Aufbau des Cyber NDB führte mehrfach zum frühzeitigen Erkennen von Angriffen und Bedrohungen. Der Lageradar ermöglicht die Übersicht der Bedrohungen und die Einschätzung der Sicherheitsrelevanz dieser Bedrohungen für die Schweiz.

Wichtig für die verbesserte Lageeinschätzung ist auch die verbesserte Attributionsfähigkeit des NDB. Es gelingt dank der intensiven Zusammenarbeit der Akteure und den wichtigen Kontakten des NDB zu Partnerdiensten vermehrt, die Täterschaft zu identifizieren. Diese Informationen sind für die Einschätzung der Lage von sehr grosser Bedeutung (mehr dazu in Kapitel 3.6).

3.4. M5 Reaktion: Vorfall-Analyse und Nachbearbeitung von Vorfällen

Titel Massnahme	Vorfall-Analyse und Nachbearbeitung von Vorfällen
Bereich	Reaktion
Ziele	Der Bund, die Kantone und die KI-Betreiber haben ihre eigenen Massnahmen im Umgang mit Vorfällen überprüft und weiterentwickelt. Die Erkenntnisse aus relevanten Vorfällen (Incident durch Malware, Botnetze, Trojaner) werden an MELANI weitergegeben, wozu bundesinterne und -externe Prozesse etabliert sind. Bei der Nachbearbeitung relevanter Vorfälle werden KI-Betreiber und IKT-Leistungserbringer auf Wunsch von MELANI technisch unterstützt. Erkenntnisse zu Staatsschutz relevanten Vorfällen im Zusammenhang mit Cyber-Risiken werden vom NDB an MELANI weitergegeben. Die technischen Kapazitäten zur Überwachung der Bundesnetze sind innerhalb der Dienstleistungserbringer (CERTs) aufgebaut. Plattformen und Infrastrukturen zur Erkennung und Eindämmung von Cyber-Bedrohungen, sowie technische Unterstützung der kritischen Infrastrukturbetreiber sind etabliert. Ebenfalls sind bei den relevanten Bundesstellen das Spezialwissen und die forensischen Fähigkeiten zur Erkennung und Bekämpfung von Cyber-Bedrohungen ausgebaut.
Verantwortliches Amt / Organisationseinheit	MELANI und NDB
Konsultierte Unterlagen für die WiÜ	Quellen: [80], [81], [82], [83]
Interviews	Siehe Anhang A.1, Interview I 10

3.4.1. *Erwartete Wirkung: Wirkungsmodell M5*

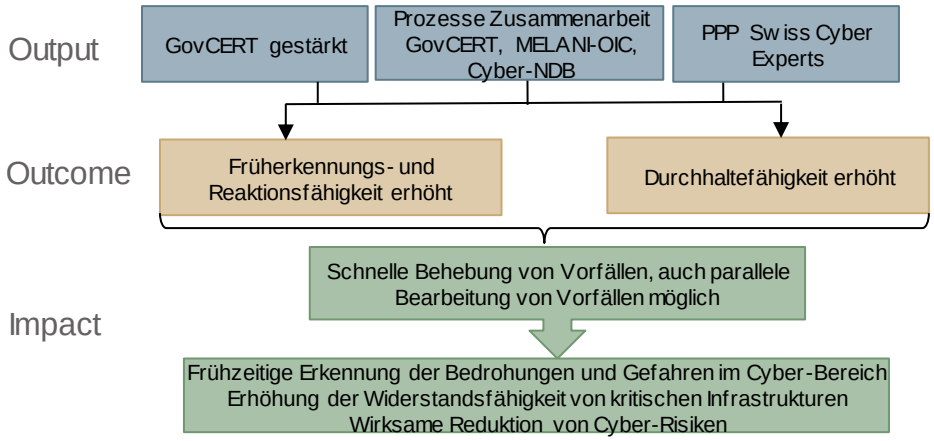

Abbildung 5 Wirkungsmodell M5

3.4.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen [Ressourcenpool für M4, M5, M14]	3 MELANI-ISB 3 MELANI-OIC (NDB) 7 NDB 1 MND 4 FUB
Finanzielle Mittel	Keine
Mitarbeit durch andere Ämter / Organisationseinheiten	Zusammenarbeit mit CSIRT des BIT

<u>Bemerkungen zu den Stellen MELANI-ISB und MELANI-OIC:</u>

Für die Umsetzung der NCS wurden im GovCERT (MELANI ISB) drei zusätzliche Stellen bewilligt. Ebenfalls drei Stellen erhielt das MELANI OIC im NDB. Aktuell (per 01.08.2016) hat das GovCERT insgesamt 460 Stellenprozente besetzt (geplant sind 560 Stellenprozente). Das OIC ist mit 8 FTEs besetzt. Zuerst wurde dadurch der Normalbetrieb für die Vorfallbehandlung sichergestellt. Zudem besteht heute auch die Möglichkeit, zwei grössere Vorfälle parallel zu behandeln.

Durch die engen Kontakte zu verwandten Stellen wie dem CSIRT-BIT, und ZEO können im Falle einer Krise weitere, gut ausgebildete Personen aus der Bundesverwaltung zur Bewältigung beigezogen werden.

Würden die entsprechenden Ressourcen nach 2017 nicht mehr zur Verfügung stehen, könnte der Grundauftrag von MELANI (Schutz der kritischen Infrastrukturen in der Schweiz sowie die Unterstützung in einer Cyber-Krise) nicht mehr mit der gewohnten Qualität durchgeführt werden. Das technische Wissen würde fehlen, die nationale und internationale Vernetzung würde massiv an Qualität einbüssen.

3.4.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome			✓	
Impact	◎ wurde erzielt			

3.4.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht:</u>

Die Kapazitäten zur Vorfallbewältigung konnten klar gestärkt werden. Dies gelang durch einen Ausbau der Ressourcen im GovCERT sowie dem OIC MELANI und durch eine verbesserte Zusammenarbeit aller Akteure. Für eine vollständige Umsetzung fehlt die vorgesehene Erstellung einer sicheren Kommunikationsplattform zum Austausch von Informationen über Vorfälle.

- **Die operativen Einheiten von MELANI (GovCERT und OIC MELANI) wurden gestärkt:** Das Swiss Government CERT (GovCERT) konnte seine Leistungen dank einer Verbesserung der personellen Situation bei MELANI deutlich hochfahren. Es ist deshalb heute bedeutend resilienter als noch vor wenigen Jahren. Zudem wurde 2013 die Organisationsstruktur des GovCERT definiert. Durch die Stärkung des analytischen Teils von MELANI im NDB (OIC MELANI) konnte der damit einhergehende zusätzliche Arbeitsaufwand zur Bearbeitung der anfallenden Informationen im Bereich Auswertung, Einschätzung und Kommunikation mit den kritischen Infrastrukturen gehandhabt werden.
- **Cyber NDB ist operativ:** Der neu gebildete Bereich Cyber-NDB hat seinen Platz innerhalb des NDB gefunden und ist auch international sehr aktiv. Mit Analysen, Quellennetz und internationalen Kontakten wurden Vorfälle frühzeitig erkannt, Attributionen vorgenommen und konnten Bedrohungen rechtzeitig eingestuft werden.
- **Die Prozesse der Zusammenarbeit GovCERT, MELANI-OIC und Cyber NDB wurden definiert:** Parallel zur Stärkung GovCERT und MELANI OIC wurden auf nachrichtendienstlicher Seite die Konzeptarbeiten zur Strukturierung der Cyberfähigkeiten des NDB abgeschlossen und die relevanten Stellenprofile zur Vorfallanalyse geschaffen. Der Wissenstransfer auf verschiedenen Kommunikationsplattformen, eine Webseite mit Vorfallmeldeformular sowie eine Malware Information Sharing Plattform (MISP Plattform) konnten ebenfalls aktiv auf- und ausgebaut werden. Erreicht wurde zudem eine Stärkung der Prozesse für den Wissensaustausch, eine Erhöhung der Durchalte- und Detektionsfähigkeiten und eine bessere Vernetzung mit diversen nationalen und internationalen CERTs (über persönliche Kontakte und Mitgliedschaften bei FIRST und EGC). Dadurch können Daten im Incident Fall so analysiert und aufbereiten werden, dass die angegriffene Organisation technische Gegenmassnahmen ergreifen kann. Durch etablierte Plattformen, Strukturen und Prozesse können die bearbeiteten Vorfälle als „Lessons Learned“ wieder zurück in die Prävention fliessen und so das Bedrohungsbild auf den aktuellen Stand gebracht werden. Damit ist man insgesamt besser vorbereitet. Noch nicht erreicht wurde der geplante Aufbau einer sicheren Kommunikationsplattform, auf der alle relevanten Akteure Informationen zu Vorfällen einfach und zeitnah austauschen können.
- **Die PPP Swiss Cyber Experts wurden gegründet:** Durch die Gründung der Public Private Partnership Swiss Cyber Experts (ein Verein aus Vertretern der IKT-

Industrie) konnte eine zusätzliche Organisation mit spezialisiertem Know-how etabliert werden, auf die man im Falle eines schweren Cyber-Vorfalls zurückgreifen kann.

Outcome: Ziele sind grösstenteils erreicht:

Dank den grösseren Kapazitäten werden Vorfälle heute schneller erkannt, es kann rascher darauf reagiert werden. Auch die Durchhaltefähigkeit im Falle von anhaltenden Bedrohungen konnte gestärkt werden. Für die Bewältigung von ausserordentlichen Lagen sind die Ressourcen jedoch nach wie vor zu knapp. Ebenfalls muss laufend überprüft werden, welche spezialisierten Fähigkeiten zusätzlich im GovCERT, sowie im OIC MELANI benötigt werden.

- **Früherkennungs- und Reaktionsfähigkeit wurde erhöht:** Mit der Verabschiedung der NCS wurde der Auftrag zur Vorfallbearbeitung von MELANI erweitert. Um diesen Auftrag zu erfüllen, wurden innerhalb des GovCERT und des Cyber-NDB die Fähigkeiten zum Threat Management sowie die analytischen und forensischen Kapazitäten ausgebaut. Dank diesem Ausbau und der verstärkten Zusammenarbeit zwischen dem GovCERT, BIT-CSIRT und dem koordinierenden, im Nachrichtendienst angesiedelten MELANI-OIC können Vorfälle heute schneller entdeckt werden. Ausserdem kann gezielt darauf reagiert werden. Die Zufriedenheit der Betreiber kritischer Infrastrukturen mit der Hilfe von MELANI bei Vorfällen ist sehr gross (Quelle: Umfrage im geschlossenen Kundenkreis).

  Trotz des erfolgten Wissensaufbaus bestehen noch Lücken im technischen Know-how. Dies betrifft insbesondere die wichtige Frage der Sicherheit von SCADA-Systemen. Die Herausforderung besteht dort darin, dass je nach System hoch spezialisiertes Wissen nötig ist. Die Zusammenarbeit mit Spezialisten aus den entsprechenden Bereichen muss weiter gestärkt werden.

- **Durchhaltefähigkeit wurde erhöht:** Für die normale Lage reichen die aktuellen Stellen aus. Bei allenfalls eintretenden ausserordentlichen Lagen, die über mehrere Tage oder Wochen anhalten würden, sind die vorhandenen Ressourcen ungenügend. Bei parallelen Vorfällen käme man mit den heutigen Ressourcen schon bald an die Grenzen. Die Vernetzung zu CERTs der Privatwirtschaft muss deshalb gestärkt werden. Zusätzlich zu den schon vorhandenen guten Kontakten zu grösseren CERTs sollten auch kleiner Response-Teams in das Netzwerk von MELANI, speziell dem technischen Kompetenzzentrum GovCERT integriert werden.

Impact: wurde erzielt

Die grösseren Kapazitäten zur Vorfallbewältigung mussten bereits bei verschiedenen Vorfällen eingesetzt werden. Es hat sich gezeigt, dass die ergriffenen Massnahmen wirkungsvoll waren.

Das Spezialwissen und Fähigkeiten sowie Durchhaltefähigkeit der operativen Teile von MELANI (GovCERT und OIC MELANI) konnten genutzt werden, um Vorfälle effizient und effektiv zu bewältigen. Auch eine parallele Bearbeitung von Vorfällen ist nun dank dem erfolgten Ressourcenausbau möglich. Durch die verbesserte Früherkennung ist man in der Lage, rascher auf Vorfälle zu reagieren und diese zu beheben.

3.5. M6 Reaktion: Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe

Titel Massnahme	Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe
Ziele	Bund und Kantone haben den Weg ihrer künftigen Zusammenarbeit zur Koordination interkantonaler Fallkomplexe in einem Konzept festgehalten, das dem Bundesrat vorgelegt wird. Dieses beschreibt, wie auf nationaler Ebene eine möglichst vollständige Fallübersicht (Straffälle) geführt werden soll, und gibt so auch Auskunft über die Ausgestaltung der Schnittstellen mit weiteren Akteuren auf dem Gebiet der Minimierung von Cyber-Risiken und über die Prozesse des Informationsflusses für die Lagedarstellung. Die Koordination interkantonaler Fallkomplexe ist mit den bereits bestehenden internationalen Bestrebungen zur strafrechtlichen Verfolgung von Cyber-Risiken abzustimmen. Auch weist das Konzept aus, ob auf Stufe Bund und Kantone rechtliche Grundlagen anzupassen und Ressourcen für die Umsetzung des Konzepts bereitzustellen sind. Informationen aus der Fallübersicht (Straffälle) und Erkenntnisse zu Fallkomplexen aus der technisch-operativen Analyse der Strafverfolgung in Strafverfahren werden fortlaufend an MELANI weitergegeben. Im Gegenzug lässt MELANI KOBIK strafrechtsrelevante Informationen aus ihren Erkenntnissen (CERT- und ND-Informationen) fortlaufend zukommen. Hierfür sind bundesinterne und -externe Prozesse etabliert.
Verantwortliches Amt / Organisationseinheit	KOBIK
Konsultierte Unterlagen für die WiÜ	Quellen: [84], [85], [86], [87], [88], [89]
Interviews	Siehe Anhang A.1, Interview I 6

3.5.1. Erwartete Wirkung: Wirkungsmodell M6

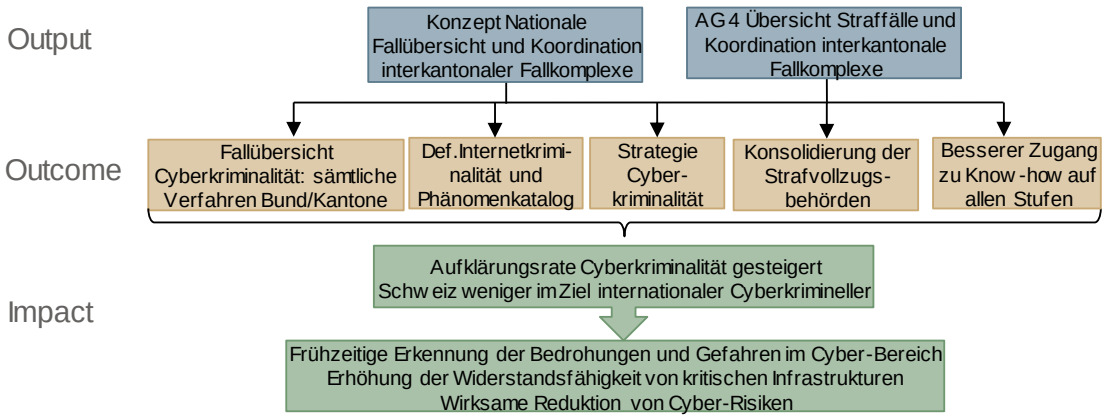

Abbildung 6 Wirkungsmodell M6

3.5.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Eine befristete Stelle (100%) für 2 Jahre.
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	

Für die Umsetzung der NCS wurde eine befristete Stelle (2 Jahre) zur Ausarbeitung des Konzepts bewilligt. Diese Stelle wurde jedoch nur 6 Monate lang genutzt. Die Rekrutierung von geeignetem Personal für die Stelle erwies sich als schwierig.

3.5.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome		✗		
Impact	☐ aktuell nicht beurteilbar			

3.5.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht:</u>

Das Konzept zur nationalen Fallübersicht ist fertig gestellt, muss aber noch verabschiedet werden. Es hat sich im Laufe der Arbeiten gezeigt, dass eine Gesamtstrategie Cyberkriminalität nötig ist, die über das Konzept hinausgeht. Der Austausch mit den Kantonen in der Arbeitsgruppe 4 war fruchtbar, über KOBIK bestand allerdings schon vorher eine gute Koordination zwischen Bund und Kantonen im Bereich Cyberkriminalität.

- **Konzept „Nationale Fallübersicht und Koordination interkantonaler Fallkomplexe“:** Das Dokument liegt vor und ist aus heutiger Sicht komplett. Es wird im Herbst 2016 der KKJPD und anschliessend dem Bundesrat vorgelegt. Ursprünglich war die Abnahme für den Frühling 2016 vorgesehen, es kam jedoch zu Verzögerungen, da die Absprachen mit den Kantonen – die das Konzept massgeblich umsetzten müssen – länger gedauert haben.

  Alle beteiligten Stellen wurden bei der Erarbeitung genügend eingebunden. MELANI steuerte die Anforderungsliste für das Lagebild bei und brachte sich durch die Arbeitsgruppe 4 (AG 4) des SVS bei der Erarbeitung des Konzepts ein. Die Kantone waren anfangs eher passiv involviert. Für sie war Sinn und Zweck dieser Massnahme nicht offensichtlich. Erst nachdem ein Phänomene-Katalog mit klaren Definitionen über die verschiedenen Formen von Cyberkriminalität vorlag, wurde auch den Kantonen der Nutzen bewusst und sie brachten sich anschliessend aktiv bei der Erarbeitung des Konzepts ein.

  Im Konzept werden allerdings keine Prozesse für die Erfassung der Fälle und die Erstellung einer Fallübersicht definiert. Es werden erst Varianten aufgezeigt, wer wann welche Informationen übermittelt und wo diese zu einer Fallübersicht konsolidiert werden. Diese Fragen sollen im Zuge der zu erstellenden Gesamtstrategie Cybercrime geklärt werden.

- **AG 4 Übersicht Straffälle und Koordination interkantonaler Fallkomplexe:** Die Arbeitsgruppe 4 des SVS war bei der Erstellung des Phänomene-Katalog hilfreich, weil die Kantone dort direkt in die Ausarbeitung der Definitionen von Fällen von Cyberkriminalität involviert waren. Im Rahmen der Arbeiten zum Konzept Fallübersicht wurde die AG 4 konsultiert, es gab jedoch keine direkte Mitarbeit der Mitglieder der Gruppe. Generell besteht über KOBIK schon seit langem eine intensive Zusammenarbeit zwischen Bund und Kantonen. Die AG 4 lieferte in Bezug auf die Stärkung der Zusammenarbeit nur einen beschränkten Mehrwert.

Outcome: Ziele sind nur teilweise erreicht:

Es gibt noch keine umfassende Fallübersicht zur Cyberkriminalität in der Schweiz, da noch nicht alle Kantone die entsprechenden Daten erfassen. Dank der erstellten Phänomene-Blätter sind nun aber die verschiedenen Arten von Cyberkriminalität beschrieben und gegeneinander abgegrenzt. Die Regelung der Zuständigkeiten konnte noch nicht gelöst werden und bleibt eine grosse Herausforderung. Sie wird nun im Rahmen der Ausarbeitung der Gesamtstrategie Cyberkriminalität angegangen.

- **Nationale Fallübersicht:** Bei der Erstellung des Konzepts zur Fallübersicht wurden die Kantone konsultiert. Sie haben auch in der Vernehmlassung ihre Stellungnahme abgegeben. Aktuell werden aber noch nicht in allen Kantonen Daten zu Cyberkriminalität erfasst. Deshalb ist im Moment noch keine umfassende Fallübersicht möglich. Das Abholen der Daten erfolgt manuell (KOBIK geht auf die Kantone proaktiv zu). Das Koordinationsvorgehen zur Erstellung der Fallübersicht ist mit den Kantonen und der Bundesanwaltschaft besprochen.
- **Definition Internetkriminalität und Phänomene-Katalog Cyberkriminalität:** Die Erstellung eines umfassenden Phänomene-Katalog zu den verschiedenen Formen von Cyberkriminalität ist ein wichtiger Schritt hin zur Fallübersicht und zur Stärkung der Zusammenarbeit in der Strafverfolgung. Er fördert das gemeinsame Verständnis und hilft, die Zuständigkeiten zu regeln. Ziel ist auch, ein Ausbildungsangebot für Polizisten auf die Beine zu stellen(Module im Angebot des Schweizerischen Polizei Instituts).
- **Strategie Cyberkriminalität:** Ein Resultat der Arbeiten an M6 war die Erkenntnis, dass eine Gesamtstrategie der Kantone zu Cyberkriminalität notwendig ist. Diese ist nun in Arbeit und wird im Einklang mit der NCS stehen. Sowohl M6 als auch die Gesamtstrategie werden von EJPD und Polizeidirektorenkonferenz zur Kenntnis genommen, sodass es keine Abweichungen geben wird. Die Arbeiten zur Strategie stehen aber noch am Anfang.
- **Konsolidierung der Strafverfolgungsbehörden:** Die Arbeiten zu M6 haben verdeutlicht, dass die Zuständigkeiten noch nicht ausreichend definiert sind. Hier steht auch noch bundesgerichtliche Rechtsprechung aus, z.B. im Zusammenhang mit Phishing-Fällen. Die Zusammenarbeit zwischen den Kantonen und dem Bund funktioniert aber dank KOBIK.
- **Besserer Zugang zu Know-how:** Die technische und analytische Ausbildung ist nicht direkt Bestandteil von M6. Über die Phänomen-Blätter soll die Ausbildung der Polizisten im Bereich Cyber-Kriminalität künftig gestärkt werden.

Impact: Nicht beurteilbar

Das Ziel der Reduktion der Cyberkriminalität ist im Moment nicht messbar. Die Strafverfolgungsbehörden verfügen heute noch nicht über eine ausreichende Datengrundlage, um diese Frage zu beurteilen. Angesichts der stark gestiegenen Aktivitäten von Cyber-Kriminellen muss das Ziel realistischerweise eher in der Eindämmung der Fälle von Cyber-Kriminalität als in deren effektiven Reduktion liegen.

3.6. M14 Reaktion: Aktive Massnahmen und Identifikation der Täterschaft

Titel Massnahme	Aktive Massnahmen und Identifikation der Täterschaft
Ziele	Im Falle einer spezifischen Bedrohung in Zusammenhang mit Cyber-Risiken verfügt der NDB in Kooperation mit ausländischen Partnern über die Fähigkeit zur Identifikation der Täterschaft. Dies mit Unterstützung von FUB und MND als Leistungserbringer. Die Bundesanwaltschaft erhält vom NDB, soweit rechtlich zulässig, Erkenntnisse über die Täterschaft. Wenn kein Strafverfahren eingeleitet wird, werden vom NDB aktive Gegenmassnahmen vorbereitet, auf der Basis der gültigen Rechtsgrundlagen.
Verantwortliches Amt / Organisationseinheit	MELANI OIC, NDB, ISB
Konsultierte Unterlagen für die WiÜ	Quellen: [71], [72], [73], [74], [75], [76], [77], [78], [79]
Interviews	Siehe Anhang A.1, Interview I 2

3.6.1. Erwartete Wirkung: Wirkungsmodell M14

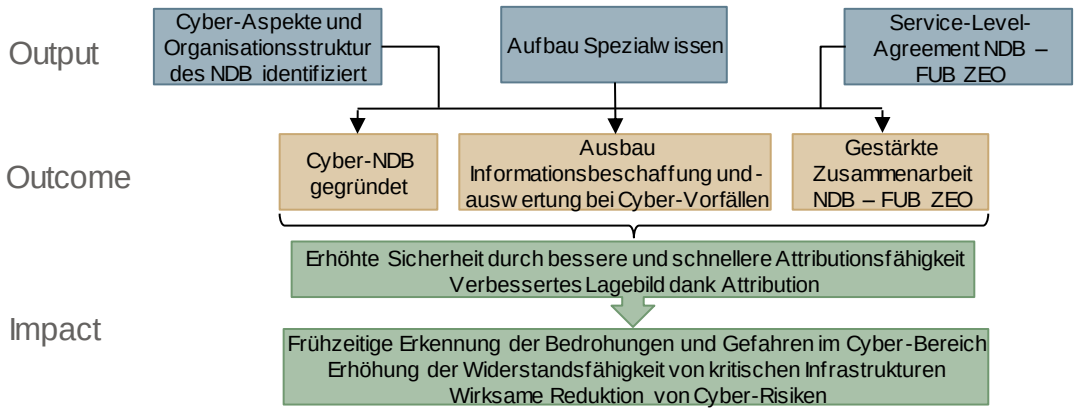

Abbildung 7 Wirkungsmodell M14

3.6.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen [Ressourcenpool für M4, M5, M14]	3 MELANI-ISB 3 MELANI-OIC (NDB) 7 NDB 1 MND 4 FUB
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	FUB, MND, MELANI

<u>Bemerkungen:</u>

Siehe Massnahme 4 (Kapitel 3.3) und 5 (Kapitel 3.4).

3.6.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome			✓	
Impact	◎ wurde erzielt			

3.6.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht</u>

Der NDB hat definiert, über welche Fähigkeiten er verfügen muss, um Täter zu identifizieren. Er hat das nötige Spezialwissen dazu auf- und ausgebaut. Die grösste Herausforderung bleibt die Analyse von Akteuren und ihres Umfelds aus den verschiedensten Regionen. In diesem Bereich muss noch mehr Spezialwissen erworben werden.

- **Identifikation Cyber-Aspekte:** Der NDB identifizierte folgende 8 Schlüssel-Fähigkeiten für die nachrichtendienstliche Arbeit im Cyber-Bereich: [74]:
  - Technische Auswertung der von den Angreifern eingesetzten Mittel
  - Informationsbeschaffung zur Erlangung weiterer Erkenntnisse zum Modus Operandi, den Zielen und dem Hintergrund der Täterschaft
  - Abgleich mit bereits vorhandenen Erkenntnissen zu Akteuren und Infrastrukturen im Cyber-Bereich
  - Abgleich mit bereits vorhandenen Erkenntnissen zu ähnlichen Vorfällen im In- und Ausland
  - Situativer Informationsaustausch mit Partnerdiensten und Koordination mit der Strafverfolgung
  - Auswertung und Aufarbeitung der vorhandenen Informationen und Erkenntnisse auf operativ-strategischer Ebene zu Händen politischer Entscheidungsträger und Anpassung der Bedrohungslageeinschätzung
  - Berücksichtigung völkerrechtlicher Implikationen
  - Verdichten der Erkenntnisse zu Analyse- und Gefährdungsberichten

  Wenn das neue Nachrichtendienstgesetz (NDG) in Kraft tritt, können weitere Fähigkeiten im Bereich der aktiven Gegenmassnahmen aufgebaut werden.

- **Aufbau Spezialwissen:** In Zusammenarbeit mit den Partnern von OIC MELANI, GovCERT und FUB-ZEO konnte der NDB Fachwissen in folgenden Bereichen auf- und ausbauen:
  - Netzwerkdatenanalyse (technische Analyse der Ziele und Methoden eines Cyberangriffs)
  - Schadsoftwareanalyse (Schwerpunkt Reverse-Engineering und Täterschaft-zuordnung)
  - Akteurs-Analyse (Bedrohungsanalyse und Täterschaft-Zuordnung)
  - Kontextanalyse (Umfeld und Rahmenbedingungen eines Cyberangriffs)

  Die Kapazitäten im Bereich der Akteurs-Analyse sind aktuell aber auf Grund von knappen Ressourcen noch beschränkt.

- **Leistungsvereinbarung zwischen NDB und FUB ZEO:** Der NDB greift zur Erfüllung seiner Aufgaben im Cyber-Bereich teilweise auf das technische Know-how der FUB-ZEO zurück. Grundlage dieser Zusammenarbeit ist die entsprechende Leistungsvereinbarung.

Outcome: Ziele sind grösstenteils erreicht:

Mit der Gründung des Cyber-NDB konnte eine Stärkung und Bündelung der Kompetenzen des NDB im Cyber-Bereich erreicht werden. Die Informationsbeschaffung funktioniert gut, die Auswertung der Informationen bleibt angesichts der knappen Ressourcen eine Herausforderung. Der Informationsaustauch mit der Bundesanwaltschaft funktioniert noch nicht optimal.

- **Cyber-NDB:** Zur Erfüllung der Aufgaben des NDB im Cyber-Bereich wurde die neue Organisationseinheit Cyber-NDB geschaffen. Er ist gut etabliert und in die Abläufe des NDB voll integriert. Das wird auch durch die bearbeiteten Fälle im 2015 erhärtet, bei denen staatliche Angriffe mit Relevanz für die Schweiz entdeckt und analysiert wurden. Der Cyber-NDB erstellte zudem mehrere Analysen für den Bundesrat und Amtsberichte für die Strafverfolgungsbehörden.
- **Informationsbeschaffung und -auswertung:** MELANI OIC ist die zentrale Drehscheibe für alle Informationen in Zusammenhang mit Cyber-Angriffen. Die Beschaffung relevanter Informationen via Cyber-NDB funktioniert gut. Informationen sind meist in ausreichender Qualität vorliegend. Dies ist auch dem guten Netzwerk aus nationalen und internationalen Informationsquellen des Cyber-NDB, sowie des GovCERT im technischen Bereich zu verdanken. Die Auswertung, Einschätzung und Kontextualisierung dieser Informationen ist jedoch ressourcenintensiv und bleibt eine grosse Herausforderung. Die Prozesse zur Weiterleitung der ausgewerteten Informationen an die richtigen Stellen sind definiert.
- **Zusammenarbeit NDB und Bundesanwaltschaft:** Der NDB liefert Berichte an die Bundesanwaltschaft und stellt sicher, dass die für die Strafverfolgung nötigen Daten korrekt erfasst und gespeichert werden. Der Rückfluss von Informationen aus der Bundesanwaltschaft funktioniert aktuell suboptimal. Zum Teil wird nicht zurückgemeldet, ob ein Fall von der Bundesanwaltschaft abgeschlossen wurde.

Impact: wurde erzielt

Der Impact wurde anhand von Beispielen illustriert, die in diesem Bericht aus Gründen der Vertraulichkeit nicht wiedergegeben werden. Die Beispiele dokumentieren jedoch, dass Täter identifiziert werden konnten. Die Informationen zu den Tätern konnten auch für die Lageeinschätzung berücksichtigt werden, womit ein substantieller Beitrag zur Früherkennung der Risiken geleistet wird.

3.7. M13 Krisenmanagement: Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise

Titel Massnahme	Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise
Ziele	Die betroffenen Akteure werden in einer Krise durch MELANI mit der Bereitstellung von Expertenwissen subsidiär unterstützt. Der freiwillige Informationsaustausch von KI-Betreibern, IKT Leistungserbringern und Systemlieferanten wird sichergestellt, um die Kontinuität und Widerstandsfähigkeit auf der Basis der Selbsthilfe zu stärken. Dazu wurden die heute vorhandenen Dienstleistungen weiter ausgebaut. Das EDA wird bei Fällen mit möglichen aussenpolitischen Implikationen informiert und ist bei der Erarbeitung von entsprechenden Vorsorgeplanungen eingebunden.
Verantwortliches Amt / Organisationseinheit	MELANI
Konsultierte Unterlagen für die WiÜ	Quellen: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Interviews	Siehe Anhang A.1, Interview I 12

3.7.1. Erwartete Wirkung: Wirkungsmodell M13

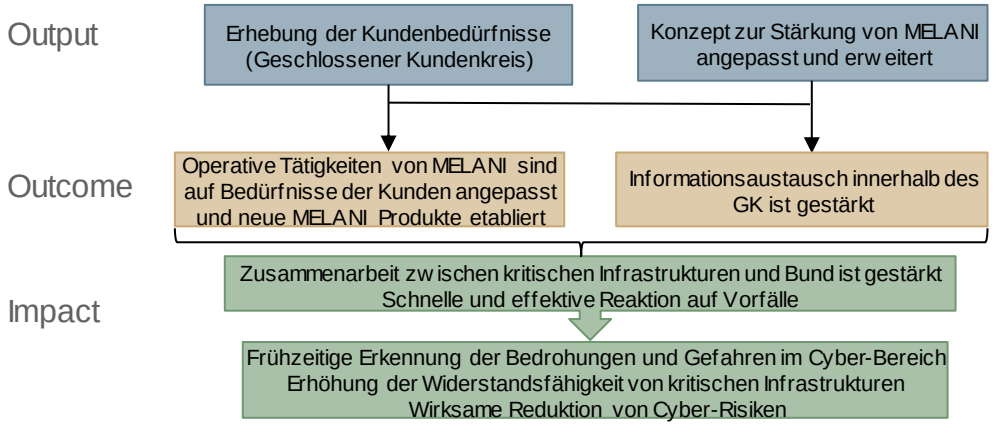

Abbildung 8 Wirkungsmodell M13

3.7.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine zusätzlichen Mittel
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	KS NCS

3.7.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome	☐ zurzeit nicht messbar			
Impact	☐ zurzeit nicht messbar			

3.7.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht:</u>

In einer Umfrage im geschlossenen Kundenkreis hat MELANI die Bedürfnisse der darin vertretenden Betreiber kritischer Infrastrukturen erhoben. Darauf aufbauend kann MELANI nun ihre Dienstleistungen so anpassen, dass sie die KI-Betreiber optimal unterstützen kann. Zum Zeitpunkt der WiÜ war die Auswertung der Umfrage abgeschlossen, aber noch keine Massnahmen zur Anpassung von MELANI formuliert.

- **Erhebung der Bedürfnisse des Geschlossenen Kundenkreises (GK):** Die Bedürfnisse der Betreiber kritischer Infrastrukturen, die bei MELANI den geschlossenen Kundenkreis bilden, wurden mittels Online-Befragung im November 2015 erhoben. Von 424 Mitgliedern haben 260 geantwortet. Die Umfrage zeigt auf, welche Stärken MELANI aktuell hat, wo Verbesserungspotential besteht und welche Wünsche die Mitglieder des GK haben. Die Resultate aus der Umfrage bieten eine gute Grundlage für die Weiterentwicklung von MELANI.

  Grundsätzlich sind die Mitglieder des GK mit den Dienstleistungen von MELANI zufrieden und schätzen MELANI als nützlich und wichtig ein. Künftige Herausforderungen liegen in der Stärkung der Sektoren mit wenigen Mitgliedern, der Ergänzung der GK durch KI-Betreiber und weiteren Erkenntnissen aus dem SKI-Inventar, der Förderung des Vertrauens zwischen den Mitgliedern des GK, der Verbesserung der Plattform für den Informationsaustausch und dem schnellen Verbreiten von verifizierten Informationen zu neuen Bedrohungen.

  Die Umfrage ist fertig ausgewertet. Zum Zeitpunkt der Wirksamkeitsüberprüfung wurden daraus aber noch keine konkreten Massnahmen abgeleitet.

- **Konzept zur Stärkung von MELANI:** Im Rahmen der Massnahme 4 wurde bereits im Februar 2014 ein Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch erarbeitet. Darin sind die Ergebnisse aus der Umfrage nicht berücksichtigt. Aufbauend auf den Resultaten der Umfrage wird das Konzept im Sommer 2016 angepasst und konsequent auf die Bedürfnisse des GK ausgerichtet. Nach Auskunft der Ersteller wird das Konzept folgende Themen berücksichtigen:
  - Sicherstellen der heute vorhandenen Dienstleistungen
  - Ausbau der bestehenden Sektoren
  - Ausbau der Dienstleistungen des GovCERT.ch
  - Einbezug von Nicht-KI-Betreibern bei MELANI

Outcome: Zurzeit nicht messbar

Die Umsetzung der Massnahme 13 hat erst kurz vor der Durchführung der WiÜ begonnen. Es kann daher noch nicht beurteilt werden, ob die Dienstleistungen von MELANI gemäss den Bedürfnissen des GK angepasst werden und ob damit der Informationsaustausch gestärkt wird.

Impact: Zurzeit nicht messbar

Zum Zeitpunkt der Wirksamkeitsüberprüfung kann der Impact der Massnahme 13 noch nicht beurteilt werden.

3.8. M15 Krisenmanagement: Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung

Titel Massnahme	**Konzept für Führungsabläufe und -prozesse mit Cyber-Ausprägung**
Ziele	Ein Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung, das der Cyber-Ausprägung Rechnung trägt, ist erstellt. Ebenso ist das allgemeine Krisenmanagement in Sachen Cyber-Risiken angepasst und beinhaltet den Cyber-Aspekt.
Verantwortliches Amt / Organisationseinheit	Bundeskanzlei
Konsultierte Unterlagen für die WiÜ	Quellen: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Interviews	Siehe Anhang A.1, Interview I 9

3.8.1. Erwartete Wirkung: Wirkungsmodell M15

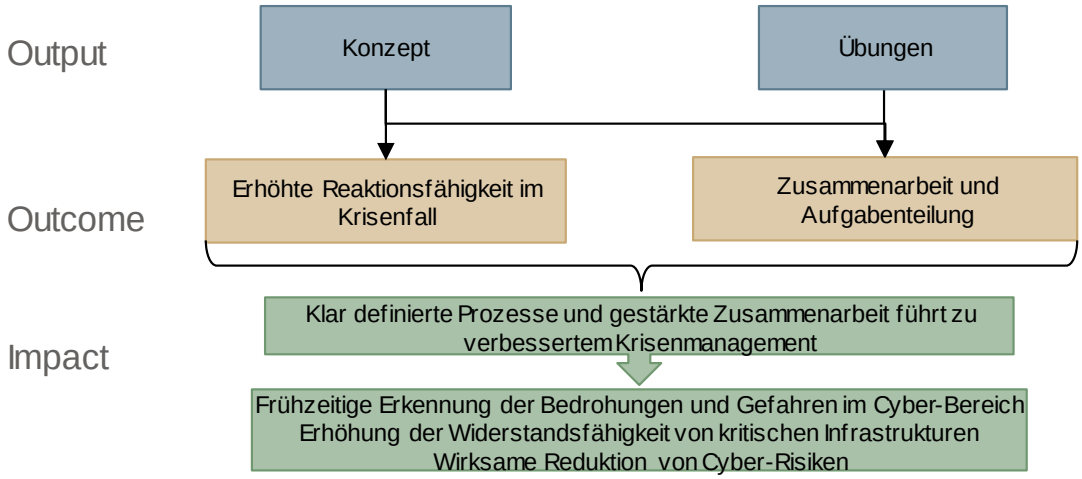

Abbildung 9 Wirkungsmodell M15

3.8.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine NCS spezifischen Ressourcen
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	KS NCS

3.8.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✔	
Outcome		✖		
Impact	☐ aktuell nicht beurteilbar			

3.8.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht:</u>

Ein Konzept für das Management von Krisen mit Cyber-Ausprägungen wurde von der Bundeskanzlei erstellt. Wichtig ist die Erkenntnis, dass Cyber-Aspekte keine neue Form des Krisenmanagements nötig machen. Das bestehende Krisenmanagement bleibt gültig. Im Cyber-Bereich muss für das Krisenmanagement das Lagebild erweitert werden und es braucht klarere Definitionen der Entscheidungsprozesse und der Kommunikationsverantwortung. Das Konzept wurde in der AG3 des SVS erweitert und anschliessend getestet. Es braucht jedoch weitere, möglichst breit angelegte Übungen.

Konzept: Das Konzept für das Krisenmanagement des Bundes bei Cyberkrisen wurde erstellt. Als wichtige Erkenntnis aus den Arbeiten zum Konzept wurde festgehalten, dass das Krisenmanagement prozess- und nicht szenarienorientiert funktionieren muss. Das bedeutet, die Führungs- und Entscheidungsprozesse verändern sich nicht, wenn eine Krise auch Cyber-Aspekte beinhaltet. Wichtig bei solchen Krisen ist, dass die Akteure mit Kompetenzen im Cyber-Bereich (v. a. MELANI) in das Krisenmanagement integriert sind.

Das Konzept beschreibt zwei entscheidende Prozesse für die Krisenbewältigung:

- **Einheitliches Lagebild:** Die Vermittlung eines aktuellen, einheitlichen und umfassenden Lagebildes ist in einer Krise entscheidend. Die Prozesse dafür im Cyber-Bereich werden im Rahmen des Lagebildes (Massnahme 4) erarbeitet.
- **Koordination:** Es gibt bislang keinen klar definierten Mechanismus zur Entscheidungsfindung auf strategischer Stufe. Beim Bund gibt es (operativ) viele Krisenstäbe. Die zuständigen Ansprechpartner bleiben oft unklar. Es gibt keine Übersicht über die definierten Prozesse. Dies führt in der Regel dazu, dass private Kommunikationskanäle genutzt werden (man kennt sich).

Übungen: Es ist teilweise schwierig, alle betroffenen Akteure einzubeziehen. Dies gelingt oft nur dank persönlicher Kontakte, was den Kreis der beteiligten Stakeholder einschränkt. Auch ist es eine Herausforderung, die Interessenvertreter für die Wahrnehmung des Risikos zu sensibilisieren. Die wichtigste Übung

zu Krisen mit Cyber-Ausprägungen war die SFU 13, bei welcher das Krisenmanagement auf Stufe Bund bei einem Szenario eines grossangelegten Cyberangriffes gegen die Schweiz getestet wurde. Im Fokus stand dabei die Zusammenarbeit zwischen den verschiedenen Departementen.

Outcome: Ziele sind nur teilweise erreicht:

Die Reaktionsfähigkeit kann nicht alleine in Hinblick auf die Cyber-Aspekte einer Krise beurteilt werden. Generell müssen die Konzepte zur Krisenbewältigung breiter abgestützt werden, im Hinblick auf das Management von komplexen Multikrisen. Bei der Zusammenarbeit hat sich gezeigt, dass an verschiedenen Stellen die Prozesse unklar sind. Erschwerend kommt hinzu, dass in den kantonalen Krisenstäben die Cyber-Aspekte oft noch wenig berücksichtigt werden.

- **Erhöhte Reaktionsfähigkeit im Krisenfall:** Im Rahmen der Arbeiten wurde erkannt, dass der Fokus zur Beurteilung der Reaktionsfähigkeit nicht alleine auf dem Cyber-Aspekt liegen darf. Krisen betreffen sehr rasch unterschiedlichste Bereiche (Multi-Krisen). Es braucht deshalb ein breiter abgestütztes Krisenbewältigungskonzept, bei dem der Fokus auch auf andere Bereiche als Cyber gelegt wird (z. B. Krisenmanagement beim Ausfall von KI mit Auswirkungen auf Wirtschaft und Gesellschaft).
- **Zusammenarbeit:** Es bestehen noch grosse Herausforderungen bei der Zusammenarbeit. Auf Stufe Bund muss die Abstimmung der verschiedenen existierenden Krisenstäbe untereinander geklärt werden. Die Führungsstrukturen beim Bund für das überdepartementale Krisenmanagement mit Rollen- und Aufgaben ist zwar grob als Grundlage definiert (siehe [117]), verschiedene Fragen bleiben aber offen.

  In den kantonalen Führungsstäben ist Cyber meist noch kein Thema. Die Integration der Cyber-Fachkräfte in die kantonalen Führungsorgane ist entsprechend noch nicht überall umgesetzt. Auch die gegenseitige Unterstützung der Kantone ist nicht geregelt. Es besteht Bedarf nach einem geeigneten Gefäss für den Informationsaustausch z. B. via AG Sicherheit der SIK oder durch die Konferenz der kantonalen Stabschefs.

Impact: Nicht beurteilbar

Im Zuge der Arbeiten am Konzept und im Rahmen der Übungen konnte die Zusammenarbeit gestärkt werden. Die Prozesse sind nun klarer ausgearbeitet. Ob sich dies in einem verbesserten Krisenmanagement manifestiert, muss noch überprüft werden. Der Impact kann zum aktuellen Zeitpunkt deshalb nicht beurteilt werden.

3.9. M9 Internationale Zusammenarbeit: Internet Governance

Titel Massnahme	Internet Governance
Ziele	Die Interessen von Behörden, Wirtschaft und Gesellschaft der Schweiz betreffend dem Thema Internet Governance sind koordiniert. Dazu wurden entsprechende Prozesse definiert. Die vom UVEK betriebene Multi-Stakeholder-Austausch-Plattform wird von den relevanten Akteuren zur Diskussion von Internet Governance-Themen benutzt. Die Interessen der Schweiz im Bereich Internet Governance werden in entsprechenden internationalen Gremien und Veranstaltungen vertreten, die Kooperati-

	on mit Partnern auf internationaler Ebene ist sichergestellt.
Verantwortliches Amt / Organisationseinheit	BAKOM
Konsultierte Unterlagen für die WiÜ	Quellen: [90], [91], [92]
Interviews	Siehe Anhang A.1, Interview I 6

3.9.1. *Erwartete Wirkung: Wirkungsmodell M9*

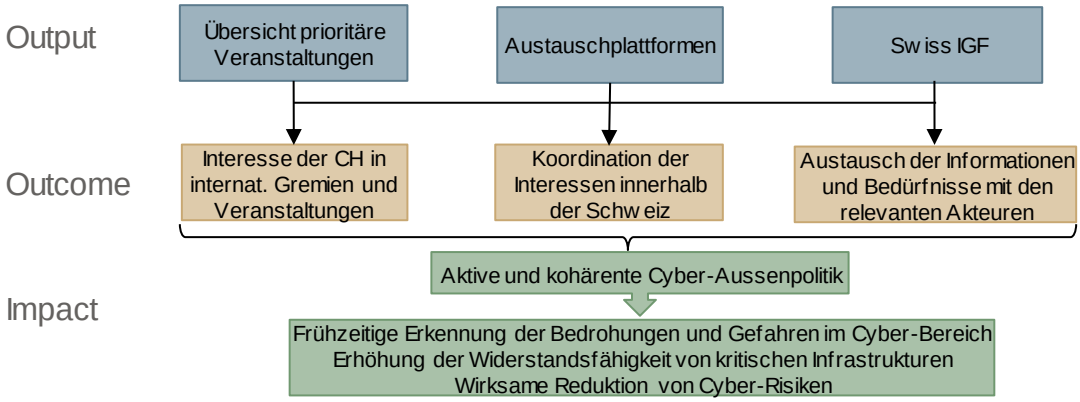

Abbildung 10 Wirkungsmodell M9

3.9.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Eine zusätzliche Stelle (Budget BAKOM)
Finanzielle Mittel	Keine zusätzlichen Mittel (ordentliches BAKOM Budget)
Mitarbeit durch andere Ämter / Organisations-einheiten	EDA, MELANI

3.9.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome			✓	
Impact	☐ aktuell nicht beurteilbar			

3.9.4. *Begründung der Beurteilung*

<u>Output: Ziele sind erreicht:</u>

Es konnte eine Übersicht zu den wichtigsten Akteuren und Veranstaltungen im Bereich Internet Governance erstellt werden. Über bestehende und neu geschaffene Formate wird der Austausch mit allen Stakeholdern aus der Verwaltung, Wirtschaft und Gesellschaft gepflegt.

- **Internet Governance (IG) und Veranstaltungen:** Es sind alle relevanten Institutionen aufgeführt, die sich mit IG beschäftigen. Mit Priorität 1 sind jene Organisationen und internationale Gremien gekennzeichnet, die eine zentrale Rolle in der IG einnehmen und sich in erster Linie um Belange in Bezug auf das Internet kümmern, sei dies technischer oder politischer Natur. Alle anderen Institutionen fallen unter Priorität 2 oder 3. Diese Übersicht soll nach ihrer Erstellung regelmässig aktualisiert werden.
- **Austauschplattformen:** In der Liste der Gremien ist definiert, wie der Informationsaustausch funktioniert (siehe [91]).
  - Bundesinterner Austausch: Als bundesinterner Informationskanal wird die Plattform ch@world genutzt. Sie erlaubt es, verschiedene Bundesstellen bei relevanten Konsultationen zu informieren, damit Inputs fristgerecht eingereicht werden können. Neben dieser Plattform wir der Austausch über herkömmliche Kanäle gepflegt (E-Mail, Telefon) und sporadisch an themenspezifischen „brown-bag Lunches“ vertieft.
  - Austausch mit Wirtschaft und Zivilgesellschaft: Die seit 2003 bestehende Plateforme Tripartite wird vom BAKOM genutzt, um Informationen zum Themenkreis Internet Governance zu diskutieren und Informationen zu verbreiten. Die Plateforme besteht aus zweimal jährlich stattfindenden Sitzungen und einer Mailingliste. Aktuell umfasst der Adressatenkreis 100 Personen (davon ca. die Hälfte aus der Bundesverwaltung).
  - Swiss Internet Governance Forum (Swiss IGF): Als neue Austauschplattform wurde das Swiss IGF aufgebaut. Das Forum bietet allen Interessierten die Möglichkeit, Informationen über eigene Aktivitäten im Bereich Internet Governance zu verbreiten (bottom-up Ansatz) und ist in dem Sinn komplementär zur Plateforme Tripartite, bei der hauptsächlich das BAKOM informiert. Das Format hat sich bewährt, 2016 besuchten rund 100 Personen die jährliche Veranstaltung des Swiss IGF.

<u>Outcome: Ziele sind grösstenteils erreicht:</u>

Die Interessen der Schweiz im Bereich Internet Governance sind koordiniert. Der Austausch funktioniert insbesondere zwischen EDA-ASP und BAKOM gut. DEZA und SECO sind aktuell zu wenig in diese Koordination integriert. Die Interessen von Wirtschaft und Gesellschaft werden abgeholt, wobei die Beteiligung aus der Privatwirtschaft bisher zurückhaltend ausfällt.

- **Koordination der Interessen der Schweiz in internationalen Gremien und Konferenzen:** Innerhalb der Bundesverwaltung werden Informationen zur Internet Governance rege ausgetauscht. Dies gilt besonders für das BAKOM und das EDA, welche die bestehenden guten Verbindungen seit Beginn der Umsetzung zu M9 intensiviert haben. Daraus resultiert ein guter Austausch im Vorfeld von internationalen Konferenzen, so dass die Schweizer Delegationen mit konsolidierten Positionen auftreten. Die Koordination erfolgt im Rahmen der Fachgruppe Cyber-International (vgl. Kapitel 3.10), welche durch ASP geleitet wird. Beispiele für Erfolge der aufeinander abgestimmten Interessensvertretung sind der Vorsitz des Schweizer Vertreters im Regierungsbeirat der ICANN, die koordinierte Teilnahme am WSIS-Prozess der UNO und die gemeinsame Lancierung der Geneva Internet Platform durch EDA und BAKOM.

  Neben dem Austausch zwischen BAKOM und EDA-ASP ist auch MELANI in die Koordination integriert. Hingegen fehlt ein regelmässiger Austausch mit der DEZA und dem SECO zu Fragen der Internet Governance.

- **Koordination der Interessen innerhalb der Schweiz und Austausch von Informationen:** Durch die Nutzung der Plateforme Tripartite und das neu geschaffenen Swiss Internet Governance Forum können die verschiedenen Interessen frühzeitig abgeholt und berücksichtigt werden. Daneben informiert das BAKOM aktiv mit Hilfe von Newslettern und Artikel in Fachzeitschriften. Es bleibt jedoch eine schwierige Aufgabe, ein möglichst breites Publikum in die Aktivitäten im Bereich Internet Governance zu integrieren. Weil die Prozesse in internationalen Gremien oft lange dauern und auf einem eher abstrakten Niveau stattfinden, engagiert sich die Privatwirtschaft zurückhaltend. Ihre Interessen sind deshalb meist nur indirekt berücksichtigt.

Impact: nicht beurteilbar

Die verstärkte Koordination hat zu einer kohärenten Cyber-Aussenpolitik geführt. Die Grundprinzipien der Schweiz in Bezug auf Internet Governance (multistakeholder Approach) sind bekannt und werden einheitlich vertreten. Zum aktuellen Zeitpunkt kann aber nicht gemessen werden, ob dadurch die Position der Schweiz gestärkt wurde. Der Impact kann darum noch nicht beurteilt werden.

3.10. M10 Internationale Zusammenarbeit: Kooperation auf der Ebene der internationalen Sicherheitspolitik

Titel Massnahme	Kooperation auf der Ebene der internationalen Sicherheitspolitik
Ziele	Die Interessen von Wirtschaft, Gesellschaft und Behörden sind auf der Ebene der internationalen Sicherheitspolitik bezüglich Cyber-Risiken koordiniert. Die internationale Kooperation, um der Bedrohung im Cyber-Raum in Zusammenarbeit mit anderen Staaten und internationale Organisationen zu begegnen, ist sichergestellt.
Verantwortliches Amt / Organisationseinheit	EDA
Konsultierte Unterlagen für die WiÜ	Quellen: [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116]
Interviews	Siehe Anhang A.1, Interview I 4

3.10.1. Erwartete Wirkung: Wirkungsmodell M10

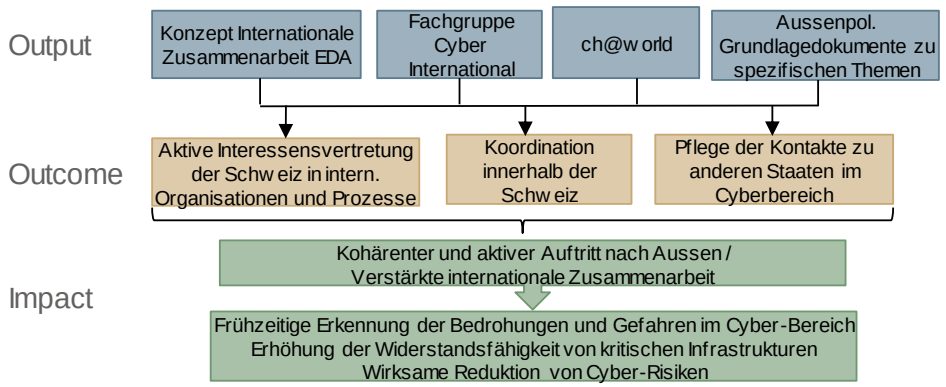

Abbildung 11 Wirkungsmodell M10

3.10.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen

Personalressourcen	2 Mitarbeitende
Finanzielle Mittel	CHF 150‘000 pro Jahr
Mitarbeit durch andere Ämter / Organisationseinheiten	MELANI, KS NCS, EJPD, VBS, BAKOM, ENSI

3.10.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome				✓✓
Impact	☐ aktuell nicht beurteilbar			

3.10.4. *Begründung der Beurteilung*

<u>Output: Ziele sind erreicht:</u>

Die Basis für eine koordinierte und kohärente Cyber-Aussen- und Sicherheitspolitik konnte geschaffen werden. In einem Konzeptpapier zur internationalen Zusammenarbeit ist die Rolle der Abteilung Sicherheitspolitik (ASP) des EDA klar definiert. Mit der Fachgruppe Cyber-International konnte ein Austauschgremium etabliert und über die Plattform ch@world die Kommunikation gestärkt werden. Es wurden auch Grundlagedokumente zu Cyber-Aussenpolitik erstellt.

- **Konzept internationale Zusammenarbeit:** Das Konzept ist erstellt. Es handelt sich um ein Dokument, das die Rolle, die Aktivitäten und Initiativen darlegt, in die das EDA entweder federführend oder unterstützend involviert ist. Die Abteilung Sicherheitspolitik (ASP) stellt zudem einmal pro Jahr eine Übersicht der wichtigsten Aktivitäten, Prozesse und Initiativen im Cyber-Bereich als „Update“ zuhanden des Departementschefs EDA, des Staatssekretärs EDA und dem NCS-Steuerungsausschuss zusammen.
- **Fachgruppe Cyber-International (FG-CI):** Die FG-CI setzt sich aus Vertretern des EDA (PD und DV), VBS (SIPOL, BABS, Bereich V und NDB), UVEK (BAKOM und BFE), EFD (ISB) und EJPD (BJ und fedpol) und seit kurzem auch ENSI zusammen. Alle Vertreter bringen sich aktiv ein. Dieses Gremium steht weiteren Bundesstellen offen, die sich mit den Themenfeldern „Cyber-Sicherheit“ und „Internet Governance“ auf internationaler Ebene befassen. Den Vorsitz über die FG-CI hat die ASP. Die Sitzungen der FG-CI finden zweimal jährlich statt. Bei Bedarf kann ein Mitglied die Einberufung einer ausserordentlichen Sitzung verlangen.
- **ch@world:** Um den Informationsaustausch zu erleichtern, wurde auf ch@world eine Plattform für den Informationsaustausch unter den Mitgliedern der FG-CI aufgebaut. Die Mitglieder können selbst Unterlagen hochladen. Diese Plattform wird regelmässig genutzt, beispielsweise insbesondere auch für die Teilnahme an Konsultationen(z. B. für Geneva Declaration for Cyberspace).
- **Aussenpolitische Grundlagedokumente:** Die aussenpolitischen Grundlagendokumente decken die wichtigsten Handlungsbereiche ab. Diese werden in Abhängigkeit der aussenpolitischen Relevanz und nach Bedarf (weiter-) entwickelt. Ein aktuelles Thema ist der Umgang mit gewaltextremistischem Inhalt im Internet und sozialen Medien (Preventing Violent Extremism).

Outcome: Ziele sind erreicht:

Die Schweiz vertritt ihre Interessen aktiv und kohärent in internationalen Gremien im Bereich der Cyber-Sicherheit und pflegt gute bilaterale Kontakte. Sie wird als aktiver und verlässlicher Akteur wahrgenommen.
Der Austausch zwischen allen beteiligten Bundesstellen hat sich gut etabliert. Dies ist direkt auf die Schaffung der Fachgruppe Cyber-International und die Nutzung der Plattform ch@world zurückzuführen.

- **Aktive Interessensvertretung der Schweiz in internationalen Gremien und Pflege der Kontakte zu anderen Staaten im Cyber-Bereich:** Die ASP hat die Schweiz an zahlreichen internationalen Verhandlungen und Prozesse mit Bezug auf Cyber-Sicherheitspolitik vertreten. Im Zuge dieser Aktivitäten werden auch bilaterale Beziehungen zu verschiedenen Ländern gepflegt. Die Schweiz wird als aktiver und verlässlicher Akteur im Cyber-Bereich wahrgenommen. Dies zeigt sich anhand verschiedener Anfragen von Staaten, sie bei der Erarbeitung von Cyber-Strategien zu unterstützen (z. B. Teilnahme der Schweiz an Public Hearing in Armenien und Serbien, Unterstützung beim Aufbau von CERTs, etc.). Nachfolgend werden die wichtigsten Aktivitäten und die daraus erzielten Resultate kurz aufgelistet:
  - OSZE-Prozess: Vertrauensbildung im Cyber-Raum. Förderung von vertrauensbildenden Massnahmen (VBM) im Rahmen des Schweizer OSZE Vorsitzes 2014. Zwei Massnahmenpakete wurden verabschiedet.
    - Aktive Teilnahme der Schweiz an der Global Conference on Cyberspace und Durchführung eines Workshops: “Mechanisms for Confidence-Building and Cooperation in Cyberspace” in Genf als Schweizer Beitrag zur Global Conference on Cyberspace.
    - Teilnahme des Geneva Center for Security Policy (GCSP) am Sino-European Cyber-Dialog (2014-2016) an welchem eine Arbeitsgruppe zur Frage der Anwendbarkeit des Internationalen Völkerrechts auf den Cyber-Bereich geschaffen wurde.
  - ICT4Peace: Projekte zum Aufbau der Kapazitäten im Cyber-Bereich in Entwicklungsländer.
  - Mitarbeit bei der Verfassung des „Tallinn Manual“ der NATO (Studie zur Anwendbarkeit des Völkerrechts im Cyberspace).
- **Koordination der Interessen innerhalb der Schweiz für einen kohärenteren internationalen Auftritt:** Ein wichtiger Mehrwert der Fachgruppe Cyber-International ist der regelmässige Austausch zwischen den Diensten. Dem gleichen Zweck dient die Plattform ch@world, die sich auch zu einer Datenbank mit den wichtigsten Unterlagen entwickelt hat. Dank diesen Instrumenten konnte die Kohärenz der Cyber-Aussenpolitik gestärkt werden. Allenfalls müsste der Sitzungsrhythmus je nach Bedarf erhöht werden. Es gilt auch zu berücksichtigen, dass je nach Thema Projektpartner beigezogen werden müssen, die nicht Mitglied der Fachgruppe Cyber-International sind.

Impact: kann aktuell nicht beurteilt werden

Die Schweiz pflegt eine aktive und kohärente Aussenpolitik mit Bezug auf Cyber-Risiken. Sie investiert damit in die Stärkung der Beziehungen zu anderen Staaten und versucht einen Beitrag zur internationalen Cyber-Sicherheit zu leisten. Weil solche Bemühungen langfristig angelegt sind, kann aktuell noch kein Impact gemessen werden.

3.11. M11 Internationale Zusammenarbeit: Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit

Titel Massnahme	**Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit**
Ziele	Die Interessen des Wirtschaftsstandortes Schweiz werden in die internationalen privaten und staatlichen Gremien im Bereich Sicherheit, Sicherung und Standardisierung koordiniert eingebracht. Dazu wurde der Informationsaustausch zwischen KI-Betreibern, IKT-Leistungserbringern, Systemlieferanten, Verbänden, nationalen Standardisierungsorganisationen, Fachbehörden und Regulatoren gestärkt. Ein diesbezüglicher Prozess ist etabliert.
Verantwortliches Amt / Organisationseinheit	BAKOM
Konsultierte Unterlagen für die WiÜ	Quellen: [93], [94], [95], [96], [97]
Interviews	Siehe Anhang A.1, Interview I 6

3.11.1. Erwartete Wirkung: Wirkungsmodell M11

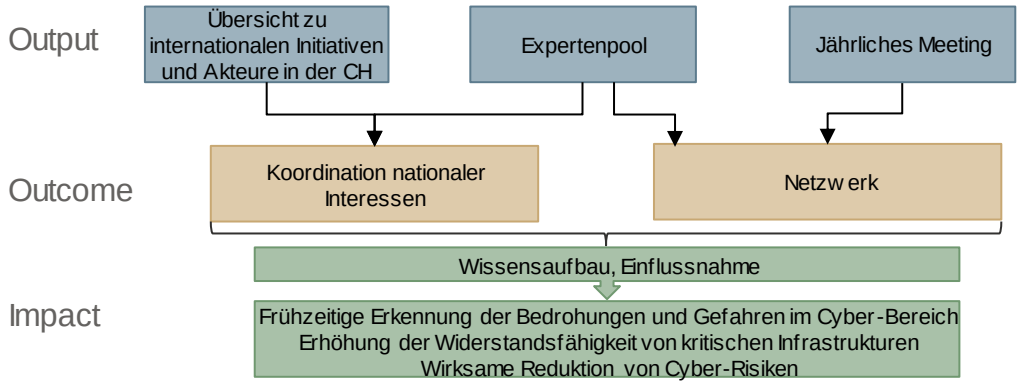

Abbildung 12 Wirkungsmodell M11

3.11.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine, Aufgabe wurde vom BAKOM ohne zusätzliche Personalressourcen übernommen
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisationseinheiten	KS NCS

3.11.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✔	
Outcome		✖		
Impact	☐ aktuell nicht beurteilbar			

3.11.4. *Begründung der Beurteilung*

<u>Output: Ziele sind grösstenteils erreicht:</u>

Die Meilensteine der Strategieplanung wurden erarbeitet und es wurde ein Netzwerk aus Akteuren aufgebaut, die sich zu Fragen der internationalen Initiativen und Standardisierungsprozesse austauschen wollen. Das Interesse von Seiten der Privatwirtschaft an einer direkten Beteiligung ist nicht sehr gross. Ein erster (potentiell jährlicher) Workshop zum Thema über aktuelle internationale Entwicklungen fand statt.
Weder konnte im Kreis der Akteure der M11 ein konkreter Koordinierungsbedarf identifiziert werden, noch wurde von anderer Seite ein solcher an die M11 herangetragen. Das im Netzwerk vorhandene Expertenwissen ist anhand der Listen und Referate dokumentiert, ob es für die NCS in einem erweiterten Kontext genutzt werden kann, ist aber noch offen.

- **Übersicht zu internationalen Initiativen unter Beteiligung von Schweizer Akteuren:** Die Übersicht existiert ([96]) und soll jährlich aktualisiert werden. Sie besteht aus einer Liste von Akteuren, die das Geschehen in internationalen Organisationen und Initiativen in Fragen der Cyber-Security verfolgen und beeinflussen. Die Liste der Akteure ist in zwei Kategorien mit unterschiedlichen Intentionen aufgeteilt:
  - Akteure der Behörden, Fachämter und Regulatoren
  - Akteure von privatwirtschaftlichen Organisationen und Bildungseinrichtungen

  Die Liste basiert auf freiwilliger Meldung. Von allen im Rahmen der M11 angeschriebenen Organisationen hat nur ca. ein Drittel geantwortet. Es fehlen Grossfirmen mit Schweizer Niederlassungen, die in internationalen Gremien vertreten sind, sich aber nicht als Schweizer Akteure verstehen (z. B. Google, Microsoft, Cisco).
- **Expertenpool zu Fragen der Standardisierung im Sicherheitsbereich:** Unter den Beteiligten hat es Experten zu verschiedenen Fragen mit Bezug auf internationale Prozesse im Bereich Cyber-Risiken. In Absprache mit den Teilnehmern muss der Fokus der Gruppe noch weiter geschärft werden. In einem ersten Workshop lag der Schwerpunkt auf Fragen zum Aufbau von CERTs. Zusätzlicher Koordinationsbedarf mit Bezug auf die NCS besteht kaum, da sich die Vertreter in internationalen Standardisierungsorganisationen bereits umfassend austauschen.

<u>Outcome: Ziele sind nur teilweise erreicht:</u>

In einem ersten Workshop wurde das Netzwerk gestärkt und eine Gruppe von 30-40 Teilnehmern mit Interesse an Standardisierung und Best-Practices konnte erreicht werden. Zum Thema internationale Standardisierung besteht aber wenig Koordinationsbedarf, die Interessenslage ist eher auf nationale Entwicklungen ausgerichtet.

- **Koordination nationaler Interessen:** Zu diesem Thema wurden bisher keine Ergebnisse erarbeitet. Aktuell ist kein Bedarf erkennbar. Der Fokus liegt bislang auf dem Aufbau und der Stärkung des Netzwerks. Mehrheitlich sind Teilnehmer an nationalen Entwicklungen interessiert, nicht an der internationalen Koordination.
- **Netzwerk:** Ein erster Workshop mit etwas über 40 Teilnehmern fand statt. Im Fokus stand das Thema „Monitoring und Response“. Der Workshop war hilfreich, um das Netzwerk zu stärken. Es bleibt aber unklar, ob das Thema der Standardisierung für die Teilnehmer genügend relevant ist, um sich weiterhin innerhalb der M11 zu engagieren.

Impact: kann aktuell nicht beurteilt werden

Aktuell ist es zu früh, um den Impact umfassend zu beurteilen. Im aufgebauten Netzwerk besteht zwar viel Expertenwissen und Einfluss, es besteht bislang in internationaler Stossrichtung kein Bedarf für eine koordinierte Einflussnahme von Vertretern aus der Schweiz.

3.12. M1 Bildung und Forschung: Identifikation von Cyber-Risiken durch die Forschung

Titel Massnahme	**Identifikation von Cyber-Risiken durch die Forschung**
Ziele	Die verantwortlichen Bundesstellen tauschen sich untereinander und mit Akteuren ausserhalb der Bundesverwaltung zu aktuellen und zu erforschenden Entwicklungen im In- und Ausland im Zusammenhang mit Cyber-Risiken aus und treiben bei Bedarf intramuros Forschung oder erteilen Forschungsaufträge.
Verantwortliches Amt / Organisationseinheit	SBFI, KS NCS
Konsultierte Unterlagen für die WiÜ	Quellen: [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]
Interviews	Siehe Anhang A.1, Interview I 1

3.12.1. Erwartete Wirkung: Wirkungsmodell M1

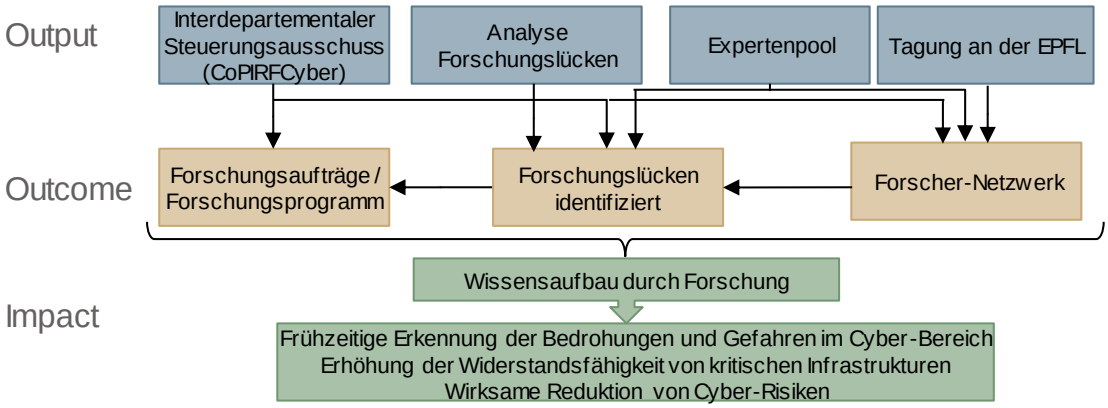

Abbildung 13 Wirkungsmodell M1

3.12.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine zusätzlichen Stellen.
Finanzielle Mittel	Keine zusätzlichen Mittel; Fachexperten aus den Hochschulen sind ehrenamtlich engagiert.
Mitarbeit durch andere Ämter / Organisations-einheiten	EDA ASP, BAKOM, FUB-ZEO, MND, KTI, BWL, MELANI, SVS

Das SBFI hat die Verantwortung für die Umsetzung der Massnahme ab 2014 übernommen und trägt den Personalaufwand selbst.

3.12.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome			✓	
Impact	☐ aktuell nicht beurteilbar			

3.12.4. *Begründung der Beurteilung*

<u>Output: Ziele sind erreicht:</u>

Durch die Schaffung eines interdepartementalen Steuerungsausschusses für Forschung und Bildung im Bereich Cyber-Risiken unter der Leitung des SBFI ist die Koordination in diesem Bereich sichergestellt. Die ersten Schritte zur Stärkung der Forschung sind gemacht: Eine Expertengruppe mit Vertretern aus Schweizer Hochschulen wurde eingesetzt, um den prioritären Forschungsbedarf in der Schweiz zu Identifizieren. Mit der ersten Swiss Cyber Risk Research Conference wurde das Netzwerk unter Forschenden gestärkt und ein Signal gegen aussen gegeben, dass der Bund Forschung im Bereich Cyber-Risiken fördern will.

- **Aufbau eines interdepartementalen Steuerungsausschuss:** Das « Comité de Pilotage Interdépartemental Recherche et Formation dans le domaine de la protection contre les Cyberrisques » (CoPIRFCyber) wurde unter der Leitung des SBFI geschaffen. Im Ausschuss sind Bundesämter vertreten, die ein Interesse an Fragen der Bildung und Forschung zu Cyber-Risiken haben. Der Ausschuss tagt viermal jährlich (oder nach Bedarf). Er koordiniert in diesem Bereich massgeblichen Aktivitäten der Bundesverwaltung.
- **Expertenpool und Analyse Forschungslücken:** Zur fachlichen Unterstützung insbesondere für die Identifikation des Forschungsbedarfs, hat der CoPIRFCyber eine Expertengruppe eingesetzt. Vierzehn Fachexperten aus Schweizer Hochschulen haben sich bereit erklärt, in der Expertengruppe mitzuarbeiten. Die Gruppe hat bereits die wichtigsten Forschungsthemen identifiziert und wird bis Ende 2016 einen Bericht verfassen, in dem die wichtigsten aktuellen Herausforderungen in der nationalen und internationalen Forschung dargestellt sind.
- **Tagung Cyber-Risiken:** Am 25. Mai 2016 fand an der EPFL die erste Swiss Cyber Risk Research Conference statt. Die Tagung wurde unter der Leitung des SBFI vom CoPIRFCyber organisiert. 350 Personen aus der Schweizerischen Forschungsland-

schaft nahmen an der Tagung teil. Als Redner konnten international anerkannte Experten gewonnen werden. Die Tagung soll künftig alle zwei Jahre stattfinden und helfen, das Netzwerk der Forschenden im Bereich Cyber-Risiken zu stärken.

Outcome: Ziele sind grösstenteils erreicht:

Mit der Swiss Cyber Risk Research Conference ist es gelungen, Forschende der verschiedensten Bereiche zum Thema Cyber-Risiken anzusprechen. Durch den aufgebauten Expertenpool konnte ein enges Netzwerk von Fachexperten geknüpft werden. Die wichtigsten Forschungsthemen und Herausforderungen wurden durch den Expertenpool identifiziert und werden bis Ende 2016 noch im Detail beschrieben. Die Arbeiten sollen dem Bund helfen, Prioritäten bei der Förderung der Forschung zu setzen.

- **Forscher Netzwerk:** An der Swiss Cyber Risk Research Conference kamen zum ersten Mal Forscher aus verschiedensten Disziplinen und verschiedenen Hochschulen zum Thema Cyber-Risiken zusammen. Der Anlass dient als Startschuss für den Aufbau des Forscher-Netzwerks. Es wird aber wichtig bleiben, auch darüber hinaus den Austausch zwischen den Forschenden zu fördern. In welcher Form dies geschehen soll, ist noch offen. Der aufgebaute Expertenpool als enges Netzwerk von Fachexperten dient als gute Ausgangsbasis.
- **Forschungslücken identifizieren:** Die eingesetzte Expertengruppe hat die wichtigsten Themen und Herausforderungen für die Schweizer Forschung identifiziert und wird bis Ende 2016 einen Bericht dazu veröffentlichen. Es ist noch zu definieren, ob und wie die Arbeiten regelmässig aktualisiert werden.
- **Forschungsaufträge / Forschungsprogramm:** Da die wichtigsten Forschungsthemen noch beschrieben werden müssen, sind noch keine konkreten Forschungsaufträge formuliert worden. Im Rahmen des Nationalfondsprogrammes „Big Data“ wird aber bereits Forschung im Bereich Cyber-Risiken gefördert.

Impact: kann noch nicht beurteilt werden

Die geschaffenen Strukturen scheinen geeignet, um den aktuellen Stand der Forschung sowie einen allfälligen zusätzlichen Forschungsbedarf im Bereich Cyber-Risiken zu identifizieren. Zum aktuellen Zeitpunkt ist es aber zu früh, um feststellen zu können, ob die Massnahme eine Wirkung erzielen konnte.

3.13. M7/M8 Bildung und Forschung: Übersicht Kompetenzbildungsangebote sowie vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken

Titel Massnahme	**Übersicht Kompetenzbildungsangebote sowie vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken**
Ziele	M7: Wirtschaft, Verwaltung und Zivilgesellschaft können sich bedürfnisgerecht über qualitativ hochstehende Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken informieren. Angebotslücken sind die identifiziert und dienen als Grundlage zur Umsetzung der Massnahme 8. M8: Der Bund hat in Abstimmung mit den Kantonen und der Wirtschaft in einem Umsetzungskonzept festgehalten, wie er eine vermehrte Nutzung der Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken erreichen will. Weiter zeigt das Konzept auf, wie Angebotslücken geschlossen und welche neuen Kompetenzbildungsangebote geschaffen werden sollen.

Verantwortliches Amt / Organisationseinheit	SBFI, KS NCS
Konsultierte Unterlagen für die WiÜ	Quellen: [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]
Interviews	Siehe Anhang A.1, Interview I 1

3.13.1. *Erwartete Wirkung: Wirkungsmodell M7 / M8*

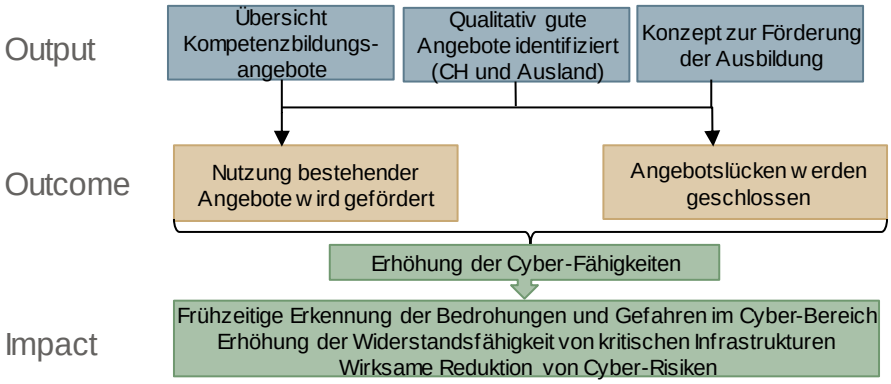

Abbildung 14 Wirkungsmodell M7 / M8

3.13.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine zusätzlichen Stellen
Finanzielle Mittel	Keine zusätzlichen Mittel
Mitarbeit durch andere Ämter / Organisations-einheiten	BAKOM, EDA, BSV

3.13.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output			✓	
Outcome				✓✓
Impact	☐ aktuell nicht beurteilbar			

3.13.4. *Begründung der Beurteilung*

Output: Ziele sind grösstenteils erreicht:

> Eine Übersicht zu bestehenden Kompetenzbildungsangeboten wurde erstellt und qualitativ hochstehende Angebote mit Hilfe von Experteninterviews identifiziert. Diese Arbeiten dienten vor allem dazu, einen Eindruck zu gewinnen, wie der Bund Kompetenzbildung im Bereich Cyber-Risiken fördern kann. Es wurde darauf verzichtet, qualitativ hochstehende Angebote speziell auszuweisen, weil eine Beurteilung des Bundes nur im Rahmen eines umfassenden Zertifizierungsprozesses zulässig wäre.
> In einem Umsetzungskonzept wird festgehalten, wie der Bund Kompetenzförderung im Bereich Cyber-Risiken betreiben will. Konkretisiert ist dabei namentlich das Vorgehen in den Bereichen Weiterbildung, Berufsbildung und auf Stufe der Hochschulen.

- **Angebotsübersicht:** Mittels Expertenbefragung wurden die bestehenden Angebote der Kompetenzbildung in der Schweiz und in benachbarten Ländern identifiziert. Es wird unterschieden zwischen Angeboten für die Bevölkerung, für die Verwaltung und für die Wirtschaft. Die Bedürfnisse der Zielgruppen, die identifizierten Angebote und die Angebotslücken wurden in einem Bericht beschrieben. Es ist aber klar, dass eine solche Übersicht in Anbetracht des dynamischen Bildungsmarkts nicht abschliessend sein kann. Eine regelmässige Aktualisierung ist nicht weiter vorgesehen, da verschiedene Verbände und Vereine ebenfalls Übersichten zu Kompetenzbildungsangeboten auf ihren Websites publizieren.
- **Identifikation qualitativ hochstehender Angebote:** Basierend auf der oben erwähnten Expertenbefragung wurde versucht, Beispiele für geeignete Kompetenzbildungsangebote zu identifizieren. Schliesslich wurde aber darauf verzichtet, die verschiedenen Angebote systematisch qualitativ zu beurteilen und die besten Angebote dann zu publizieren. Der Bund sollte aus ordnungspolitischen Gründen nicht in den bestehenden Bildungsmarkt eingreifen. Eine umfassende Beurteilung wäre nur im Rahmen von Zertifizierungsverfahren zulässig, was aber über die in Massnahme 7 und 8 vorgegebenen Ziele hinausgehen würde.
- **Konzept zur Förderung der Ausbildung:** Das Konzept zur Förderung der Ausbildung im Bereich Cyber-Risiken ist erstellt. Es ist ein Produkt des CoPIRFCyber (vgl. Kapitel 3.12) und legt dar, welche Massnahmen der Bund zur Förderung der Bildung im Bereich Cyber-Risiken ergreifen wird. In erster Priorität will der Bund die Kompetenzbildung auf den Stufen Weiterbildung, Berufsbildung und Hochschulen fördern. Dazu werden im Konzept bereits konkrete Schritte beschrieben. Die Grundbildung liegt massgeblich in der Kompetenz der Kantone, weshalb diese bisher nicht angegangen wurde.

Outcome: Ziele sind erreicht:

> Mit der Lancierung des Abschlusses als eidg. dipl. ICT Security Expert, einem Projekt in Zusammenarbeit mit dem Verband ICT-Berufsbildung, konnte ein wichtiger Schritt zur Förderung der Kompetenzbildung auf den Stufen Weiterbildung und Berufsbildung vollzogen werden. Im Bereich Hochschulen wird die Bildung vor allem indirekt über die Forschungsförderung gestärkt (vgl. M1, Kap. 3.12).

- **Förderung bestehender Angebote und Schliessung von Angebotslücken:** Zur Förderung der Nutzung bestehender Angebote und zur Schliessung von Angebotslücken im Bereich Cyber-Risiken wurde in Zusammenarbeit mit dem Verband ICT-Berufsbildung das neue Berufsbild „ICT Security Expert“ kreiert (siehe [32]). Die ers-

ten Abschlüsse sollen im Herbst 2018 möglich sein. Das Projekt stösst in der Privatwirtschaft auf viel Interesse und wird von verschiedenen Firmen mitfinanziert. Es basiert auf bestehenden Ausbildungen, ergänzt diese aber dort, wo noch Lücken bestehen. Das Qualifikationsprofil wird gemeinsam mit Vertretern der Privatwirtschaft definiert.

Im Bereich der Hochschulen fördert der Bund die Ausbildung im Rahmen der Forschung. Die Umsetzung der Massnahme ist darum eng mit der Massnahme 1 verknüpft und wird vom CoPIRFCyber koordiniert (vgl. M1, Kap. 3.12). Durch die gezielte Förderung von Forschungsvorhaben soll die Ausbildung an den Hochschulen gestärkt werden. Ein besonderes Augenmerk wird dabei auf die Förderung von interdisziplinären Ausbildungen gelegt.

Impact: kann aktuell nicht beurteilt werden

Ausbildung ist eine langfristige Aufgabe. Es ist aktuell zu früh, um einen konkreten Impact zu messen.

3.14. M16 Gesetzliche Grundlagen: Handlungsbedarf rechtlicher Grundlage

Titel Massnahme	Handlungsbedarf rechtlicher Grundlage
Ziele	Die zuständigen Departemente haben bestehende Gesetzgebungslücken als prioritär identifiziert, die nötigen rechtlichen Anpassungen gemacht sowie die dazu nötigen Entwürfe auf den passenden Normstufen erarbeitet. Ein Regelungskonzept wird dem Bundesrat vorgelegt.
Verantwortliches Amt / Organisationseinheit	ISB
Konsultierte Unterlagen für die WiÜ	Quellen: [127]
Interviews	Siehe Anhang A.1, Interview I 13

3.14.1. Erwartete Wirkung: Wirkungsmodell M16

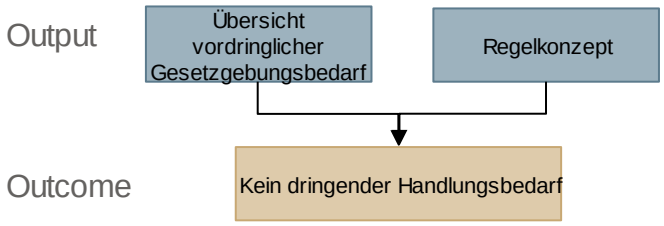

Abbildung 15 Wirkungsmodell M16

3.14.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Durch KS NCS bearbeitet
Finanzielle Mittel	Keine
Mitarbeit durch andere Ämter / Organisationseinheiten	Die zuständigen Bundesstellen wurden involviert (siehe Liste im Anhang M16 1).

3.14.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome	☐ aktuell nicht beurteilbar			
Impact	☐ aktuell nicht beurteilbar			

3.14.4. *Begründung der Beurteilung*

<u>Output: Ziele sind erreicht:</u>

> Eine Übersicht über den dringlichen Gesetzgebungsbedarf wurde erstellt. Dazu wurden alle zuständigen Bundesstellen befragt. Es wurde kein dringender Gesetzgebungs- oder Revisionsbedarf festgestellt.

- **Übersicht vordringlicher Gesetzgebungsbedarf:** Das Dokument „Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarf zum Meilenstein 16.1 (siehe [127]) enthält die geforderte Übersicht. Alle zuständigen Bundesstellen wurden begrüsst. Die KS NCS hat via Generalsekretariate und Bundeskanzlei 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.
- **Regelkonzept:** Das VBS/V war die einzige Bundesstelle, die einen vordringlichen Handlungsbedarf angegeben hatte. In der Zwischenzeit wurde dieser Punkt durch das neue Militärgesetz im Art. 100 geregelt. Aktuell wird dazu die Verordnung erstellt.

Der STA-NCS hat die Übersicht zum Gesetzgebungsbedarf zur Kenntnis genommen und entschieden, die weitere Umsetzung der Massnahme 16 zu sistieren. Es ist nicht Aufgabe der NCS, den Rechtssetzungsbedarf festzustellen, sondern diejenige der zuständigen Bundesstellen.

<u>Outcome kann nicht beurteilt werden:</u>

> Es wurde kein dringender Handlungsbedarf festgestellt. Dadurch entfällt der Schritt der Ausarbeitung von rechtlichen Anpassungen. Eine Beurteilung des Outcome der Massnahme 16 ist deshalb nicht möglich.

- **Es besteht kein dringender Handlungsbedarf.** Die Massnahme ist umgesetzt, muss jedoch wie jede NCS Massnahme regelmässig überprüft werden. Durch die beschriebene Übersicht existiert nur eine erste Auslegeordnung. Die rechtliche Situation muss sich den stetig veränderten Cyber-Bedrohungen anpassen (siehe z. B. laufende Arbeiten zum Informationssicherheitsgesetz (ISG) oder die *Network Information Security Directive* (NIS), die im Juni 2016 von der EU verabschiedet wurde).

<u>Impact: Nicht zu beurteilen</u>

> Weil die Massnahme mit der Erstellung der Übersicht abgeschlossen wurde, kann kein Impact gemessen werden.

4. Schnittstellen

Die Massnahmen der NCS fokussieren auf die Aufgaben der zivilen Bundesverwaltung und sollen einen Beitrag zur Stärkung des Schutzes von kritischen Intrastrukturen leisten. Im Rahmen dieser Aufgaben sind zwei Schnittstellen von grosser Bedeutung: die Schnittstelle zu den Aktivitäten der Kantonen und die Schnittstelle zu den Aktivitäten der Armee im Bereich Cyber-Defense. Um die Wirkung der NCS vollumfänglich beurteilen zu können, wurden auch diese beiden Schnittstellen analysiert.

4.1. Schnittstelle zu den Kantonen – Arbeiten des Sicherheitsverbunds Schweiz

Art der Schnittstelle	Schnittstelle Umsetzung der NCS in den Kantonen
Ziele	Einbezug der Kantone in sämtliche sie betreffende Umsetzungsmassnahmen der NCS, Koordination der laufenden Aktivitäten der Kantone zum Schutz vor Cyber-Risiken, Austausch von Informationen und Wissen.
Verantwortliches Amt / Organisationseinheit	Sicherheitsverbund Schweiz (SVS)
Konsultierte Unterlagen für die WiÜ	Quellen: [128], [129], [130]
Interviews	

4.1.1. Erwartete Wirkung: Wirkungsmodell Schnittstelle Kantone

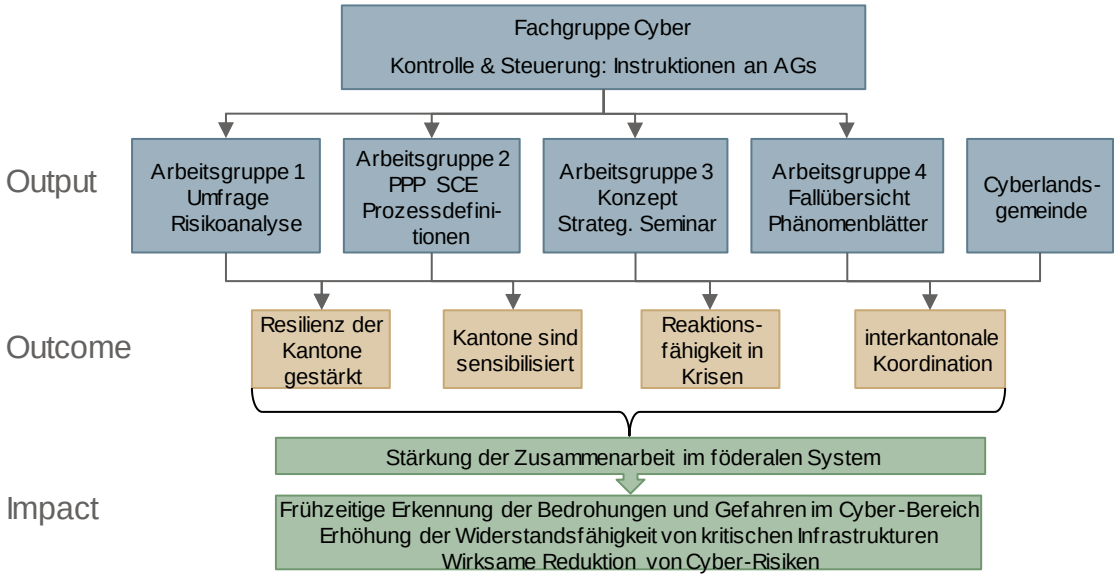

Abbildung 16 Wirkungsmodell SVS

4.1.2. Input: Eingesetzte Ressourcen

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Die Koordinationsarbeiten werden vollumfänglich vom SVS ohne zusätzliche Ressourcen übernommen.
Finanzielle Mittel	Vom SVS getragen
Mitarbeit durch andere Ämter / Organisations-einheiten	Aus der Bundesverwaltung sind hauptsächlich folgende Stellen Involviert: KS NCS, MELANI, KOBIK, BK, BABS, Armee.

4.1.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output				✓✓
Outcome			✓	
Impact	☐ aktuell nicht beurteilbar			

4.1.4. *Begründung der Beurteilung*

<u>Output: Ziele erreicht</u>

Die Fachgruppe Cyber und die vier dazugehörigen Arbeitsgruppen haben sich etabliert und einen wichtigen Beitrag zur Verankerung der NCS in den Kantonen geleistet. Durch die jährlich stattfindende Cyber-Landsgemeinde ist der gegenseitige Austausch sichergestellt.

- **Fachgruppe Cyber:** Im Umsetzungsplan NCS wird der Sicherheitsverbund Schweiz (SVS) damit beauftragt, eine Fachgruppe-Cyber (FG-C) zu konstituieren, welche die Schnittstelle zwischen der NCS Umsetzung und den Aktivitäten der Kantone wahrnimmt.

  Die Fachgruppe-Cyber wurde 2013 geschaffen. Sie besteht aus folgenden Organisationen: Sicherheitsverbund Schweiz (SVS), Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), Koordinationsstelle NCS, Staatsschreiberkonferenz, MELANI, Schweizerische Informatikkonferenz (SIK), Armee, Konferenz der Kantonsregierungen (KdK), Schweizerischer Städteverband und Gemeindeverband. Die Fachgruppe tagt zweimal jährlich und stellt so die Koordination aller laufenden Arbeiten sicher. Für die operative Wahrung der Schnittstellen zur NCS hat die FG-C vier Arbeitsgruppen etabliert, deren Leiter ebenfalls in der Fachgruppe vertreten sind.

  Arbeitsgruppen: Die Arbeitsgruppen wurden entlang der wichtigsten Schnittstellen der NCS zu den Kantonen definiert. Die vier Arbeitsgruppen haben folgende Ziele erreicht:

  – **AG1 Risikoanalyse und Präventionsmassenahmen** (als Schnittstelle zu den NCS-Massnahmen 2 und 3): Die Kantone haben in Form eines Fragebogens ein Hilfsmittel zur Selbstevaluation zum Umgang mit Cyber-Risiken erhalten. Die Arbeitsgruppe hat die Antworten ausgewertet und den Kantonen Vorschläge unterbreitet, wie sie die erkannten Cyber-Risiken reduzieren können. Als nächster Schritt wird die Arbeitsgruppe die Kantone bei der Integration der Cyber-Risiken in das generelle Risikomanagement unterstützten.

  – **AG2 Incident-Management** (als Schnittstelle zu den NCS-Massnahmen 4 und 5): Die Arbeitsgruppe hat die Prozesse zur Bearbeitung von Cyber-Vorfällen in mehreren Dokumenten beschrieben. Z. B. werden die Prozesse zur Zusammenarbeit zwischen MELANI und den Kantonen im Falle eines Incidents festgehalten (Dokument IMTP6 [130]). Die Kantone haben in der AG2 den Wunsch geäussert, auf breites Expertenwissen zugreifen zu können. Diesem Wunsch ist mit der Gründung der Public Private Partnership „Swiss Cyber Experts“ entsprochen worden.

  – **AG3 Krisenmanagement Bund und Kantone** (als Schnittstelle zur NCS-Massnahme 15): Die Arbeitsgruppe erweiterte den Fokus des Krisenmanagements um die Dimension der Kantone und bindet auch kritische Infrastrukturen

ein. Das Konzept wurde an zwei Veranstaltungen erprobt: am strategischen Seminar vom 11. Juni 2015 sowie an einem Test in der RUAG Cyber-Range am 23. Februar 2016. Das strategische Seminar hat auf bestehende Unklarheiten hingewiesen. Als Fallbeispiel wurde ein Angriff auf das Rentensystem der Schweiz simuliert. Die Integration der involvierten Fachbereiche in das Krisenmanagement wurde analysiert. Im Zentrum stand die Koordination zwischen Bund und Kantonen als Hauptpartner im SVS. Die einzelnen Akteure konnten die erkannten Schwachstellen und Unklarheiten in ihren Organisationen thematisieren und angehen.

– **AG4 Übersicht Straffälle und Koordination interkantonale Fallkomplexe** (als Schnittstelle zur NCS-Massnahme 6): Erarbeitete unter der Leitung der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) und unter Einbezug der Kantone ein Konzept zur Führung einer nationalen Fallübersicht (Straffälle) und zur Koordination von interkantonalen Fallkomplexen. Auch die Phänomene-Blätter mit den Beschreibungen der verschiedenen Arten von Cyber-Kriminalität sind für die Kantone wichtig. Sie waren bei der Erstellung der Phänomen-Blätter involviert, erhielten diese zur Stellungnahme und haben sie im Rahmen der Vernehmlassung inhaltlich gutgeheissen. Die Frage der staatsanwaltschaftlichen Zuständigkeit konnte noch nicht geregelt werden. Da KOBIK bereits eine von Bund und Kantonen gemeinsam getragene Organisationseinheit ist, konnte viel Koordinationsarbeit direkt von KOBIK erledigt werden.

– **Cyber-Landsgemeinde:** Die erste Cyber-Landsgemeinde fand 2013 statt und wird nun jährlich durchgeführt. Sie hat sich gut etabliert und erfreut sich einer grossen Teilnehmerzahl aus den Kantonen. Sie leistet damit einen wichtigen Beitrag zum Informationsaustausch zwischen Bund und Kantonen im Bereich der Cyber-Risiken.

<u>Outcome: Ziele sind grösstenteils erreicht</u>

Die Zusammenarbeit zwischen Bund und Kantonen und zwischen den Kantonen selbst konnte gestärkt werden. Da nun alle Kantone Mitglied bei MELANI sind, wurde die Reaktionsfähigkeit verbessert. Der Einbezug der Kantone in Krisenmanagement-Übungen hilft, Schwachstellen im Resilienz-Management zu erkennen und zu beseitigen. Die Zusammenarbeit ist aber in allen Bereichen noch weiter ausbaubar.

- **Zusammenarbeit:** Die Zusammenarbeit und Vernetzung der Kantone und des Bundes wurden durch die Arbeitsgruppen und die Cyber-Landsgemeinde wesentlich gestärkt. Als Beispiel dafür kann der deutlich verbesserte Einbezug der Kantone bei MELANI dienen: Zu Beginn der NCS-Umsetzung hatten 10 Kantone bei MELANI noch nicht mitgemacht. Dank der Unterstützung des SVS sind seit Ende 2015 sämtliche Kantone Mitglied beim GK von MELANI.

  Die Arbeiten haben aber auch gezeigt, dass weiterer Koordinationsbedarf zwischen Bund und Kantonen besteht. In folgenden Bereichen besteht noch weiteres Potential für eine stärkere Zusammenarbeit:

  – Gemeinsames Lagebild und Beurteilung der Lage
  – Abstimmung der Handlungsoptionen und Synchronisation der Entscheide
  – Ressourcenüberblick und Ressourcenmanagement
  – Abstimmung des Kontinuitätsmanagements
  – Erarbeitung gemeinsamer Botschaften und deren Kommunikation

- **Resilienz-Management:** Ein Beitrag zur Stärkung der Resilienz der Kantone gegenüber Cyber-Risiken konnte dank der Selbstevaluation der AG1 geleistet werden. Die Kantone haben nun einen besseren Eindruck, wo sie stehen und welche Mass-

nahmen sie zusätzlich ergreifen sollten. Wichtig war auch das Durchführen von Übungen zum Krisenmanagement unter Einbezug der Kantone und der kritischen Infrastrukturen. Erst in diesen Übungen wurde klar, wo die Prozesse noch nicht genügend ausgearbeitet sind.

- **Reaktionsfähigkeit:** Dank der Mitgliedschaft bei MELANI haben nun sämtliche Kantone direkten Zugang zur 7x24h Pikettdienst von MELANI. Einzelne Kantone sind zudem am Aufbau von Security Operation Centers (im Kanton Waadt ist dieses schon operativ). Der gegenseitige Austausch ermöglicht es, von Erfahrungen zu profitieren und die geeignetsten Lösungen zu identifizieren. Die Definition der Prozesse bei einem Cyber Incident erlaubt den richtigen Umgang und die schnelle Reaktion auf einen Vorfall.
- **Interkantonale Koordination:** Durch die Diskussionen in den AGs mit Beteiligung verschiedener Kantone können Wissen und Erfahrungen ausgetauscht werden. Die erarbeiteten Produkte werden allen Kantonen zur Verfügung gestellt. Sich zu kennen führt zum Aufbau eines Vertrauensverhältnisses und einem leichteren Austausch von Informationen.

Impact: nicht beurteilbar

Die Zusammenarbeit mit den Kantonen hat sich klar verbessert. Inwieweit dies bereits zu einer gefestigten Struktur der föderalen Zusammenarbeit im Bereich Cyber-Risiken geführt hat, kann noch nicht beurteilt werden, da die meisten Arbeiten noch nicht vollständig abgeschlossen sind. Aktuell hängt die Arbeit in den Arbeitsgruppen stark vom freiwilligen Einsatz von Einzelpersonen ab.

4.2. Schnittstelle zur Armee

Art der Schnittstelle	Schnittstelle Umsetzung der NCS in den Kantonen
Ziele	Die vorhandenen Fähigkeiten der Armee sollen von den verantwortlichen Ämtern in ihren Umsetzungsprozessen bei Bedarf eingebaut und abgerufen werden können. Dies entspricht dem bewährten Ansatz der Subsidiarität der Armee z. B. bei Naturkatastrophen.
Verantwortliches Amt / Organisationseinheit	Organisationseinheit Cyber Defence des MND, KS NCS
Konsultierte Unterlagen für die WiÜ	Quellen: Interviews, vertrauliche Unterlagen
Interviews	I 10

Die Armee gehört zu den kritischen Infrastrukturen des Landes. Aufgrund ihrer Aufträge sind die Verwendung des Cyber-Raums im Allgemeinen und besonders die Cyber-Bedrohungen zentrale Themen geworden. Zu den wichtigsten unmittelbaren Aufgaben der Armee gehört der Schutz ihrer eigenen IKT-Systeme und -Infrastrukturen in allen Lagen, um ihre Einsatzfähigkeit und Handlungsfreiheit permanent sicherzustellen.

Die NCS schliesst den Kriegs- und Konfliktfall explizit aus und delegiert die Zuständigkeit im Falle eines entsprechenden Cyberangriffs an die Armee. Es ist aber nicht definiert wie und wann die Zuständigkeit von den zivilen Stellen zur Armee wechselt bzw. wie die formelle Zusammenarbeit im Krisenfall funktionieren sollte.

In Krisen unterhalb der Konfliktschwelle kommt der Armee eine subsidiäre Rolle zu. Voraussetzung für den subsidiären Einsatz der Armee im Rahmen der NCS ist, dass frühzeitig Synergien identifiziert und genutzt werden. Die frühe Einbindung der Armee soll

auch dazu führen, die von der Armee im 2013 erarbeitete Konzeptionsstudie Cyber-Defence (KS CYD) auf das Gesamtsystem Schweiz abzustimmen.

4.2.1. *Erwartete Wirkung: Wirkungsmodell Schnittstelle zur Armee*

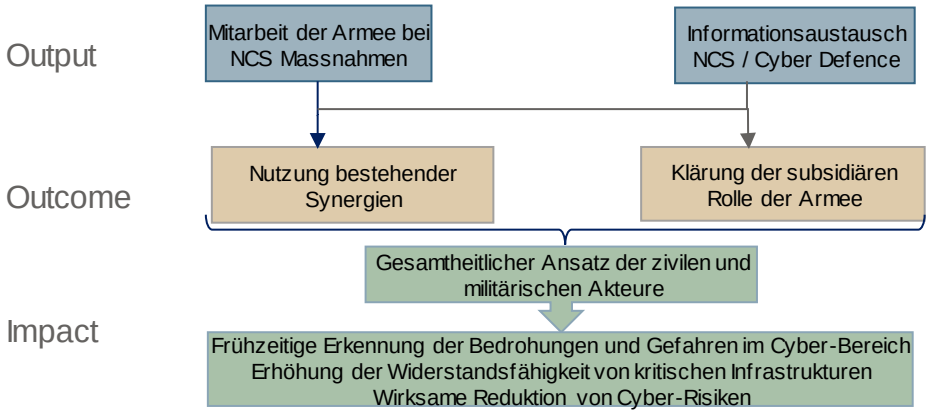

Abbildung 17 Wirkungsmodell Schnittstellen Armee

4.2.2. *Input: Eingesetzte Ressourcen*

Art der Ressource	Anzahl eingesetzter NCS-Ressourcen
Personalressourcen	Keine zusätzlichen Ressourcen. Für die Armee trägt die Organisationseinheit Cyber Defence den Aufwand der Koordination mit der NCS, für die NCS übernimmt die Koordinationsstelle NCS.
Finanzielle Mittel	Keine
Mitarbeit durch andere Ämter / Organisationseinheiten	An der Zusammenarbeit beteiligte Organisationseinheiten: MELANI, NDB, SBFI, EDA, BK

4.2.3. *Beurteilung der Zielerreichung und Wirkung*

Ebene	Ziele nicht erreicht	Ziele nur teilweise erreicht	Ziele grösstenteils erreicht	Ziele erreicht
Output		✖		
Outcome		✖		
Impact	☐ aktuell nicht beurteilbar			

4.2.4. *Begründung der Beurteilung*

<u>Output: Ziele nur teilweise erreicht</u>

Die Armee arbeitet bei einem grossen Teil der NCS mit. Auf der operativen Eben besteht deshalb auch ein guter Informationsaustausch. Aufgrund der knappen Ressourcen beschränkt man sich aber auf die wichtigsten Aufgaben und die Kompetenzen sind somit stark beschränkt. Die jeweiligen Verantwortlichen kennen die gegenseitigen Fähigkeiten und Aktivitäten. Auf der strategischen Ebene findet jedoch zu wenig Austausch statt, so dass verschiedene Fragen der Zuständigkeit und der Erwartungen an die Armee nicht genügend geklärt sind.

- **Mitarbeit der Armee bei NCS Massnahmen:** Die Armee ist an unterschiedlichen Massnahmen direkt oder indirekt eingebunden. Dies betrifft folgende Massnahmen:
  - M1, M7, M8: Die Armee hat sich bei diesen Massnahmen stark engagiert und die erste Informationserhebung finanziert. Sie hat den Anstoss zur Gründung des CoPIRFCyber (vgl. Kapitel 3.12) gegeben, der nun vom SBFI geleitet wird. Die Vertreter der Armee sind weiterhin involviert.
  - M4, M5, M14: Die Armee ist direkt eingebunden, insbesondere über die Leistungsvereinbarung zwischen dem NDB und dem FUB ZEO. Zum Lagebild trägt die Armee nur beschränkt bei, da dieses noch wenig konsolidiert ist. Die wenig vorhandenen Informationen werden jedoch mit dem NDB wöchentlich ausgetauscht. Mit MELANI gibt es einen regen Austausch auf der operativen Ebene; die Informationen aus dem MELANI-Netz werden der OE CYD MND nicht geliefert. Auf der strategischen Ebene gibt es zu wenig Austausch und das gegenseitige Verständnis über die Rollen und Zuständigkeiten sind nicht restlos geklärt.
  - M2/12: Die Armee war bei der Erarbeitung der Risiko und Verwundbarkeitsanalyse des kritischen Teilsektors Armee massgeblich beteiligt und führt bereits im Rahmen eigener Projekte verschiedene Analysen und Massnahmen (ISK VBS) zur Verbesserung der Resilienz ihrer eigenen Infrastrukturen durch.
  - M10: Die Armee nimmt an den Sitzungen der Fachgruppe Cyber-International teil und ist deshalb gut informiert. Umgekehrt informiert sie die Gruppe über die internationalen Aspekte der Aktivitäten im Bereich Cyber-Defence.
  - M15: Die Armee ist involviert, es bleibt aber weitgehend ungeklärt, inwiefern die Armee im Falle einer Krise mit Cyberausprägung einen subsidiären Beitrag zur Bewältigung der Krise leisten kann. Das VBS hat aber das Ziel, dies bis Ende 2016 zu klären.
  - M6: Es erfolgt ein informeller Austausch. Der Fokus der militärischen Lageeinschätzung unterscheidet sich aber naturgemäss vom Fokus der polizeilichen Ermittler.
  - Übrige Massnahmen: Die Armee wird teilweise informiert, ist aber nicht direkt involviert. Obschon die Armee ein grosser Leistungserbringer ist, wurde sie nicht im STA NCS eingeladen; das Problem ist aber intern beim VBS zu suchen.
- **Informationsaustausch NCS / Cyber Defence der Armee**: Der Austausch von Informationen zwischen der Armee und der NCS erfolgt auf der operativen Ebene informell und ist seit Jahren etabliert. Die Armee ist generell über den Inhalt und den Umsetzungsstand der NCS informiert und umgekehrt kennen die beteiligten Ämter die Fähigkeiten der Armee. Zu bemängeln ist, dass der Austausch nur auf operativer Ebene stattfindet. Auf strategischer Ebene findet nur ein unstrukturierter und unregelmässiger Austausch statt. Die Klärung der Rollen im Kriegs- und Konfliktfall wird von der Armee durch Übungen gefördert (z.B. Cyber Coalition, Cyber Pakt, Locked Shield).

Outcome: Ziele nur teilweise erreicht

Durch das Engagement der Armee bei verschiedenen NCS-Massnahmen konnten Synergien genutzt werden. Hingegen bleibt die subsidiäre Rolle der Armee ungeklärt. Es ist nicht definiert, welche Zuständigkeiten die Armee im Falle einer Eskalation einer Cyber-Krise hat und wann sie alarmiert wird. Ohne klare Definitionen ist eine subsidiäre Unterstützung der Armee im Krisenfall nicht möglich, insbesondere wenn ihre Mittel primär für den Selbstschutz eingesetzt werden und somit keine Mittel für Aussenaufgaben zur Verfügung stehen.

- **Nutzung bestehender Synergien:** Die Armee erbringt aktuell Leistungen in den oben erwähnten Massnahmen. Dabei werden Synergien gut genutzt. Die Zusammenarbeit erfolgt hauptsächlich über persönliche Beziehung und weniger über formale Prozesse (mit Ausnahme der Leistungsvereinbarung zwischen FUB ZEO und NDB). Zwischen den CERTs hat sich eine gute Zusammenarbeit entwickelt, wobei die Zuständigkeiten noch klarer definiert werden müssen. Gestärkt werden könnte der Einbezug des MND bei der Erstellung des Lagebilds.
- **Klärung der subsidiären Rolle der Armee:** Die subsidiäre Unterstützung ist nicht geregelt. Die NCS macht diesbezüglich keine klaren Vorgaben. Zudem verfügt die Armee aktuell nicht über die Mittel, um den Auftrag der subsidiären Unterstützung quer über alle Massnahmen wahrnehmen zu können. Priorität hat der Schutz der eigenen Systeme.

  Ungeklärt bleibt insbesondere die Frage nach der Führungsverantwortung im Fall einer Eskalation einer Cyber-Krise zu einem Cyber-Konflikt. Hier muss eine revidierte NCS klarere Angaben machen. Wichtig wäre auch, dass diese Fälle in Übungen mit allen Beteiligten berücksichtigt werden, so dass getestet werden kann, ob die richtigen Personen zum richtigen Zeitpunkt alarmiert werden und ob genügend Durchhaltefähigkeit vorhanden ist. Eine subsidiäre Unterstützung ist nur möglich, wenn klar definiert wird, zu welchem Zeitpunkt innerhalb einer Krise welche Leistungen von der Armee erwartet werden.

Impact: kann derzeit nicht beurteilt werden

Ob es gelungen ist, die Zusammenarbeit zwischen Armee und NCS soweit zu stärken, dass in Zukunft ein gesamtheitlicher Ansatz zum Umgang mit Cyber-Risiken gelebt wird, kann erst beurteilt werden, wenn eine revidierte Fassung der NCS vorliegt. Es muss dann gelingen, genauer zu definieren, was die Rolle der Armee im Bereich der Cyber-Risiken ist.

5. Massnahmenübergreifende Fragestellungen

Nach der Beurteilung der einzelnen Massnahmen, geht es in diesem Kapitel um die Beurteilung folgender Punkte:

- **Ressourcen:** Sind für die NCS insgesamt die richtige Menge an personellen und finanziellen Ressourcen gesprochen worden?
- **Inhalte der NCS:** Waren die Ziele der Strategie die richtigen und sind sie weiterhin gültig? Ist das Portfolio der Massnahmen vollständig?
- **Organisationsstrukturen:** Hat sich die dezentrale Umsetzung der NCS bewährt? Wie gut haben der STA NCS und die KS NCS ihre jeweiligen Rollen wahrgenommen?
- **Kommunikation:** Wurde intern und extern ausreichend kommuniziert?

Zur Beurteilung dieser Fragen wird auf die Antworten der befragten Massnahmenverantwortlichen und übrigen Beteiligten zurückgegriffen. In jedem Interview wurde den Befragten auch Gelegenheit gegeben, sich zu diesen massnahemenübergreifenden Fragen zu äussern. Nicht alle konnten oder wollten sich zu diesen Fragen Stellung beziehen, aber zusammen mit der Auswertung der Dokumente ergibt sich ein relativ deutliches Bild, das es ermöglicht, die oben aufgelisteten Fragen zu beurteilen.

5.1. Ressourcenplanung (Input)

✔ **Die Ressourcenplanung war grösstenteils zutreffend**

Für die Umsetzung der Massnahmen wurden insgesamt knapp genügend Stellen eingeplant. Weil in den meisten beteiligten Organisationseinheiten bereits zu ähnlichen Themen gearbeitet wird, konnte von vorhandenem Know-how profitiert werden. Dies ermöglichte die Umsetzung der Massnahmen mit wenigen Personalressourcen. Teilweise war es für die Organisationseinheiten schwierig, die Stellen zu besetzen, da nur befristete Arbeitsverträge angeboten werden konnten. Die NCS verfügt über kein eigenes Budget, was den Entscheidungsspielraum des STA NCS einschränkt.

- **Ressourcenplanung für die Umsetzung der Massnahmen:** Von den für die NCS insgesamt gesprochenen 30 Stellen wurden 28 direkt in den für die Umsetzung der Massnahmen verantwortlichen Organisationseinheiten geschaffen. Es wurde bereits in Kapitel 3 pro Massnahmen aufgezeigt, für welche Massnahme welche Ressourcen eingesetzt wurden. Aus einer gesamtheitlichen Perspektive lässt sich sagen, dass der Ressourcenbedarf realistisch eingeschätzt wurde. Es standen für die meisten Massnahmen genügend, wenn auch eher knapp bemessene Ressourcen zur Verfügung. Unterschätzt wurde der Ressourcenbedarf für die Umsetzung der Massnahme 3. Nicht (bzw. nur kurz) besetzt wurde die Stelle bei KOBIK für die Massnahme 6.

  Verschiedene Interviewpartner haben darauf hingewiesen, dass die Befristung von Stellen Schwierigkeiten bei der Rekrutierung bereiten kann. Befristete Stellen sind für potentielle Arbeitnehmer weniger attraktiv und haben daher tendenziell einen negativen Einfluss auf die Anzahl und Qualität der Bewerber.

- **Ressourcenplanung für die übergeordneten Aufgaben:** Für die massnahmenübergreifende Aufgaben der Koordination, des Controllings und der Berichtserstattung wurden zwei Stellen der KS NCS im Informatiksteuerungsorgan des Bundes (ISB) geschaffen. Auch diesbezüglich lässt sich festhalten, dass sich die Dotierung

der KS NCS mit zwei Stellen als im Rahmen der Aufgaben knapp genügend herausgestellt hat.

Die NCS verfügt nicht über ein eigenes Budget. Die übergeordneten Aufgaben (NCS-Tagung, Wirksamkeitsüberprüfung) werden durch das ISB finanziert. Das Fehlen eines eigenen Budgets bedeutet, dass der STA NCS wenig Spielraum hat, eigene Projekte zu lancieren oder über die Finanzierung von externer Unterstützung bei ausgewählten Massnahmen Prioritäten zu setzen.

5.2. Beurteilung der Inhalte der NCS

Die Inhalte der NCS haben sich bewährt

Die strategischen Ziele der NCS haben sich bewährt und sind nach wie vor sinnvoll. Die aus den Zielen abgeleiteten Massnahmen decken das breite Feld der nötigen Aktivitäten zur Bekämpfung von Cyber-Risiken gut ab, das Massnahmenportfolio könnte aber stärker zusammengefasst werden.

Im Umsetzungsplan wurden Massnahmenziele festgelegt, aber keine Messgrössen für die Bestimmung des Umsetzungserfolgs definiert. Grund dafür war, dass bei vielen Massnahmen zuerst Wissen und Strukturen aufgebaut werden mussten und exakte Sollvorgaben wenig sinnvoll erschienen. Mit dem Aufbau des strategischen Controllings wurde ein Instrument zur Prüfung des Umsetzungsfortschritts geschaffen. Das Vorgehen hat sich insgesamt als richtig erwiesen.

Zu den einzelnen Aspekten der inhaltlichen Gestaltung der NCS lassen sich folgende Bemerkungen festhalten:

- **Gültigkeit der übergeordneten Ziele:** Die meisten Interviewpartner betrachten die übergeordneten Ziele der NCS – die frühzeitige Erkennung von Cyber-Gefahren und -Bedrohungen; die Stärkung der Widerstandsfähigkeit bei den kritischen Infrastrukturen und die Reduktion von Cyber-Risiken – als weiterhin gültig. Die Ziele haben sich als generelle strategische Vorgaben bewährt.
- **Rahmenbedingungen und Schnittstellen:** In der NCS sind die wichtigsten Strategien und Projekte des Bundes mit Anknüpfungspunkten zur NCS genannt. Weil Cyber ein Querschnittsthema ist, sind diese Schnittstellen von grosser Bedeutung. Bei einer allfälligen Weiterführung der NCS müssen die Entwicklungen in diesen Strategien und Projekten berücksichtigt werden.
- **Vollständigkeit des Massnahmenportfolios:** Auch das Massnahmenportfolio der NCS hat sich grundsätzlich bewährt. Die formulierten Massnahmen haben die wichtigsten Aspekte gut abgedeckt. Es ist aber den Massnahmenverantwortlichen bewusst, dass bisher vor allem Aufbauarbeit geleistet wurde. Die aufgebauten Strukturen müssen dazu genutzt werden, die nächsten Schritte anzugehen. Die Sicherstellung der Kontinuität der bisher geleisteten Arbeiten ist allen Beteiligten ein grosses Anliegen.

  In Bezug auf das Gesamtportfolio hat sich gezeigt, dass gewisse Massnahmen inhaltlich eng verbunden sind. Es wäre teilweise möglich gewesen, bereits im Umsetzungsplan verschiedene Massnahmen zusammenzuführen (z. B. hätte man M7 und M8 jeweils zu einer Massnahme fusionieren können). Eine Verdichtung des Portfolios auf weniger Massnahmen wäre für eine bessere Übersichtlichkeit nützlich und sollte in Zukunft angedacht werden.

Als wichtigste künftige Themen, die in der NCS aktuell noch nicht abgedeckt sind, haben die Interviewpartner folgende Themen identifiziert:

- Bedeutung und Konsequenzen der Network Information Security (NIS) Directive der EU für die Schweiz
- Frage der Einführung einer Meldepflicht von sicherheitsrelevanten Cyber-Vorfällen für Betreiber kritischer Infrastrukturen (diese Frage gewinnt ebenfalls im Zuge der NIS-Directive an Relevanz)
- Engagement der Schweiz bei Capacity-Building-Initiativen für Entwicklungsländer

- **Konkretisierung der Massnahmenziele im Umsetzungsplan:** Die in der NCS formulierten Ziele für die einzelnen Massnahmen werden im Umsetzungsplan NCS konkretisiert. Für alle Massnahmen wurden Massnahmenziele definiert, es wurde aber darauf verzichtet, Messgrössen für den Erfolg der Umsetzung zu bestimmen. Die Meilensteinplanung und die Definition der zu leistenden Lieferobjekte legten die Massnahmenverantwortlichen selbst in Zusammenarbeit mit der KS NCS fest. Aus Sicht des Controllings und des Wirksamkeitsnachweises wäre es wünschenswert gewesen, wenn solche Kriterien bereits im Umsetzungsplan festgelegt worden wären. Ausserdem hätten sich einige der befragten Massnahmenverantwortlichen solche Vorgaben gewünscht.

  Andererseits haben mehrere Massnahmenverantwortliche erwähnt, dass es während der Umsetzung aufgrund von neuen Erkenntnissen oder Ereignissen nötig wurde, die Meilensteinplanung anzupassen. Bei vielen Massnahmen ging es um den Aufbau von Wissen und Strukturen und es wäre kaum möglich gewesen, die richtigen Messkriterien schon vor dem Beginn der Arbeiten zu definieren. Verschiedene Befragte haben darum betont, dass eine gewisse Flexibilität für eine erfolgreiche Umsetzung unabdingbar ist und eher generelle Massnahmenziele statt strikte Vorgaben formuliert werden sollten.

  Es besteht ein Spannungsfeld zwischen der Forderung nach vorformulierten Kriterien für die Zielerreichung und Messbarkeit sowie der Wunsch nach Flexibilität. Der Umsetzungsplan gab den Massnahmenverantwortlichen genügend Spielraum, da er keine unmittelbar messbaren Ziele vorgibt. Dies wurde durch das von der KS NCS aufgebaute strategische Controlling kompensiert. Damit wurde ein guter Mittelweg gefunden, bei dem zwar Vorgaben gemacht werden, der aber den Massnahmenverantwortlichen genügend Spielraum liess.

5.3. Organisationsstrukturen der NCS

✓ **Die Organisationsstruktur der NCS war grösstenteils richtig gewählt**

Die dezentrale Umsetzung der NCS, mit einer Verteilung der Verantwortung an die jeweils für eine Massnahme zuständigen Ämter, hat sich als sehr gut geeignet erwiesen. Sie ist der richtige Ansatz für den Umgang mit dem Querschnittsthema Cyber-Risiken. Voraussetzung für den Erfolg dieser Lösung sind gut funktionierende Koordinationsorgane. Der STA NCS und die KS NCS haben sich diesbezüglich bewährt. Leichten Korrekturbedarf gibt es bei der Zusammensetzung des STA NCS, bei dem Vertreter zu wichtigen Schnittstellen Einsitz erhalten sollten. In Bezug auf die KS NCS ist deren Angliederung an MELANI ungünstig gewählt, da die KS NCS gegenüber den Massnahmenverantwortlichen (zu denen MELANI gehört) unabhängig sein sollte, damit sie bei Bedarf neutral zwischen verschiedenen Interessen vermitteln und das strategische Controlling effektiv durchführen kann.

Aufgrund der geführten Interviews und der Auswertung der Dokumente, lassen sich zur Organisationsstruktur der NCS folgende Beurteilungen abgeben:

- **Die dezentrale Organisationsstruktur:** Generell wird die dezentrale Organisationsstruktur der NCS als wichtigstes Element der erfolgreichen Umsetzung der NCS bezeichnet. Sie entspricht dem themenübergreifenden Charakter der Cyber-Risiken und passt auf das föderale System der Schweiz. Eine der Herausforderungen der dezentralen Umsetzung liegt darin, alle relevanten Akteure einzubeziehen. Es ist nicht immer gelungen, alle Regulatoren im notwendigen Ausmass in die Arbeiten einzubinden. Diese Bemühungen müssten in Zukunft verstärkt werden. Eine weitere Herausforderung besteht im einheitlichen und klar erkennbaren Auftritt gegen aussen. Dies ist schwieriger, wenn mehrere Akteure an der Umsetzung beteiligt sind. Ob dies gelungen ist, wird im Kapitel 5.4 Interne und externe Kommunikation genauer betrachtet.

- **Rolle und Zusammensetzung des STA NCS:** Der Steuerungsausschuss NCS hat seine Funktion als Aufsichtsorgan über die Verabschiedung des halbjährlichen strategischen Controllings wahrgenommen. Der Beschluss zur Ergreifung einer Sondermassnahme zu Massnahme 3 hat gezeigt, dass der STA NCS auch bereit ist, korrigierend in die Umsetzung der NCS einzugreifen.

  Die direkte Vertretung aller beteiligten Organisationseinheiten hat sich bewährt, ebenso ist zu begrüssen, dass die Economiesuisse als Beobachterin vertreten ist. Hingegen sind die Armee und das BABS nicht im STA NCS vertreten, was die Koordination zwischen Cyber-Defence der Armee, der Nationalen Strategie zum Schutz der kritischen Infrastrukturen und der NCS eher erschwert hat.

  Geleitet wird der STA NCS vom Delegierten für die Informatiksteuerung des Bundes. Die Federführung durch das ISB wird generell als sinnvoll, jedoch nicht als zwingend erachtet. Das ISB eignet sich als Steuerungsorgan gut für die Führung einer Strategie und befasst sich über MELANI und ISB-SEC schon lange mit der Thematik der Cyber-Risiken. Nicht zwingend ist die Federführung durch das ISB deshalb, weil ein Querschnittsthema wie die NCS grundsätzlich von verschiedenen Organisationen geleitet werden könnte. Einzelne Akteure erachten die Federführung durch das ISB als problematisch, weil dadurch mögliche Zielkonflikte mit anderen Kernaufgaben des ISBs bestehen.

- **Rolle der KS NCS:** Die KS NCS ist bei der Umsetzung verschiedener Massnahmen direkt involviert, erledigt die administrativen Arbeiten für den STA NCS, organisiert die jährliche NCS Tagung, verfasst die NCS-Jahresberichte und führt das strategische Controlling durch. Diese Aufgaben werden von den Beteiligten als sehr wichtig eingeschätzt. Angesichts der dezentralen Umsetzung ist ein koordinierendes Organ entscheidend.

  Einige Interviewpartner äusserten sich kritisch zur organisatorischen Ansiedlung der KS NCS bei MELANI. Weil die KS NCS für den STA NCS das strategische Controlling durchführt, sollte sie nicht einer Einheit unterstehen, die sie zugleich kontrollieren muss. Bei einer allfälligen Weiterführung der NCS sollte die Unabhängigkeit der KS NCS gestärkt werden, indem sie nicht mehr bei MELANI angesiedelt wird.

5.4. Interne und externe Kommunikation

✖ **Die Kommunikationsaufgabe wurde nur teilweise wahrgenommen**

Für den Erfolg einer dezentralen Umsetzung der Strategie ist es entscheidend, dass die Kommunikation zwischen den beteiligten Partnern sehr gut funktioniert und dass auch gegen aussen gut vermittelt wird, wie und durch wen die Strategie implementiert wird. Die interne Kommunikation wurde gut wahrgenommen, die Beteiligten verfügten jeweils rechtzeitig über die nötigen Informationen.

Gegen aussen wurde aber zu wenig gut vermittelt, welche Ziele die NCS verfolgt, wie sie konkret umgesetzt werden und wie der Umsetzungsstand ist. Dies führt dazu, dass zu wenig bekannt ist, was der Bund im Bereich der Cyber-Risiken unternimmt und wo er die Grenzen seiner Zuständigkeit sieht.

Im Rahmen der Wirksamkeitsüberprüfung wurden die Beteiligten befragt, wie sie die interne und externe Kommunikation zur NCS beurteilen. Es ergaben sich folgende Beurteilungen:

- **Interne Kommunikation:** Die Befragten zeigen sich zufrieden mit dem Stand der internen Kommunikation. Viele Massnahmenverantwortliche tauschen sich regelmässig mit der KS NCS und mit weiteren Beteiligten aus. Über den Stand der Umsetzung der Strategie wird jeweils an den Sitzungen des STA NCS informiert. Generell wird geschätzt, dass die NCS die Kommunikation der Akteure mit einer Rolle im Bereich Cyber-Risiken stark verbessert oder teilweise sogar erst etabliert hat. Erleichtert wird die Kommunikation dadurch, dass viele Massnahmenverantwortliche sich aktiv bei der Umsetzung anderer Massnahmen beteiligen und so ein sehr gutes gegenseitiges Verständnis aufgebaut werden konnte.
- **Externe Kommunikation:** Während der Stand der internen Kommunikation gelobt wird, besteht in Bezug auf die externe Kommunikation Handlungsbedarf. Aufgrund der dezentralen Struktur bleibt es Aussenstehenden oft unklar, wer konkret für die Umsetzung der NCS generell oder einer spezifischen Massnahem verantwortlich ist. Als Kommunikationsmittel für ein breiteres Publikum stehen der Jahresbericht und die jährlich stattfindende NCS-Tagung zur Verfügung. Die KS NCS und die Massnahmenverantwortlichen treten zudem regelmässig an Veranstaltungen auf, um die NCS oder einzelne Massnahmen zu präsentieren. Es hat sich aber gezeigt, dass diese Kommunikationskanäle nicht genügen. Rückmeldungen aus der Wirtschaft und der Bevölkerung, aber auch die Rezeption in den Medien nach grösseren Cyber-Vorfällen haben gezeigt, dass teilweise falsche Erwartungen an die NCS gestellt werden. Es wurde zu wenig klar vermittelt, dass die Verantwortung für die Unternehmenssicherheit nicht von der NCS getragen wird, sondern weiterhin bei den Unternehmen selbst liegt. Es ist darum nötig, das Profil der NCS gegen aussen zu stärken und klarer zu kommunizieren.

6. Fazit

Mit dem Entscheid zur Umsetzung der NCS hat der Bundesrat signalisiert, dass er gewillt ist, den Cyber-Risiken mit Massnahmen in verschiedenen Bereichen zu begegnen. Die 16 Massnahmen des Umsetzungsplans geben vor, was welche Organisationseinheiten bis Ende 2017 leisten müssen, damit die strategischen Ziele der NCS – die Früherkennung von Bedrohungen und Gefahren, die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen und die Reduktion von Cyber-Risiken – erreicht werden können. Der Bundesrat war sich bei seinem Entscheid bewusst, dass die Thematik der Cyber-Risiken komplex ist und sich sehr rasch entwickelt. Er hat darum verfügt, dass fünf Jahre nach dem Beschluss der Strategie eine Wirksamkeitsanalyse vorgelegt werden soll, die aufzeigt, ob die Massnahmen wie vorgesehen umgesetzt werden konnten und ob sie geeignet sind, um die gesetzten Ziele zu erreichen. Mit dem vorliegenden Bericht wurde dieser Auftrag erfüllt und es ist nun möglich, ein Fazit zur Wirkung der NCS zu ziehen.

Zunächst kann festgestellt werden, dass die Umsetzung der Massnahmen gut vorangekommen ist. Die Wirksamkeitsüberprüfung hat gezeigt, dass die im Umsetzungsplan vorgesehenen Organisationsstrukturen und Prozesse grösstenteils implementiert sind und verschiedene Produkte (Berichte und Konzepte) termingerecht geliefert wurden. Dies gelang dank dem grossen Engagement der verantwortlichen Stellen mit einem bescheidenen zusätzlichen Ressourcenaufwand.

Der geleistete Output führte auch bereits zu einem beachtlichen Outcome. Die geschaffenen Strukturen und Prozesse und Produkte haben nachweislich zu gestärkten Kapazitäten, breiterem Wissensstand und besserer Koordination in den verschiedenen Bereichen geführt. Nicht bei allen Massnahmen ist der Outcome schon gleich gut messbar und bei drei der 16 Massnahmen wurde festgestellt, dass nicht alle Ziele wie gewünscht erreicht werden konnten. Insgesamt kann aber festgehalten werden, dass die Arbeiten zu den gewünschten Ergebnissen geführt haben und sich die Fähigkeiten zum Umgang mit Cyber-Risiken im Vergleich zur Situation vor der NCS deutlich verbessert haben.

Am schwierigsten messbar ist die direkte Wirkung (Impact) der geleisteten Arbeiten auf die strategischen Ziele. Im komplexen und dynamischen Kontext der Cyber-Risiken ist es kaum möglich kausale Zusammenhänge zwischen den ergriffenen Massnahmen und ihrer Wirkung auf die Ziele der NCS nachzuweisen. Zudem ist der Zeitpunkt der Wirksamkeitsüberprüfung für eine solche Messung zu früh. Typischerweise entfalten die getroffenen Massnahmen ihre Wirkung erst nach einem gewissen Zeitraum. Entsprechend konnte erst bei drei Massnahmen ein Impact auf mindestens eines der drei strategischen Ziele gemessen werden. Dies bedeutet jedoch keineswegs, dass für die übrigen Massnahmen kein Impact erwartet wird. In den im Rahmen der Überprüfung entwickelten Wirkungsmodellen für alle Massnahmen wird aufgezeigt, welche konkrete Wirkung auf Grund der bisher erzielten Resultate zu erwarten ist.

Die Wirksamkeitsüberprüfung beschränkte sich aber nicht nur auf die Beurteilung der einzelnen Massnahmen. Es wurde auch untersucht, ob die Schnittstellen der NCS zu den Arbeiten der Kantone und der Armee ausreichend berücksichtigt wurden. Während diese Frage in Bezug auf die Kantone bejaht werden kann, blieben an der Schnittstelle zur Armee noch wichtige Fragen ungeklärt. Die Abgrenzung und Zuständigkeit zwischen den zivilen Aufgaben der NCS und der Führung durch die Armee im Konfliktfall sind nicht abschliessend geklärt. Ebenfalls offen bleibt, wie die Armee die zivilen Behörden in Bezug auf Cyber-Risiken subsidiär unterstützen kann und soll.

Schliesslich wurde auch die massnahmenübergeordneten Fragen untersucht: Waren die Ziele der NCS überhaupt richtig gewählt? Sind genügend Ressourcen gesprochen worden? Hat sich die dezentrale Organisationstruktur bewährt? Und hat die Kommunikation funktioniert? Generell lässt sich auch zu diesen Fragen ein positives Fazit ziehen. Die In-

halte haben sich grundsätzlich bewährt, die Ressourcen waren knapp ausreichend und die dezentrale Organisationsstruktur wird begrüsst. Bemängelt wurde einzig die Kommunikation gegen aussen, die nach Ansicht verschiedener Interviewpartner gestärkt werden muss.

Abschliessend kann gesagt werden, dass die NCS sowohl auf der Ebene der Massnahmen, als auch der Schnittstellen und der massnahmenübergreifenden Fragen als Erfolg zu werten ist. Es muss aber gleichzeitig betont werden, dass mit den umgesetzten Massnahmen erst ein erster Schritt vollbracht ist. Ein Etappenziel ist erreicht, es ist aber klar zu früh und wäre dem Thema unangemessen, sich mit dem Erreichten zufrieden zu geben. Weil sich Cyber-Risiken rasant weiterentwickeln bedeutet Stillstand Rückschritt. Zum Fazit aus der Wirksamkeitsüberprüfung gehört darum auch die Erkenntnis, dass die aufgebaute Arbeit zwingend weitergeführt werden sollte. Nur durch kontinuierliche Anstrengung wird es möglich sein, die Schweiz so gut wie möglich vor Cyber-Risiken zu schützen.

A. Interviews / Fragebogen

A.1. Liste der durchgeführten Interviews

Die Interviews sind mit einem Index versehen (I 1 - I 14) für die Verlinkung innerhalb des Dokuments.

Nr.	Datum	Massnahmen	Massnahmenverantwortliche	Zeit und Ort
I 1	26. Februar 2016	M1, M7, M8	Blaise Roulet (Delegierter FB/SBFI) Manuel Suter (Koordinator NCS im ISB)	14:00-16:00 AWK, Laupenstrasse 4, Bern
I 2	4. März 2016	M4, M14	Philipp Kronig Marc Henauer (Leiter MELANI OIC im NDB) Mauro Vignati (Leiter Cyber NDB im NDB) Pascal Lamia (Leiter MELANI im ISB)	10:00-12:00 P20, Bern
I 3	15. März 2016	M2, M12	Ruedi Rytz (Leiter der Geschäftsstellen Infrastrukturbereiche im BWL) Daniel Caduff (Wissenschaftlicher Mitarbeiter im BWL) Dario Walder (Wissenschaftlicher Mitarbeiter im BWL)	10:00-12:00 AWK, Laupenstrasse 4, Bern
I 4	15. März 2016	M10	Michele Coduri (Leiter der ASP im EDA) Laura Crespo (Wissenschaftliche Mitarbeiterin bei der ASP im EDA)	14:00-16:00 EDA/ASP, Bernastrasse, Bern
I 5	22. März 2016	M6	Adrian Lobsiger (stellvertretender Direktor des Bundesamts für Polizei (fedpol)) Tobias Bolliger (Kommissariatsleiter a.i. KOBIK im EJPD)	10:00-12:00 AWK, Laupenstrasse 4, Bern
I 6	5. April 2016	M9, M11	Rene Dönni (Vizedirektor Leiter Abteilung Telecomdienste und Post beim BAKOM) Nicolas Rollier (Wissenschaftlicher Mitarbeiter beim BAKOM) Matthias Ziehl, (Telecomingenieur im BAKOM)	M9, M11 10:00-12:00 AWK, Laupenstrasse 4, Bern
I 7	5. April 2016	M3	Marcel Frauenknecht (Leiter ISB SEC im ISB) Rolf Oppliger (ISB)	14:00-16:00 AWK, Laupenstrasse 4, Bern
I 8	12. April 2016	M2, M12	Stefan Brem (Chef Risikogrundlagen und Forschungskoordination im BABS) Angelika Bischof (Wissenschaftliche Mitarbeiterin im BABS) Giorgio Ravioli (Wissenschaftlicher Mitarbeiter im BABS)	14:00-16:00 AWK, Laupenstrasse 4, Bern
I 9	15. April 2016	M15, SVS	André Duvillard (Delegierter des SVS) Melanie Friedli (Wissenschaftliche Mitarbeiterin im SVS) Nicolas Mueller (Leiter Krisenmanagement-Ausbildung des Bundes in der BK)	10:00-11:30 AWK, Laupenstrasse 4, Bern
I 10	25. April 2016	M5	Pascal Lamia (Leiter MELANI ISB) Reto Inversini (Analytiker GovCERT)	10:00-12:00 AWK, Laupenstrasse 4, Bern

Nr.	Datum	Massnahmen	Massnahmenverantwortliche	Zeit und Ort
I 11	3. Mai 2016	Schnittstelle Armee, M4, M14	BV_CYD MND Gérald Vernez BV_FUB ZEO (CNO) Riccardo Sibillia	10:00-12:00 P20
I 12	3. Mai 2016	M13	Stefanie Frey (Koordinatorin NCS im ISB) Ronja Tschümperlin (Analytikerin MELANI OIC im NDB) Manuel Suter (Koordinator NCS im ISB)	14:00-16:00 P20
I 13	24. Mai 2016	M16	Stefanie Frey	Fragebogen schriftlich ausgefüllt
I 14	3. Juni 2016	M2, M12	BFE Marc Kenzelmann, Vizedir. BFE, Leiter Aufsicht und Sicherheit Hans-Peter Binder, Leiter Risikomanagement und Aufsicht Rohrleitungen Christian Holzner, Fachspezialist Risikomanagement	10:00-12:00 AWK, Laupenstrasse 4, Bern

A.2. Liste der verschickten Fragebogen

Eine Befragung mittels Fragebogen zu den Massnahmen M2 und M12 wurde in einigen Teilbereichen der kritischen Infrastruktur vorgenommen. Auch diese Befragungen sind für die Verlinkung innerhalb des Dokuments mit einem Index versehen (F 1 - F 6).

Nr.	Bereich	Kontaktierte Massnahmenverantwortliche der Teilbereiche
F 1	Erdgasversorgung	• Andre Martin, Gasverbund Mittelland, andre.martin@gvm-ag.ch • Jens Harenberg, Swissgas harenberg@swissgas.ch
F 2	Luftverkehr	• Peter Frey, Flughafen Zürich, peter.frei@zurich-airport.com • Reto Gasser, reto.gasser@2assistu.ch
F 3	Gesundheit	Teilsektor Labors • Samuel Roulin, Bundesamt für Gesundheit BAG samuel.roulin@bag.admin.ch • Martin Risch, Präsident SULM (Schweiz. Union für Labormedizin) und stv. Verwaltungsratspräsident Labormed. Zentrum Dr. Risch martin.risch@risch.ch Teilsektor Ärztliche Betreuung & Spitäler • Philipp Stoll, Vertreter H+ philipp.stoll@ukbb.ch
F 4	Banken	• Yves Obrist, FINMA Yves.Obrist@finma.ch • Michael Brügger, FINMA Michael.Bruegger@finma.ch • Thomas Rhomberg, SIX Group Services AG Thomas.Rhomberg@six-group.com
F 5	Medien	• Andreas Schneider, Schweizerische Radio und Fernsehgesellschaft SRG, andreas.schneider@srgssr.ch • René Wehrlin, Bundesamt für Kommunikation BAKOM rene.wehrlin@bakom.admin.ch
F 6	Stromversorger	• Reto Bondolfi, EWZ reto.bondolfi@ewz.ch • Daniel Schelbert, Elektrizitätswerk des Bezirks Schwyz d.schelbert@ebs-strom.ch • Beat Schüpbach, Swissgrid beat.schuepbach@swissgrid.ch (hat trotzt mehrfachem nachhacken nicht geantwortet)

B. Referenzierte Dokumente

Titel		Autor / Herausgeber	Datum
[1]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	19.06.2012
[2]	Umsetzungsplanung	Eidgenössisches Finanzdepartement EFD, Informatiksteuerungsorgan des Bundes ISB	13.05.2013
[3]	Detailkonzept zur Wirksamkeitsprüfung NCS)	ECOPLAN	28.07.2015
[4]	Ausschreibung „Offerten-Anfrage - Wirksamkeitsüberprüfung «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken»“	Eidgenössisches Finanzdepartement EFD, Informatiksteuerungsorgan des Bundes ISB	16.11.2015
[5]	Offerte für Beratungs- und Ingenieurleistungen Wirksamkeitsüberprüfung NCS	AWK	22.10.2015
[6]	Roadmap NCS	ISB	13.07.2015
[7]	Programm Tagung Cyber-Risiken Schweiz 2015	ISB	02.11.2015
[8]	Mandat Steuerungsausschuss NCS und Koordinationsstelle NCS	ISB	15.05.2013
[9]	Strategisches Controlling des Steuerungsausschusses NCS zum Umsetzungsstand per 01.01.2015	KS NCS	27.05.2015
[10]	Protokoll der 1. Sitzung des Steuerungsausschusses NCS	KS NCS	30.10.2013
[11]	Protokoll der 2. Sitzung des Steuerungsausschusses NCS	KS NCS	11.02.2014
[12]	Protokoll der 3. Sitzung des Steuerungsausschusses NCS	KS NCS	19.08.2014
[13]	Protokoll der 4. Sitzung des Steuerungsausschusses NCS	KS NCS	10.02.2015
[14]	Protokoll der 5. Sitzung des Steuerungsausschusses NCS	KS NCS	20.08.2015
[15]	Protokoll der 6. Sitzung des Steuerungsausschusses NCS	KS NCS	25.02.2016
Forschung (M1), Übersicht Kompetenzbildung (M7) und Kompetenzbildung (M8)			
[16]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 1: Identifikation von Cyber-Risiken durch Forschung, Meilenstein 1.1: Organisationsstruktur und Prozessbeschreibung	KS NCS	30.07.2015
[17]	Protokoll CoPIRFCyber	Eidgenössisches Finanzdepartement EFD	11.09.2015
[18]	Protokoll CoPIRFCyber	Eidgenössisches Finanzdepartement EFD	18.12.2015
[19]	Protokoll CoPIRFCyber	Eidgenössisches Finanzdepartement EFD	22.05.2015
[20]	Provisorisches Programm	Swiss Cyber Risk Research Conference 2016	24.11.2015
[21]	Expertengruppe „Forschung und Bildung zu Cyber-Risiken“	Eidgenössisches Finanzdepartement EFD	November 2015
[22]	Thematische Untergruppen: Projekt „Forschung und Bildung zu Cyber-Risiken“	Eidgenössisches Finanzdepartement EFD	
[23]	Research Capabilities in Switzerland	Bernhard Hämmerli & Solange Ghernaoutie	
[24]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 7: Über-	Eidgenössisches Finanzdepartement EFD	26.06.2014

Titel		Autor / Herausgeber	Datum
	sicht Kompetenzbildungsangebote, Meilenstein 7.1: Übersicht Kompetenzbildungsangebote für den Umgang mit Cyber-Risiken		
[25]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 7: Übersicht Kompetenzbildungsangebote, Meilenstein 7.2: Kurzbericht Identifizierung qualitativ hochstehender Kompetenzbildungsangebote durch Expertenempfehlungen	Eidgenössisches Finanzdepartement EFD	30.06.2014
[26]	Kompetenzbildungsangebote im Umgang mit Cyber-Risiken (Massnahme 7 NCS)	international institute for management in technology - iimt	16.03.2015
[27]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Abschlussbericht für die Massnahme M8 „Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung der Angebotslücken“	Eidgenössisches Finanzdepartement EFD	25.02.2016
[28]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 8: Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung der Angebotslücken, Meilenstein 8.1: Organisationsstruktur (Mandat und Mitgliedschaft der steuernden Einheit)	Eidgenössisches Finanzdepartement EFD	30.07.2015
[29]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 8: Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung der Angebotslücken, Meilenstein 8.2: Konzeptentwurf	Eidgenössisches Finanzdepartement EFD	30.07.2015
[30]	Cybersecurity Competence Building Trends	DiploFoundation	November 2015
[31]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS, Massnahme 8: Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung der Angebotslücken, Meilenstein 8.4: Umsetzungskonzept	Eidgenössisches Finanzdepartement EFD	02.02.2016
[32]	ICT Security Expert, Ein neues Berufsbild	Informatiksteuerorgan des Bundes ISB	20.05.2016
[33]	Ressourcen Tabelle NCS	Informatiksteuerorgan des Bundes ISB	10.02.2016
Analysen Sektoren (M2, M12)			
[34]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Luftverkehr	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	27.11.2015
[35]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Medien	Bundesamt für Bevölkerungsschutz BABS	03.12.2015
[36]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Labors	Bundesamt für Bevölkerungsschutz BABS	05.02.2016
[37]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Zivilschutz	Bundesamt für Bevölkerungsschutz BABS	16.02.2016
[38]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	26.09.2014
[39]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Strassenverkehr	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	12.02.2015
[40]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	27.11.2015
[41]	Massnahmen zur Stärkung der IKT-Resilienz der Erdgasversorgung	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	23.02.2016

Titel		Autor / Herausgeber	Datum
[42]	Methode: Risiko- und Verwundbarkeitsanalyse kritischer Teilsektoren	Bundesamt für Bevölkerungsschutz BABS	26.05.2015
[43]	Risiko- und Verwundbarkeitsanalyse des Teilsektors ärztliche Betreuung und Spitäler	Bundesamt für Bevölkerungsschutz BABS	18.12.2015
[44]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Banken	Bundesamt für Bevölkerungsschutz BABS	07.03.2016
[45]	Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Blaulichtorganisationen	Bundesamt für Bevölkerungsschutz BABS	20.05.2016
[46]	Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Parlament, Regierung, Justiz und Verwaltung	Bundesamt für Bevölkerungsschutz BABS	20.05.2016
[47]	Checkliste: Überprüfung der Vorarbeiten zur Verwundbarkeitsanalyse SKI / NCS	Bundesamt für Bevölkerungsschutz BABS	
[48]	Aktennotiz Besprechung BWL-BABS Umsetzung NCS- / SKI-Strategie	Bundesamt für Bevölkerungsschutz BABS	24.03.2014
[49]	E-Mail von Daniel Schelbert	Elektrizitätswerk des Bezirks Schwyz AG	21.07.2015
[50]	E-Mail von Hansjörg Holenstein	Verband Schweizerischer Elektrizitätsunternehmen VSE	19.03.2015
[51]	Zusammenarbeit MELANI – BWL / Abgleich Informationen NCS	Prozess Zusammenarbeit MELANI-BWL	
[52]	Befundsliste: Bundesamt für Zivilluftfahrt	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF	20.09.2015
[53]	Review Kommentare Stromversorgung	Review-Kommentare-Stromversorgung	???
[54]	Erstellung und Abnahme von Verwundbarkeitsanalysen	Bundesamt für wirtschaftliche Landesversorgung BWL	11.09.2014
[55]	Massnahmen zur Steigerung der Resilienz im Luftverkehr	Bundesamt für wirtschaftliche Landesversorgung BWL	12.01.2016
[56]	Kommentiertes Inhaltsverzeichnis Risiko- und Verwundbarkeitsanalyse in kritischen Teilsektoren	Bundesamt für Bevölkerungsschutz	
[57]	Meilensteinreporting MS 2.1 Risiko- und Verwundbarkeitsanalyse NCS	Bundesamt für Bevölkerungsschutz	
[58]	Umsetzungsplanung M2 NCS / M15 SKI-Strategie	Bundesamt für Bevölkerungsschutz BABS / Bundesamt für wirtschaftliche Landesversorgung BWL	18.03.2014
[59]	Kommentiertes Inhaltsverzeichnis Massnahmen zur Verbesserung der Resilienz kritischer Teilsektoren	Bundesamt für Bevölkerungsschutz	
[60]	Meilensteinreporting MS 12.1: „Massnahmen zur Verbesserung der Resilienz NCS“	Bundesamt für Bevölkerungsschutz BABS / Bundesamt für wirtschaftliche Landesversorgung BWL	
[61]	Aktennotiz Besprechung BWL-BABS Umsetzung NCS- / SKI-Strategie	Bundesamt für Bevölkerungsschutz BABS	24.03.2014
[62]	E-Mail – Weitere Adressen: Strategie zum Schutz der Schweiz vor Cyberrisiken	Hansjörg Holenstein, Verband Schweizerischer Elektrizitätsunternehmen VSE	19.03.2015
[63]	Review-Kommentare Stromversorgung		15.03.2016
[64]	Prozessdarstellung zur Erstellung und Freigabe von Verwundbarkeitsanalysen NCS	Bundesamt für wirtschaftliche Landesversorgung BWL	11.09.2014
Verwundbarkeitsanalyse IKT Bund (M3)			

Titel		Autor / Herausgeber	Datum
[65]	Antrag für den STA NCS vom 25. Februar 2016: Sondermassnahme zur Massnahme 3	Eidgenössisches Finanzdepartement EFD	25.02.2016
[66]	Verwundbarkeitsanalyse für die Prozesse- und IKT-Systemkomponenten		
[67]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept, Basisdokument	Eidgenössisches Finanzdepartement EFD	11.11.2015
[68]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept, Meilenstein 3.3: Prüfkonzept	Eidgenössisches Finanzdepartement EFD	11.11.2015
[69]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept, Meilenstein 3.2: Konzept steht im Entwurf und wird fortlaufend weiterentwickelt	Eidgenössisches Finanzdepartement EFD	04.02.2015
[70]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), Massnahme 3: Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept, Meilenstein 3.1: Grobkonzept (Konzept zur Erstellung eines Prüfkonzepts)	Eidgenössisches Finanzdepartement EFD	02.09.2014
Lagebild (M4) und Identifikation Täterschaft (M14)			
[71]	Bedrohungslage im Cyberraum	Melde- und Analysestelle Informationssicherung MELANI	
[72]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), Massnahme 4 und 14 „Lagebild und Täterschaft Identifikation“, Meilensteine 4.6 und 14.3: Spezialwissen und Fähigkeiten im Cyber-Bereich sind beim NDB aufgebaut, mit FUB und MND als Leistungserbringer	Eidgenössisches Finanzdepartement EFD	
[73]	NCS-Massnahme 4: Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch	Eidgenössisches Finanzdepartement EFD	20.02.2014
[74]	Umsetzung der Nationalen Cyber Strategie (NCS) im NDB, Bericht zu den Meilensteinen 4.2 / 5.1 / 14.1 der Umsetzungs-Roadmap	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport	
[75]	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 4 „Erstellung Lagebild und Lageentwicklung“, Meilenstein 4.3: Anpassung Service Level Agreement (SLA) zusammen mit FUB-ZEO ist etabliert.	Eidgenössisches Finanzdepartement EFD	
[76]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): Mesure 4 „Etablissement de l’image et du développement de la situation“, Etappe 4.4: Radar de la situation.	Eidgenössisches Finanzdepartement EFD	
[77]	Passive DNS Plattform	Melde- und Analysestelle Informationssicherung MELANI	22.12.2014

Titel	Autor / Herausgeber	Datum
[78] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 4 und 14 „Lagebild und Täterschaft Identifikation“, Meilensteine 4.6 und 14.3: Spezialwissen und Fähigkeiten im Cyber-Bereich sind beim NDB aufgebaut, mit FUB und MND als Leistungserbringer	Eidgenössisches Finanzdepartement EFD	
[79] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 14 „Aktive Massnahmen und Identifikation der Täterschaft“, Meilenstein 14.2: Anpassung Service Level Agreement (SLA) zusammen mit FUB-ZEO ist etabliert.	Eidgenössisches Finanzdepartement EFD	
Vorfallanalyse (M5)		
[80] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 5 „Vorfallanalyse und Nachbearbeitung von Vorfällen“, Meilenstein 5.2: Organisationsstruktur GovCERT	Eidgenössisches Finanzdepartement EFD	29.04.2014
[81] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 5 „Vorfallanalyse und Nachbearbeitung von Vorfällen“, Meilenstein 5.3: Erhöhung der Durchhaltefähigkeit im GovCERT	Eidgenössisches Finanzdepartement EFD	30.06.2014
[82] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 5 „Vorfallanalyse / Nachbearbeitung von Vorfällen“, Meilenstein 5.4: Die Malware Information Sharing Plattform (MISP) ist etabliert.	Eidgenössisches Finanzdepartement EFD	16.06.2014
[83] Passive DNS Platform	Melde- und Analysestelle Informationssicherung MELANI	18.06.2015
Übersicht Straffälle (M6)		
[84] Cyberkriminalitäts-Phänomene: Definitionen, Modus operandi und Massnahmen	Eidgenössisches Justiz- und Polizeidepartement EJPD	28.05.2015
[85] Stand der Umsetzung M6 NCS: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	Eidgenössisches Justiz- und Polizeidepartement EJPD	20.08.2015
[86] Jahresbericht 2014: Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK	Eidgenössisches Justiz- und Polizeidepartement EJPD	26.03.2015
[87] Konzept zur Massnahme 6 NCS: Nationale Fallübersicht und Koordination interkantonaler Fallkomplexe	Eidgenössisches Justiz- und Polizeidepartement EJPD	März 2016
[88] Strukturtabelle Deliktsschwerpunkt/-bereich		
[89] Stand der Umsetzung M6 NCS: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	Eidgenössisches Justiz- und Polizeidepartement EJPD	20.08.2015
Internet Governance (M9) und Internationale Standardisierung (M11)		
[90] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): Massnahme 9 „Internet Governance“, Meilenstein 9.1: Übersicht zu prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet Governance	Bundesamt für Kommunikation BAKOM	30.05.2014
[91] Nationale Strategie zum Schutz der Schweiz	Bundesamt für Kommunikation BAKOM	30.05.2014

Titel		Autor / Herausgeber	Datum
	vor Cyber-Risiken (NCS): Massnahme 9 „Internet Governance“, Meilenstein 9.2: Übersicht zu den Prozessen zur Internet Governance und zur Beteiligung der Schweiz ist erstellt		
[92]	NCS Meilenstein 9.3: Prioritäten der Schweiz in der Internet Governance und die Einbindung relevanter Akteure	Bundesamt für Kommunikation BAKOM	20.10.2014
[93]	Workshop NCS-M11	Bundesamt für Kommunikation BAKOM	15.02.2016
[94]	NCS-M11 Internationale Standardisierung und Initiativen im Bereich Sicherheit: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	Bundesamt für Kommunikation BAKOM	10.12.2014
[95]	NCS-M11 Internationale Standardisierung und Initiativen im Bereich Sicherheit: Übersicht über beteiligte Akteure aus der Schweiz und deren Tätigkeiten	Bundesamt für Kommunikation BAKOM	11.12.2015
[96]	NCS-M11 Internationale Standardisierung und Initiativen im Bereich Sicherheit: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	Bundesamt für Kommunikation BAKOM	11.12.2015
[97]	NCS-M11 Internationale Standardisierung und Initiativen im Bereich Sicherheit: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	Bundesamt für Kommunikation BAKOM	10.12.2014
Internationale Kooperation (M10)			
[98]	Jahresübersicht der Aktivitäten im Cyber-Bereich		2014
[99]	Jahresübersicht der Aktivitäten im Cyber-Bereich		2015
[100]	Fragenkataloge WiÜ NCS – Fokus Internationale Kooperation Cyber-Sicherheit (M10)	Philipp Grabher, Markus Meier AWK	08.03.2016
[101]	Notiz an den Staatssekretär: Cyber-Kriminalität: Aussenpolitische Positionierung und Handlungsfelder für die Schweiz	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	10.02.2015
[102]	Notiz an den Staatssekretär: Cyber-Sicherheit: Schweizer Handlungsfelder zur Förderung von staatlichen Verhaltensnormen	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	12.08.2015
[103]	Konzept zur Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken im EDA		20.12.2013
[104]	Übersicht der in 2014 geleisteten Aktivitäten im Bereich Cyber-Aussenpolitik	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	09.04.2015
[105]	Stand der Umsetzung M6 NCS: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	Eidgenössisches Justiz- und Polizeidepartement EJPD	20.08.2015
[106]	Aussenpolitische Aufgaben im Cyber-Bereich – Eine Übersicht der in 2015 geleisteten Aktivitäten	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	04.01.2016
[107]	A Geneva Declaration for Cyberspace	Stein Schjolberg, Norway	Januar 2016
[108]	Mandat Fachgruppe Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	21.03.2014

Titel	Autor / Herausgeber	Datum
[109] Notiz an den Staatssekretär: Cyber-Kriminalität: Aussenpolitische Positionierung und Handlungsfelder für die Schweiz	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	10.02.2015
[110] Notiz an den Staatssekretär: Cyber-Sicherheit: Schweizer Handlungsfelder zur Förderung von staatlichen Verhaltensnormen	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	12.08.2015
[111] Notiz an den Staatssekretär: Internet Governance: Aussenpolitische Grundlagen und Handlungsfelder für das EDA	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	04.03.2015
[112] Konstituierende Sitzung der Fachgruppe Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	25.10.2013
[113] Protokoll Fachgruppe Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	21.03.2014
[114] Protokoll Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	18.12.2014
[115] Protokoll Fachgruppe Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	30.06.2015
[116] Protokoll: Fachgruppe Cyber-International (FG-CI)	Eidgenössisches Departement für auswärtige Angelegenheiten EDA	25.09.2015
Krisenmanagement (M13, M15)		
[117] Konzept für das nationale Krisenmanagement bei Krisen mit Cyberausprägung auf der Grundlage der Massnahme 15 NCS		16.04.2016
[118] Auswertung Evaluation MELANI	Manuel Suter, KS NCS	07.01.2016
[119] Fragebogen Evaluation MELANI	Manuel Suter, KS NCS	
[120] Resultate Evaluation MELANI	KS NCS	März 2016
[121] Bericht der ersten Cyber Koordinationssitzung	Dario Walder, SVS	25.03.2013
[122] Foliensatz 3. Cyber Landsgemeinde		23.04.2015
[123] Strategische Seminar vom 11. Juni 2015, Kurzbericht		11.06.2015
[124] Umsetzung Massnahme 15 NCS Konzept für das Krisenmanagement bei Cyberkrisen	Stéphane Derron	26.09.2013
[125] Umsetzung Massnahme 15 NCS Konzept für das Krisenmanagement bei Cyberkrisen (Stufe Bund)	Stéphane Derron	17.02.2014
[126] Programm zur 4. Cyber-Landsgemeinde		06.04.2016
Gesetzliche Grundlagen (M16)		
[127] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): NCS Massnahme 16 „Handlungsbedarf rechtliche Grundlagen“ Meilenstein 16.1: Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarfs im Cyber-Bereich	Stefanie Frey, KS NCS	30.06.2014
Schnittstellen SVS		
[128] Informationsblatt zur Fachgruppe und den Arbeitsgruppen Cyber des SVS	Sicherheitsverbund Schweiz SVS	25.02.2016
[129] SVS: NCS und Schnittstellen zu den Kantonen	Sicherheitsverbund Schweiz SVS	20.05.2016

Titel	Autor / Herausgeber	Datum
[130] Bearbeitung der von MELANI ausgegebenen Meldungen	Sicherheitsverbund Schweiz SVS	22.10.2015

C. Sammlung sämtlicher Fragebogen aus den Interviews

Sämtliche mit den Interviewpartnern erarbeiteten Fragebogen sind in einem separaten Anhang zusammengefasst. Dieser Anhang ist VERTRAULICH klassifiziert. Er kann bei der KS NCS eingesehen werden.