Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022

Der vorliegende Entwurf wurde unter Mitwirkung folgender Organisationen erstellt:

- **Bundesstellen:** EJPD-fedpol, EJPD-GS, UVEK-BAKOM, UVEK-BAV, UVEK-BAZL, UVEK-BFE, EDA-ASP, WBF-SBFI, WBF-BWL, VBS-BABS, VBS-GS, VBS-NDB, VBS-FUB, VBS-armasuisse, BK, EDI-GS, EDI-MeteoSchweiz EDI-BAG, EDI-BSV, EFD-ISB, EFD-GS, EFD-BIT, FINMA
- **Privatwirtschaft / Verbände:** economiesuisse, ICT-Switzerland, Schweizerischer Vesicherungsverband (SVV), Swissmem, RUAG, Swisscom, UBS, ISPIN, SATW
- **Kantone:** Vertretung durch Sicherheitsverbund Schweiz (SVS)

1 Einleitung

Die Schweiz befindet sich im Prozess der Digitalisierung. Die umfassende digitale Vernetzung prägt bereits heute Gesellschaft, Wirtschaft und Staat, und der rasche technologische Fortschritt wird diese Entwicklung weiter vorantreiben. Dieser Prozess eröffnet grosse Chancen, und die Schweiz ist gewillt, diese zu nutzen, um die Wohlfahrt in unserem Land langfristig zu sichern und auszubauen.
Dabei gilt es jedoch zu beachten, dass die Digitalisierung nicht nur Chancen, sondern auch Risiken birgt. Die damit einhergehende, zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) macht unser Land verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien.
Wie relevant diese Verwundbarkeit ist, zeigt sich mit Blick auf die Entwicklung der Bedrohungen im Cyber-Raum. Die grassierende Cyber-Kriminalität, die Häufung von Spionagetätigkeiten mit Hilfe von Cyber-Angriffen, Fälle von Cyber-Sabotage auf kritische Infrastrukturen wie Spitäler oder Energieversorger, die Verbreitung von gestohlener oder manipulierter Information zu Desinformations- und Propagandazwecken und die Zunahme von hybriden Konfliktformen, in welchen Cyber-Angriffe zur Destabilisierung von Staaten und Gesellschaften eingesetzt werden, machen deutlich, wie vielfältig diese Bedrohungen sind und wie rasant sie sich entwickeln.
Die Kombination aus der gestiegenen Abhängigkeit von funktionierenden IKT und der intensivierten Bedrohungslage führt dazu, dass die sich daraus ergebenden Risiken – welche als Cyber-Risiken bezeichnet werden – bei der Entwicklung der digitalen Gesellschaft zwingend beachtet werden müssen. Aus sicherheitspolitischer Sicht müssen Massnahmen getroffen werden, um die Unabhängigkeit und Sicherheit des Landes vor den neu entstehenden oder sich akzentuierenden Bedrohungen und Gefahren im Cyber-Raum zu wahren. Aus wirtschafts- und gesellschaftspolitischer Sicht muss sich die Schweiz vor Cyber-Risiken schützen, um die Chancen der Digitalisierung konsequent nutzen zu können und den Standortvorteil als sicheres Land zu erhalten. Ein vollständiger Schutz vor Cyber-Risiken ist mit verhältnismässigen Massnahmen jedoch nicht erreichbar. Deshalb muss die Schweiz ihre Resilienz gegenüber Cyber-Vorfällen erhöhen.
Die vorliegende Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) zeigt auf, wie diese Ziele bis 2022 erreicht werden sollen. Sie baut auf der von 2012-17 umgesetzten ersten NCS auf, entwickelt diese entsprechend der Verwundbarkeiten der Schweiz, der seit 2012 deutlich veränderten und intensivierten Bedrohungslage und deren absehbaren künftigen Entwicklung weiter und ergänzt sie mit weiteren Massnahmen. Sie bildet damit den strategischen Rahmen für die Stärkung der Prävention, Früherkennung, Reaktion und Resilienz in allen in Bezug auf Cyber-Risiken relevanten Bereichen.
Der Schutz vor Cyber-Risiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Dies bedeutet zunächst, dass alle Akteure für ihren eigenen Schutz die Verantwortung tragen. Die NCS unterstützt und koordiniert diese individuellen Schutzbemühungen. Darüber hinaus formuliert sie dort zusätzliche Massnahmen, wo die Cyber-Risiken wesentliche Auswirkungen auf die Entwicklung und das Wohlergehen unserer Gesellschaft haben. Aus der gemeinsamen Verantwortung ergibt sich auch die gemeinschaftliche Umsetzung der NCS. Bund, Kantone, Wirtschaft und Gesellschaft sollen die Massnahmen der NCS in enger Kooperation implementieren und dabei ihre jeweiligen Kompetenzen einbringen.
Die Herausforderungen im Umgang mit Cyber-Risiken sind gross, und sie werden weiter virulent bleiben. Umso wichtiger ist es, dass alle Akteure gemeinsam und koordiniert diese Herausforderungen angehen. Eine möglichst effektive Zusammenarbeit aller kompetenten Stellen und eine systematische internationale Vernetzung sind entscheidend für die Schaffung eines sicheren Umfeldes für die Digitalisierung der Gesellschaft und Wirtschaft. Die NCS 2018-22, welche von Bund, Kantonen und Wirtschaft gemeinsam entwickelt wurde, soll dabei als Handlungsanleitung und Orientierungshilfe dienen. Der zur Strategie gehörende Umsetzungsplan definiert die Zuständigkeiten und Umsetzungsverantwortung für die in der Strategie bestimmten Massnahmen.

2 Ausgangslage

Der erste Schritt zu einem effektiven Schutz der Schweiz vor Cyber-Risiken besteht in der Einschätzung der aktuellen und künftigen Bedrohungs- und Gefährdungslage. Angesichts der hohen Dynamik in der Entwicklung der Cyber-Bedrohungen geht es dabei nicht um eine präzise Berechnung der Risiken für die Schweiz, sondern um eine Abschätzung der strategischen Bedeutung der verschiedenen Bedrohungen und Gefährdungen sowie um einen Ausblick auf wahrscheinliche Tendenzen ihrer Entwicklung.
Neben der Bedrohungs- und Gefährdungslage ist der aktuelle Stand beim Schutz der Schweiz vor Cyber-Risiken der zweite wesentliche Faktor der Ausgangslage. Der künftige Handlungsbedarf wird ersichtlich, wenn die Bedrohungslage und deren künftige Entwicklung dem bestehenden Dispositiv zum Schutz der Schweiz vor Cyber-Risiken gegenübergestellt werden.

2.1 Die Cyber-Bedrohungslage

Um Klarheit zu erhalten, woher Cyber-Risiken stammen, werden die wichtigsten Bedrohungen und die durch sie bestehenden Gefährdungen für die Schweiz beschrieben. Dabei ist zu beachten, dass sich die Bedrohungen sehr dynamisch entwickeln. Wichtigste Treiber dafür sind die Digitalisierung, welche unsere Gesellschaft und Wirtschaft zunehmend verwundbarer gegenüber Störungen und Ausfällen von IKT-Systemen macht sowie die zu beobachtende Professionalisierung von Angreifern und die Ausweitung von Machtpolitik in den Cyber-Raum, welche die Bedrohung durch Cyber-Angriffen verstärken. Weil davon auszugehen ist, dass sich diese Trends fortsetzen, ist mit einer weiteren Intensivierung der Bedrohungslage zu rechnen.
Für die Einschätzung der Lage ist es wichtig, zwischen Bedrohungen durch beabsichtigte unerlaubte Handlungen (Cyber-Angriffe) und solchen Gefährdungen durch unbeabsichtigt herbeigeführte Ereignisse (menschliches Fehlverhalten und technische Ausfälle) zu unterscheiden. Diese werden deshalb in separaten Abschnitten beschrieben.

2.1.1 Cyber-Angriffe

Gleichzeitig zum zunehmenden Einsatz von IKT in allen geschäftlichen und sozialen Prozessen und den damit verbundenen Vorteilen von Effizienz, Informationsaustausch und Effektivität, sind die Bedrohungen und Gefährdungen durch Cyber-Angriffe in den letzten Jahren gestiegen. Erfolgreich durchgeführte Angriffe im In- und Ausland mit teilweise gravierenden Konsequenzen haben gezeigt, dass nicht nur die Häufigkeit und Komplexität der Cyber-Angriffe zunehmen, sondern diese auch vermehrt zielgerichtet gegen Staaten oder Unternehmen eingesetzt werden.
Zur Einschätzung der Lage ist es angesichts der Vielzahl von möglichen Cyber-Angriffen wichtig, zwischen verschiedenen Phänomenen zu unterscheiden. Unterscheidungskriterien sind der Zweck der Angriffe, die Akteure, welche hinter den Angriffen stehen und der Kreis jener, welche angegriffen werden. Auf dieser Grundlage lassen sich fünf Arten von Cyber-Angriffen unterscheiden, wobei zu beachten ist, dass diese häufig in Kombination auftreten und zwischen ihnen Überschneidungen bestehen.

Cyber-Kriminalität: Cyber-Kriminalität umfasst generell die Gesamtheit aller strafbaren Handlungen im Cyber-Raum. Im engeren Sinn geht es um Aktivitäten mit dem Motiv der Bereicherung. Der Cyber-Raum eignet sich gut dafür, da das Risiko für die Täter gering ist und durch die grosse Zahl von leicht erreichbaren Opfern hohe Gewinne möglich sind. Es erstaunt darum nicht, dass die Cyber-Kriminalität in den letzten Jahren stark zugenommen hat. Sie betrifft Unternehmen, Behörden und Bevölkerung gleichermassen und ist die Bedrohung mit der höchsten Eintrittswahrscheinlichkeit. Da es nicht das eigentliche Ziel der Angreifenden ist, das Funktionieren der Gesellschaft, Wirtschaft oder des Staates zu gefährden, be-

schränken sich die unmittelbaren Auswirkungen oft auf die betroffenen Opfer. Cyber-Kriminelle nehmen jedoch hohe Kollateralschäden in Kauf oder nutzen das Wissen um solche Auswirkungen sogar, um von den Opfern höhere Summen zu erpressen. Aus diesem Grund bergen Angriffe durch Cyber-Kriminelle ein hohes Schadenspotential für die gesamte Gesellschaft und Wirtschaft.
Im Umfeld der Cyber-Kriminalität entstehen eigentliche Geschäftsfelder, in welchen viel Geld verdient werden kann. Aufgrund der grossen Konkurrenz, aber auch der stetigen Nachrüstung der Abwehrmassnahmen ist der Innovationsdruck unter den kriminellen Akteuren hoch, weshalb die Angreifer laufend neue Geschäftsmodelle entwickeln. Entsprechend muss mit einer weiter wachsenden Häufigkeit und Spezialisierung der kriminellen Aktivitäten im Cyber-Raum gerechnet werden.

Cyber-Spionage: Cyber-Spionage ist eine Tätigkeit, um im Cyber-Raum für politische, militärische oder wirtschaftliche Zwecke unerlaubt an Informationen zu gelangen. Sie wird sowohl von staatlichen als auch nicht-staatlichen Akteuren ausgeübt. Im Fokus der Angreifer stehen sowohl Unternehmen als auch staatliche, gesellschaftliche oder internationale Institutionen. Die Schweizer Wirtschaft ist eine der innovativsten der Welt, und viele internationale Konzerne haben ihren Hauptsitz oder wichtige Datenzentren hier. Zudem beherbergt die Schweiz viele internationale Organisationen und ist häufig Gastgeber von internationalen Verhandlungen. Dies macht die Schweiz zu einem attraktiven Ziel von Cyber-Spionage. Die Auswirkungen können ein sehr unterschiedliches Ausmass annehmen, je nach Art und Umfang der Daten, zu welchen sich die Angreifer Zugang verschaffen. Die Auswirkungen sind meist nicht unmittelbar ersichtlich, da politische und wirtschaftliche Nachteile erst dann entstehen, wenn die Angreifer ihr erlangtes Wissen nutzen.
Cyber-Spionage wird weiter an Attraktivität gewinnen, da sie ein effizienter Weg ist, Informationen zu beschaffen. Die Angreifer haben Methoden entwickelt, um nach dem Eindringen in Netzwerke möglichst lange unentdeckt zu bleiben. Da die Schweiz bezüglich IKT in hohem Mass abhängig von ausländischen Herstellern ist, bleibt das Risiko bestehen, dass diese Produzenten in Zusammenarbeit mit den Nachrichtendiensten ihrer Länder bewusst Sicherheitslücken zum Zweck der Spionage offen lassen.

Cyber-Sabotage und -Terrorismus: Cyber-Sabotage bezeichnet eine Tätigkeit, um im Cyber-Raum das zuverlässige und fehlerfreie Funktionieren von IKT zu stören oder zu zerstören, was je nach Art der Sabotage und des angegriffenen Ziels auch zu physischen Auswirkungen führen kann. Die Motivation für solche Akte kann sehr unterschiedlich sein. So können sich beispielsweise frustrierte Mitarbeiter dazu entschliessen, die IKT einer Organisation zu sabotieren. Wird ein Sabotageakt von Tätern mit terroristischen Motiven durchgeführt, spricht man von Cyber-Terrorismus. Bei Cyber-Sabotage und Cyber-Terrorismus geht es nicht nur darum, möglichst grosse Schäden zu erzielen, sondern auch um Machtdemonstration und Einschüchterung, verbunden mit der Absicht, eine Organisation oder sogar die ganze Gesellschaft zu destabilisieren. Während auf internationaler Ebene verschiedene Sabotageakte, unter anderem auf die Energieversorgung von Staaten, bekannt sind, sind in der Schweiz bisher keine grösseren Fälle bekannt. Sollte die Schweiz oder Organisationen in oder aus der Schweiz aber aus politischen Gründen in den Fokus von staatlichen oder nicht-staatlichen Akteuren mit den entsprechenden Fähigkeiten geraten, würde die Wahrscheinlichkeit eines solchen Ereignis stark steigen. Die potenziellen Schäden sind dabei sehr gross.
Die Relevanz dieser Bedrohung wird mit der fortschreitenden Digitalisierung der Gesellschaft und Wirtschaft weiter steigen. Die zunehmende digitale Vernetzung von physischen Geräten über das Internet der Dinge lässt auch neue Formen der digitalen Manipulation zu – mit wiederum direkten Auswirkungen auf die physische Umwelt.

Desinformation und Propaganda: Die Bedrohung durch gezielte Verbreitung von Falschinformationen oder von illegal über Cyber-Angriffe beschafften Informationen mit dem Zweck der Diskreditierung von politischen, militärischen oder zivilgesellschaftlichen Akteuren hat stark an Bedeutung gewonnen. In verschiedenen Ländern wurden vor wichtigen Wahlen solche Aktivitäten beobachtet. Auch in der Schweiz muss mit der Möglichkeit gerechnet werden, dass staatliche oder nicht-staatliche Akteure versuchen, das Vertrauen der Bürgerinnen und Bürger in Staat und Institutionen zu unterminieren

Da die Bedeutung von sozialen Medien als Informationsquelle weiterhin zunimmt, muss auch davon ausgegangen werden, dass diese Kanäle für Propaganda genutzt werden, mit einer Mischung aus Falschinformationen, politischen Argumenten und gestohlenen Informationen, welche nur noch sehr schwer zu durchschauen ist.

Cyber in Konflikten: Während ein ausschliesslich im Cyber-Raum geführter Krieg (Cyber-War) gegenwärtig als unrealistisches Szenario betrachtet wird, hat sich gezeigt, dass Cyber-Angriffe aller Arten als Mittel der Kriegführung in verschiedenen Konflikten eingesetzt werden. Typischerweise handelt es sich dabei um hybride Konflikte, in welchen neben den militärischen auch politische, wirtschaftliche und kriminelle Mittel verwendet werden. Ein Zweck hybrider Konfliktführung ist es, die Verantwortlichkeiten in einem Konflikt unscharf zu machen. Cyber-Angriffe sind dafür ein probates Instrument, da sie kaum eindeutig zuzuordnen sind, vergleichsweise wenig kosten, sofort Wirkung erzielen, über beliebig grosse Distanzen hinweg einsetzbar sind und es erlauben, politisch-militärische Wirkung in der Grauzone unterhalb der Kriegsschwelle zu erzielen.
Die beträchtlichen Investitionen vieler Staaten zum Schutz und zur aktiven Abwehr von Cyber-Bedrohungen unterstreichen die Bedeutung von Cyber-Mitteln in der Sicherheitspolitik. Entsprechend ist zu erwarten, dass die Bedeutung von Cyber-Angriffen in Konflikten weiter zunehmen wird. Die Schweiz muss deshalb die Cyber-Diplomatie in die Vorbeugung von Konflikten sowie die Cyber-Abwehr in die Vorbereitungen auf einen Konfliktfall miteinbeziehen.

2.1.2 Menschliches Fehlverhalten und technische Ausfälle

Neben den gezielten und vorsätzlichen Cyber-Angriffen können auch unbeabsichtigte Ereignisse zu Schäden im Cyber-Raum oder in der physischen Umwelt führen. Solche entstehen aufgrund menschlichen Fehlverhaltens bei der Bereitstellung und Nutzung von IKT oder durch technische Ausfälle, welche wiederum verschiedene Ursachen haben können (z.B. Überalterung der Infrastruktur oder Naturereignisse). Solche Ereignisse unterschiedlicher Grössenordnung kommen häufig vor und gehören zum Alltag der IT-Abteilungen in Unternehmen und Behörden. Entsprechend sind die Auswirkungen dieser Fehler und Ausfälle in der Regel gut beherrschbar. Dennoch haben die Erfahrungen gezeigt, dass hinter vielen grossen Cyber-Vorfällen nicht gezielte Angriffe, sondern eine Verkettung verschiedener Umstände wie menschliches Fehlverhalten oder technisches Versagen, verbunden mit einer unzureichenden Vorbereitung stehen.
Cyber-Risiken aufgrund von menschlichem Fehlverhalten oder technischen Ausfällen werden weiterhin sehr wichtig bleiben. Die zunehmende Komplexität durch die Vernetzung verschiedenster Bereiche macht es zudem schwierig, die Auswirkungen dieser unbeabsichtigten Ereignisse abzuschätzen und einzugrenzen. Eine gute Vorbereitung und vorsorgliche Planung gegenüber solchen Vorfällen bleiben deshalb zentrale Elemente im Umgang mit Cyber-Risiken.

2.2 Stand des Schutzes der Schweiz vor Cyber-Risiken

Basis für die bisherigen Arbeiten war die erste NCS, welche 2012 beschlossen und bis Ende 2017 umgesetzt wurde. Zu beachten ist aber auch der strategische Kontext der NCS. Verschiedene Strategien des Bundes haben einen direkten Einfluss darauf, wie sich die Schweiz vor Cyber-Risiken schützt und setzten so den Rahmen für die weiteren Arbeiten.

2.2.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2012-17

Die erste NCS umfasste 16 Massnahmen, welche dezentral von den jeweils zuständigen Organisationseinheiten in der Bundesverwaltung in Zusammenarbeit mit Verbänden und Be-

treibern kritischer Infrastrukturen umgesetzt worden sind. Im Detail sind die Ergebnisse der NCS im Bericht zur Wirksamkeitsüberprüfung[1] beschreiben. Zur Einschätzung der Ausgangslage für die NCS 2018-22 sind folgende erreichte Ziele der NCS wichtig:

- **Aufbau von Kapazitäten, Fähigkeiten und Wissen:** Ein zentrales Anliegen der NCS war der Aufbau von Kapazitäten, Fähigkeiten und Wissen in den zuständigen Organisationen. 2012 wurde festgestellt, dass in vielen Bereichen die nötigen Ressourcen und das Fachwissen fehlen. Dank der Umsetzung der NCS-Massnahmen hat sich die Situation verbessert.
- **Aufbau von Prozessen, Strukturen und Grundlagen:** Weil Cyber-Risiken viele unterschiedliche Akteure betreffen, war es von grosser Bedeutung, die Zusammenarbeit zwischen den verschiedenen Stellen zu organisieren, die Zuständigkeiten zuzuteilen und Grundlagen zu erarbeiten. Die vorgesehenen Prozesse, Strukturen und Grundlagen sind erstellt und müssen jetzt genutzt und kontinuierlich weiter verbessert werden.
- **Fokus auf den Schutz kritischer Infrastrukturen**: Die Massnahmen der NCS bezogen sich in erster Linie auf den Schutz der kritischen Infrastrukturen. Für die kritischen Teilsektoren wurden Risiko- und Verwundbarkeitsanalysen durchgeführt, Massnahmen identifiziert, die Unterstützung bei Vorfällen ausgebaut und ein Lagebild zu den Cyber-Bedrohungen entwickelt. Diese Arbeiten bildeten den Kern der NCS und können nun vertieft und ausgebaut werden.
- **Stärkung der Zusammenarbeit mit Dritten:** Neben der Verbesserung der Koordination innerhalb der Verwaltung ist auch die Zusammenarbeit mit weiteren Partnern wichtig. Die NCS hat die Zusammenarbeit mit den Kantonen, der Wirtschaft sowie mit verschiedenen internationalen Partnern gestärkt. Durch die Etablierung dieser Kooperationen konnte das gegenseitige Vertrauen gestärkt und der Informationsaustausch gefördert werden. Damit besteht einen gute Basis für eine weitere Vertiefung und Erweiterung der Zusammenarbeit auf allen Ebenen.

2.2.2 Strategischer Kontext

Verschiedene Strategien des Bundes legen Leitlinien fest, die für die Thematik der Cyber-Risiken massgeblich sind. Sie bilden den strategischen Kontext für den Schutz der Schweiz vor Cyber-Risiken. Die dafür grundlegenden Strategien sind:

- **Der Bericht des Bundesrates über die Sicherheitspolitik der Schweiz:** Im sicherheitspolitischen Bericht 2016 definiert der Bundesrat die grundsätzliche strategische Ausrichtung der Sicherheitspolitik der Schweiz. Der Bericht erläutert die grosse und weiter wachsende Bedeutung der Cyber-Bedrohungen für die Sicherheitspolitik und definiert wichtige Begriffe im Zusammenhang der Thematik. Er verweist auf die NCS als Grundlage für den Schutz der Schweiz vor Cyber-Risiken und betont, dass dem Schutz von Informations- und Kommunikationssystemen und -infrastrukturen in der Sicherheitspolitik künftig ein noch grösserer Stellenwert zukommen soll.
- **Strategie des Bundesrates für eine Digitale Schweiz:** Die Strategie zeigt auf, wie die Schweiz die Chancen der Digitalisierung nutzen will. Eines der strategischen Kernziele ist es, Transparenz und Sicherheit zu schaffen, damit die Einwohnerinnen und Einwohner der Schweiz in der Lage sind, ihre informationelle Selbstbestimmung auszuüben. Voraussetzung dafür ist, dass der Staat seiner Aufgabe zum Schutz von Gesellschaft und Wirtschaft auch im digitalen Zeitalter gerecht wird. Zudem legt die Strategie und der dazugehörige Aktionsplan die Ziele und Massnahmen für die Positionierung der Schweiz im internationalen Umfeld zu Fragen der Digitalisierung und den damit einhergehenden Transformationsprozessen fest. Im Bereich der Cyber-Sicherheit soll dies insbesondere durch die Umsetzung der NCS erreicht werden.

[1] https://www.isb.admin.ch/dam/isb/de/dokumente/themen/NCS/NCS-Bericht-Wirksamkeitsueberpruefung-de.pdf.download.pdf/NCS-Bericht-Wirksamkeitsueberpruefung-de.pdf

- **Nationale Strategie zum Schutz kritischer Infrastrukturen:** Die SKI-Strategie definiert den Begriff kritische Infrastrukturen und legt fest, welche Sektoren und Teilsektoren in der Schweiz als kritisch gelten. Sie enthält Massnahmen, die zum Ziel haben, die Resilienz der Schweiz im Hinblick auf kritische Infrastrukturen zu verbessern. Die NCS deckt dabei alle Risiken für kritische Infrastrukturen im Cyber-Bereich ab.

2.3 Handlungsbedarf: notwendige Weiterentwicklung der NCS

Die erreichten Ziele aus der ersten NCS und der strategische Kontext bilden die Grundlage für die weiteren Arbeiten. Der Vergleich zwischen der aktuellen Bedrohungslage und ihrer vermuteten Entwicklung mit dem bestehenden Dispositiv zum Schutz der Schweiz vor Cyber-Risiken zeigt aber deutlich auf, dass eine Beibehaltung des Status quo nicht genügt, um ein ausreichendes Schutzniveau zu gewährleisten. Es besteht Handlungsbedarf auf verschiedenen Ebenen. Einerseits geht es darum, die vorhandenen Kapazitäten und Fähigkeiten weiter auszubauen und die geschaffenen Prozesse, Strukturen und Grundlagen für die Umsetzung von Massnahmen zu nutzen. Andererseits braucht es aber auch strategische Anpassungen. Die NCS soll verstärkt als nationale Strategie über die Bundesverwaltung und die kritischen Infrastrukturen hinaus wirksam sein, um so der Tatsache gerecht zu werden, dass Cyber-Bedrohungen die ganze Wirtschaft, Gesellschaft und Politik betreffen. Dazu müssen die Zielgruppe der NCS entsprechend erweitert und die bisherige Zusammenarbeit gestärkt und verknüpft werden, so dass ein Netzwerk zum Schutz der Schweiz vor Cyber-Risiken entsteht. Schliesslich soll auch die dezentrale Organisationsstruktur mit einer stärkeren strategischen Führung ergänzt werden, damit angesichts der hohen Dynamik der Cyber-Risiken jederzeit auf neue Entwicklungen reagiert werden kann und die NCS in der Öffentlichkeit und der Politik klarer wahrgenommen wird.

Tabelle 1 fasst den Handlungsbedarf zusammen.

Ebene	NCS 2012 - 2017	Handlungsbedarf
Kapazitäten, Fähigkeiten und Wissen	Gesteigerte Kapazitäten und besseres Wissen im Vergleich zu 2012.	Weiterer Ausbau der Kapazitäten und des Wissens ist nötig, um der intensivierten Bedrohungslage gerecht zu werden.
Ziele der NCS-Massnahmen	Schaffung von Prozessen, Strukturen und Grundlagen.	Produktive Nutzung der Prozesse, Strukturen und Grundlagen zur Reduktion der Cyber-Risiken. Die konzipierten Massnahmen und Produkte sind umzusetzen, weiterzuentwickeln und wo nötig zu ergänzen.
Organisationsstruktur	Die Umsetzung erfolgt dezentral durch die jeweils zuständigen Stellen.	Die gestiegene politische, wirtschaftliche und gesellschaftliche Relevanz und die rasche Entwicklung der Cyber-Risiken machen eine stärkere strategische Führung der NCS nötig. Die dezentrale Organisationsstruktur ist dahingehend zu komplementieren.
Zielgruppen	Fokus auf den Schutz kritischer Infrastrukturen vor Cyber-Risiken.	Die Cyber-Bedrohungen betreffen die ganze Schweiz, weshalb die Zielgruppe der NCS erweitert werden muss
Zusammenarbeit	Etablierung der Zusammenarbeit mit Kantonen, Wirtschaft und internationalen Partnern.	Die weiterhin zunehmende Vernetzung stärkt die Bedeutung der Zusammenarbeit auf allen Stufen. Die bestehenden Kooperationen und Public-Private-Partnerships müssen gestärkt und verknüpft werden, so dass ein Netzwerk zum Schutz der Schweiz vor Cyber-Risiken entsteht.

Die zweite NCS soll die Arbeiten der ersten NCS fortführen,diese wo nötig ausweiten und sie mit neuen Massnahmen ergänzen. Sie muss gleichermassen die Kontinuität der Arbeiten aus der ersten NCS gewährleisten und sicherstellen, dass ihre Ziele, Grundsätze, Hand-

lungsfelder und Massnahmen den Entwicklungen seit 2012 gerecht werden und künftige Trends so gut wie möglich antizipieren.

3 Strategische Ausrichtung der NCS 2018-2022

Aus dem identifizierten Handlungsbedarf leitet sich die strategische Ausrichtung der NCS 2018-22 ab. Die Vision und die strategischen Ziele geben vor, was in dieser Zeitspanne erreicht werden soll, die strategischen Grundsätze beschreiben, wie dies geschehen soll und im Abschnitt „Zielgruppen“ wird definiert, an welche Adressaten sich die Strategie richtet.

3.1 Vision und strategische Ziele

Weil Cyber-Risiken verschiedene Bereiche der Wirtschaft, Politik und Gesellschaft gleichzeitig betreffen, sind Massnahmen in unterschiedlichen Bereichen nötig. Damit die Strategie in ihrer Diversität kohärent bleibt, ist es entscheidend, eine gemeinsame Vision zu verfolgen und übergeordnete strategische Ziele zu formulieren.

Vision der NCS 2018-22

«Bei der Nutzung der Chancen der Digitalisierung ist die Schweiz angemessen vor Cyber-Risiken geschützt und ist diesen gegenüber resilient. Die Handlungsfähigkeit und Integrität ihrer Bevölkerung, Wirtschaft und des Staates gegenüber Cyber-Bedrohungen ist gewährleistet.»

Strategische Ziele:

Diese Vision lässt sich dann realisieren, wenn die folgenden sieben strategischen Ziele der NCS 2018-22 erreicht werden:

- Die Schweiz verfügt über die Kompetenzen, das Wissen und die Fähigkeiten, Cyber-Risiken frühzeitig zu erkennen und einzuschätzen.
- Die Schweiz entwickelt wirksame Massnahmen zur Reduktion der Cyber-Risiken und setzt diese im Rahmen der Prävention um.
- Die Schweiz verfügt in allen Lagen über die nötigen Kapazitäten und Organisationsstrukturen, um Cyber-Vorfälle rasch zu erkennen und auch dann zu bewältigen, wenn diese über längere Zeit andauern und verschiedene Bereiche gleichzeitig betreffen.
- Die Schweiz ist gegenüber Cyber-Risiken resilient. Die Fähigkeit der kritischen Infrastrukturen, wichtige Dienstleistungen und Güter zur Verfügung zu stellen, bleibt auch bei grossen Cyber-Vorfällen gewährleistet.
- Der Schutz der Schweiz vor Cyber-Risiken wird als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat wahrgenommen, wobei die Verantwortungen und Zuständigkeiten klar definiert und von allen Beteiligten gelebt werden.
- Die Schweiz engagiert sich für die internationale Kooperation zur Erhöhung der Cyber-Sicherheit. Sie fördert den Dialog in der Cyber-Aussen- und Sicherheitspolitik, beteiligt sich aktiv in den internationalen Fachgremien und pflegt den Austausch mit anderen Staaten und internationalen Organisationen.
- Die Schweiz lernt aus Cyber-Vorfällen im In- und Ausland. Cyber-Vorfälle werden sorgfältig analysiert und aufgrund der Erkenntnisse entsprechende Massnahmen getroffen.

3.2 Grundsätze

Die Vision und die strategischen Ziele geben vor, *was* die NCS 2018-22 erreichen will. Die Grundsätze definieren nun, *wie* dies geschehen soll.

- Die NCS geht von einem **risikobasierten, umfassenden Ansatz** aus, welcher zum Ziel hat, die Resilienz der Schweiz zu verbessern. Dies impliziert die Annahme, dass kein vollständiger Schutz vor Cyber-Risiken möglich ist, die Risiken aber soweit behandelt werden können, dass das Restrisiko tragbar ist. In einem umfassenden Ansatz werden alle relevanten Verwundbarkeiten, Bedrohungen und Gefährdungen berücksichtigt.
- Die Cyber-Sicherheit betrifft nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche. Alle müssen handeln und stehen gemeinsam in der Verantwortung für den Schutz der Schweiz vor Cyber-Risiken. Die NCS bestärkt diese gemeinsame Verantwortung, indem sie die Akteure mit den benötigten Kompetenzen in die Pflicht nimmt und die bestehenden Strukturen nutzt. Daraus ergibt sich eine **dezentrale Struktur zu ihrer Umsetzung**, welche aber zentral durch die strategische Führung der NCS gesteuert wird und eine klare Aufgaben und Rollenverteilung ausweist.
- Der NCS liegt ein Verständnis einer **subsidiären Rolle des Staates** zugrunde, was bedeutet, dass der Staat erst dann eingreift, wenn das Wohlergehen unserer Gesellschaft wesentlich betroffen ist und private Akteure nicht in der Lage oder nicht willens sind, das Problem selbständig zu lösen. Der Staat kann in diesem Fall unterstützend wirken, Anreize setzen oder regulativ eingreifen.
- Die NCS verfolgt einen kooperativen Ansatz. Sie stärkt und koordiniert auf nationaler Ebene die bestehende **Public-Private Partnership**, fördert weitere öffentlich-private Kooperationen und baut die Zusammenarbeit zwischen Bund, Kantonen und Gemeinden aus.
- Die NCS fördert auf der internationalen Ebene die **Zusammenarbeit mit internationalen Partnern**.
- Die Umsetzung der NCS erfolgt transparent, soweit dies nicht zu einer Beeinträchtigung der Wirkung der Massnahmen führt. Erreicht wird dies über **eine aktive Kommunikation zur NCS** gegenüber Gesellschaft, Wirtschaft und Politik.

3.3 Zielgruppen

Als vom Bundesrat beschlossene Strategie für die Schweiz definiert die NCS Massnahmen, welche primär von den Organisationseinheiten der Bundesverwaltung in Zusammenarbeit mit Behörden, Verbänden und Unternehmen umzusetzen sind. Die beabsichtigte Wirkung der NCS betrifft jedoch die ganze Schweiz. Explizit adressiert die NCS folgende Zielgruppen:

- **Kritische Infrastrukturen:** Hauptzielgruppe der NCS sind die Betreiber kritischer Infrastrukturen. Sie stellen die Verfügbarkeit von essenziellen Gütern und Dienstleistungen sicher. Deshalb ist ihr Funktionieren unabdingbar für die Bevölkerung und die Wirtschaft der Schweiz. Ihr Schutz hat oberste Priorität und steht bei allen Massnahmen der NCS im Fokus.
- **Behörden:** Zu den kritischen Infrastrukturen zählen auch die Dienstleistungen der Verwaltungen und Behörden. Für deren Schutz stehen Bund, Kantone und Gemeinden direkt in der Verantwortung.
- **Bevölkerung:** Der Schutz der Bevölkerung ist letztendlich Zweck aller Massnahmen der NCS (beispielsweise der Schutz vor Ausfällen kritischer Infrastrukturen). Er steht aber insbesondere im Zusammenhang mit Cyber-Kriminalität im Fokus. Darüber hinaus trägt die NCS durch transparente Information dazu bei, der Bevölkerung einen sicheren, informierten und vertrauensvollen Umgang mit IKT zu ermöglichen.

- **Wirtschaft:** Für die Wirtschaft ist ein sicheres und vertrauenswürdiges Umfeld eine wichtige Grundlage und ein Standortfaktor. Cyber-Risiken stellen nicht nur kritische Infrastrukturen, sondern auch alle übrigen Unternehmen und vor allem auch die KMUs vor grosse Herausforderungen. Die NCS schafft möglichst sichere Bedingungen für die Unternehmen der Schweiz und stellt ihnen subsidiär zu den Angeboten des Marktes gezielte Unterstützung beim Umgang mit Cyber-Risiken zur Verfügung.

4 Handlungsfelder und Massnahmen der NCS 2018-2022

Um die strategischen Ziele zu erreichen, müssen Massnahmen in sehr unterschiedlichen Bereichen umgesetzt werden. Die NCS unterscheidet zehn Handlungsfelder, welche verschiedene Teilaspekte der Cyber-Risiken adressieren. In diesen Handlungsfeldern werden insgesamt 30 Massnahmen formuliert.

Tabelle 2 listet die Handlungsfelder und Massnahmen der NCS 2018-2022 auf:

Handlungsfeld	Massnahmen
Kompetenzen- und Wissensaufbau	1. Früherkennung von Trends und Technologien und Wissensaufbau 2. Ausbau und Förderung von Forschungs- und Bildungskompetenz 3. Schaffung von günstigen Rahmenbedingungen für eine innovative IT-Sicherheitswirtschaft in der Schweiz
Bedrohungslage	4. Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage
Resilienz-Management	5. Verbesserung der IKT-Resilienz der kritischen Infrastrukturen 6. Stärkung der IKT-Resilienz in der Bundesverwaltung 7. Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen
Standardisierung / Regulierung	8. Evaluierung und Einführung von Minimalstandards 9. Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung 10. Globale Internet-Gouvernanz 11. Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit
Vorfallbewältigung	12. Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen 13. Aufbau von Dienstleistungen für alle Unternehmen 14. Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren
Krisenmanagement	15. Integration von MELANI in die Krisenstäbe des Bundes 16. Gemeinsame Übungen zum Krisenmanagement 17. Vorbereitung der Krisenkommunikation
Strafverfolgung	18. Lagebild Cyber-Kriminalität 19. Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung 20. Ausbildung 21. Zentralstelle Cyber-Kriminalität
Cyber-Abwehr	22. Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG 23. Aufbau von Kapazitäten zur Schaffung und zum Erhalt von Abwehrmassnahmen im Cyber-Raum
Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik	24. Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik 25. Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit 26. Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik
Aussenwirkung und Sensibilisierung	27. Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS 28. Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)

Diese Handlungsfelder und Massnahmen werden im Folgenden ausführlicher beschrieben.

4.1 Kompetenzen- und Wissensaufbau

Übersicht Handlungsfeld	
Beschreibung	Die möglichst frühe Erkennung und die richtige Einschätzung von Cyber-Risiken sind Voraussetzung dafür, dass diese Risiken gemindert werden können. Damit dies den Akteuren aus Wirtschaft, Gesellschaft und Behörden gelingt, sind einerseits Grundkompetenzen und andererseits Fachwissen und spezifische Kompetenzen notwendig. Die Faktoren müssen durch die bestehenden Bildungs- und Forschungsinstitutionen bereichsübergreifend aufgebaut, vermittelt und weiterentwickelt werden. Besonders herausfordernd sind in diesem Zusammenhang die Vielfältigkeit und die hohe Dynamik von Cyber-Risiken.
Ausgangslage	Die Schweiz verfügt über ein leistungsfähiges Netzwerk an Ausbildungs- und Forschungsinstitutionen auf den verschiedenen Stufen. Durch die rasche Entwicklung der Cyber-Risiken ist der Bedarf an entsprechenden Kompetenzen und Wissen stark gestiegen. Es fehlt heute an spezifischem Wissen und an Fachkräften in den verschiedenen Bereichen, welche für Cyber-Risiken relevant sind. Dies erschwert den Schutz vor Cyber-Risiken und schränkt die Möglichkeiten der Wirtschaft ein, sich auf dem wachsenden Markt der IT-Sicherheit zu positionieren. Generell bleibt es eine grosse Herausforderung, die wichtigen Trends und Technologien frühzeitig zu erkennen. Bisher findet keine systematische und koordinierte Erfassung dieser Trends und Technologien unter Einbezug internationaler Aspekte statt.
Ziele und Handlungsbedarf	Der Bildungs- und Forschungsplatz Schweiz soll dem Thema Bereich Cyber-Risiken in angemessenem Masse Gewicht beimessen und Gesellschaft, Wirtschaft und Behörden mit den notwendigen Kompetenzen und Forschungserkenntnissen versorgen. Neue Trends und Technologien im Bereich der Cyber-Sicherheit müssen frühzeitig erkannt werden, um so auf diese Risiken vorbereitet zu sein und entsprechende Handlungen schnellstmöglich einleiten zu können. Die Wirtschaft muss über genügend Know-how und Fachkräfte verfügen, um kompetent mit Cyber-Risiken umgehen und die Chancen des aufkommenden IT-Sicherheitsmarktes nutzen zu können. IT-Sicherheitslösungen sollen vermehrt in der Schweiz hergestellt werden. Dazu soll in Zusammenarbeit zwischen Wirtschaft, Forschung und Staat ein Umfeld („Ökosystem“) geschaffen werden, das die Entstehung, Produktion und Vertrieb von innovativen Lösungen im Bereich IT-Sicherheit fördert. Die Grundlage für die Erreichung dieser Ziele wird durch Forschung im Bereich der Cyber-Sicherheit geschaffen. Die Forschung soll in diesem interdisziplinären Bereich deshalb bestmöglich koordiniert werden.

Massnahmen
1) Früherkennung von Trends und Technologien und Wissensaufbau Neue Angriffsstrategien und -muster, Trends sowie Technologien sind in regelmässigen Abständen und frühzeitig zu identifizieren. Sich daraus ergebende Chancen sollen erkannt und Risiken abgeschätzt werden. Grundlagenforschung zu den eruierten Trends und Technologien werden im Rahmen der bestehenden Gefässe und Prozesse gefördert (z.B. NFP, Innovations- und Start-up-Förderung, BRIDGE, Nationale thematische Netzwerke NTN, EU-Forschungsrahmenprogramme)

2) Ausbau und Förderung der Kompetenzbildung Es wird im Austausch zwischen Wirtschaft, den Hochschulen, Bund und Kantonen laufend analysiert, welche Lücken in Bezug auf die Kompetenzbildung zu Cyber-Risiken bestehen. Dabei wird insbesondere überprüft, wie das Thema Cyber-Risiken verstärkt in bestehende Ausbildungsgänge integriert werden kann. Die zuständigen Akteure werden vom Bund im Rahmen der bestehenden Instrumente und Prozesse bei der Schliessung der Angebotslücken unterstützt.
3) Schaffung von günstigen Rahmenbedingungen für eine innovative IT-Sicherheitswirtschaft in der Schweiz Die Schweiz soll ein attraktiver Standort für Unternehmen im Bereich der IT-Sicherheit sein. Ein verstärkter Austausch zwischen Wirtschaft und Forschung soll dazu beitragen, innovative Start-ups in diesem Bereich zu fördern. Zu diesem Zweck wird ebenfalls auf die in Massnahme 1 erwähnten bestehenden Gefässe der Innovationsförderung zurückgegriffen. In Zusammenarbeit mit den Verbänden und den Hochschulen werden bei Bedarf weitere Fördermassnahmen geprüft und umgesetzt.

4.2 Bedrohungslage

Übersicht Handlungsfeld	
Beschreibung	Wie im Kapitel zur Ausgangslage beschrieben, ist die Cyber-Bedrohungslage durch eine Vielzahl von möglichen Bedrohungen geprägt. Diese unterscheiden sich hinsichtlich des Zwecks eines Angriffs, der Akteure, welche hinter den Angriffen stehen und des Kreises der Betroffenen. Die Grenzen zwischen den verschiedenen Bedrohungen sind dabei oft nicht klar zu ziehen, da Angreifer verschiedene Zwecke gleichzeitig verfolgen können und auch die Art und Ziele des Angriffs kombinieren können. Zusammen mit der hohen Dynamik, mit welcher sich Cyber-Risiken entwickeln, machen es diese Komplexität und Diffusität zu einer Herausforderung, sich einen umfassenden Überblick zur Cyber-Bedrohungslage zu verschaffen. Ein solcher Überblick ist aber ein zentrales Element zum Schutz vor Cyber-Risiken. Er ist die Grundlage für die Wahl und Priorisierung von präventiven und reaktiven Massnahmen und unabdingbar, um bei Vorfällen und in Krisenlagen die richtigen Entscheidungen zu treffen. Benötigt werden dazu eine Einschätzung der vorhandenen Bedrohungen und ihrer künftigen Entwicklungen (Lagebeschreibung und -beurteilung).
Ausgangslage	Im Rahmen der Umsetzung der NCS von 2013-2017 wurden die Fähigkeiten in der Lagebeschreibung und -beurteilung, der Früherkennung und der Attribution aufgebaut. Die nötigen Prozesse zur Erstellung eines gesamtheitlichen Lagebilds sind etabliert und die Informationen zur Bedrohungslage werden mit Hilfe eines dynamischen, interaktiven Lageradars zusammengefasst und dargestellt und via MELANI den Behörden und Betreibern kritischer Infrastrukturen zur Verfügung gestellt. Der Nachrichtendienst verfügt über Spezialwissen und Fähigkeiten zur punktuellen Beschaffung, Einschätzung und Verifikation von Informationen und zur Identifikation der Urheberschaft von Cyber-Angriffen. Das Nachrichtendienstgesetz erlaubt es seit dem 1. September 2017, zusätzliche Beschaffungsmittel einzusetzen.

Ziele und Handlungsbedarf	Zum Schutz der Schweiz vor Cyber-Risiken bleibt die Schweiz darauf angewiesen, über ein gesamtheitliches Cyber-Lagebild zu verfügen, für die Schweiz relevante Fallkomplexe zu identifizieren, Cyber-Angriffe frühzeitig zu erkennen und die Täterschaft identifizieren zu können. Die bereits vorhandenen Fähigkeiten müssen angesichts der intensivierten Bedrohungslage ausgebaut und der Informationsaustausch mit der Wirtschaft und den Kantonen weiter gestärkt werden. Eine nachhaltige Aufarbeitung und Verfolgung von Cyberangriffen ist derzeit nicht gewährleistet, da die vorhandenen Ressourcen stark vom Tagesgeschäft absorbiert werden. Bei der Einschätzung von relevanten Bedrohungen für die Schweiz soll eine grössere Tiefe und Körnigkeit erreicht werden. Erkenntnisse über die Bedrohungslage sollen zudem nicht mehr nur den Behörden und Betreibern kritischer Infrastrukturen zur Verfügung gestellt, sondern in geeigneter Form auch weiteren Schweizer Unternehmen und der Bevölkerung zugänglich gemacht werden.

Massnahmen

4) Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage

Die Fähigkeiten zur Beschaffung, Einschätzung und Verifikation von Informationen zur Bedrohungslage im Nachrichtendienst sind weiter auszubauen. Dazu braucht es eine systematische Nutzung von *Open Source Intelligence (OSINT)* und den damit verbundenen Fachkenntnissen, die Nutzung technischer Hilfsmittel sowie die Pflege und der Ausbau des Netzwerkes an nationalen und internationalen Partnern. Die gewonnenen Erkenntnisse zur Bedrohungslage sind systematisch aufzuarbeiten, regelmässig zu aktualisieren und über den Lageradar zielgruppengerecht darzustellen. Es soll auch eine Version des Lageradars für die Öffentlichkeit erstellt werden.

4.3 Resilienzmanagement

Übersicht Handlungsfeld	
Beschreibung	Kritische Infrastrukturen sind stark von funktionierenden und sicheren Informations- und Kommunikationsinfrastrukturen abhängig. Massnahmen zur Reduktion der IKT-Verwundbarkeiten sind deshalb von grosser Bedeutung für den Schutz der Schweiz vor Cyber-Risiken. Sie beziehen sich nicht nur auf eine Stärkung der Abwehr, sondern schliessen Massnahmen zur Eindämmung von Schäden und zur Verringerung der Ausfallszeit bei Vorfällen ein. Ziel ist die Verbesserung der Resilienz (Widerstands- und Regenerationsfähigkeit) der kritischen Infrastrukturen in der Schweiz. Ein grosser Teil der kritischen Infrastrukturen wird in der Schweiz von privaten Unternehmen betrieben. Die Umsetzung der Massnahmen zur Verbesserung der IKT-Resilienz erfolgt durch diese Unternehmen. Trotzdem trägt der Staat eine verfassungsmässige Verantwortung, kritische Infrastrukturen zu schützen und damit die Verfügbarkeit der für Bevölkerung und Wirtschaft lebenswichtigen Güter und Dienstleistungen zu gewährleisten. Diese Aufgabe hat er subsidiär und in enger Zusammenarbeit mit der Wirtschaft umzusetzen. Aus diesem Grund übernimmt der Bund eine aktive Rolle bei der Definition von Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren und überwacht auch deren Umsetzung. Je nach Massnahme kann deren Umsetzung auf verschiedenen Ebenen erfolgen - beispielsweise auf den Stufen Unternehmen oder Branche. Einen Sonderfall bilden die kritischen IKT-Infrastrukturen der Behörden selber. Hier sind Bund und Kantone selber zuständig für die Umsetzung der Massnahmen.
Ausgangslage	Zwischen 2013 und 2017 haben das BABS und das BWL in Zusammenarbeit mit den zuständigen Behörden, Verbänden und Vertretern von KI-Betreibern die IKT-Risiken und -Verwundbarkeiten in 28 kritischen Teilsektoren identifiziert und gemeinsam Massnahmenvorschläge zur Verbesserung der IKT-Resilienz ausgearbeitet (und teilweise bereits umgesetzt). Zum Schutz der eigenen IKT-Infrastruktur hat der Bund ein Konzept erarbeitet, mit welchem er eine regelmässige Analyse der Verwundbarkeiten der IKT-Systeme in der Bundesverwaltung sicherstellt. Die Kantone haben im Rahmen von zwei Projekten des SVS für ihre Verwaltungen Risikoanalysen durchgeführt.
Ziele und Handlungsbedarf	Die identifizierten Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren und in den Verwaltungen sollen umgesetzt und basierend auf periodisch zu aktualisierenden Risiko- und Verwundbarkeitsanalysen weiterentwickelt werden. Dies erfolgt in Abstimmung mit den Massnahmen des Handlungsfelds Standardisierung und Regulierung und unter Nutzung von Synergieeffekten zu den laufenden Arbeiten des Bundes im Bereich Schutz kritischer Infrastrukturen, der wirtschaftlichen Landesversorgung, des Risikomanagements Bund, IKT-Sicherheit sowie weiterer involvierten Stellen.

Massnahmen
5) Verbesserung der IKT-Resilienz der kritischen Infrastrukturen Im Fokus steht die Umsetzung von Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Teilsektoren unter Einbezug der relevanten Regulierungsbehörden und Fachämter. Grundlagen dafür sind die bestehenden Risiko- und Verwundbarkeitsanalysen und die daraus abgeleiteten Massnahmenvorschläge aus der NCS 2012-17. Neben der Umsetzung der identifizierten Massnahmen müssen die bestehenden Analysen und die Massnahmen regelmässig aktualisiert und wo nötig an neue Erkenntnisse und Entwicklungen angepasst werden.
6) Stärkung der IKT-Resilienz in der Bundesverwaltung Die Stärkung der Resilienz der IKT in der Bundesverwaltung erfolgt über die Umsetzung des vorhandenen Konzepts zur Analyse und zum Umgang mit IKT-Verwundbarkeiten in der Bundesverwaltung. Das Konzept sieht vor, aus den identifizierten Verwundbarkeiten direkt auf eine Selektion von sinnvollerweise umzusetzenden IKT-Sicherheitsmassnahmen zu schliessen.
7) Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen Es wird ein Behördennetzwerk geschaffen (oder bestehende Netzwerke genutzt) um Erfahrungen auszutauschen und gemeinsame Grundlagen für die Stärkung der IKT-Resilienz in den Kantonen zu schaffen. Ziel ist die gegenseitige Unterstützung und ein koordiniertes Vorgehen der Behörden aus Bund und Kantonen.

4.4 Standardisierung / Regulierung

Übersicht Handlungsfeld	
Beschreibung	IKT-Standardisierungen und -Regulierungen sind wichtige Instrumente zum Schutz vor Cyber-Risiken. Indem sie Minimalanforderungen bezüglich der zu treffenden Schutzvorkehrungen formulieren, stärken sie die Prävention und durch Vorgaben zu Massnahmen bei Cyber-Vorfällen (z.B. über Vorgaben zur Meldepflicht) tragen sie zu einer verbesserten und nachhaltigen Reaktion bei. Standardisierung und Regulierung sind auch im internationalen Umfeld wichtig, da sie wesentlich zur Sicherheit und Vertrauen in der globalisierten digitalen Gesellschaft und Wirtschaft beitragen. Bei der Einführung von Standardisierungen und Regulierungen gilt es aber, die grossen Unterschiede zwischen den Wirtschaftssektoren und Unternehmen verschiedener Grösse zu beachten. Die Branchen sind unterschiedlich stark exponiert gegenüber Cyber-Risiken und die finanziellen und personellen Möglichkeiten von Unternehmen divergieren stark. Standardisierungen und Regulierungen sind deshalb in enger Zusammenarbeit zwischen Privatwirtschaft und Staat zu entwickeln und einzuführen. Zudem ist in der Standardisierung und Regulierung das internationale Umfeld von grosser Bedeutung. Der Cyber-Raum ist grenzüberschreitend, und entsprechend müssen Standards international und Regulierungen möglichst kompatibel sein. Die Arbeiten der internationalen Standardisierungsgremien und die regulatorische Entwicklung im Umfeld der Schweiz sind darum massgebend. Zum Themenbereich der Standardisierung und Regulierung gehören auch die verschiedenen Prozesse zur Internet-Gouvernanz, welche durch den UNO-Weltgipfel zur Informationsgesellschaft (WSIS) geschaffen wurde. Diese befassen sich mit der Entwicklung von Prinzipien, Normen, Regeln und Entscheidungsmechanismen zur Entwicklung und Nutzung des Internets auf internationaler Ebene. Bei der Umsetzung der WSIS-Aktionslinie C5 (Sicherheit und Vertrauen) nimmt die ITU die Rolle des Moderators verschiedener Projekte und Arbeitsstränge ein. Zudem haben weitere internationale Akteure, wie z.B. die OECD oder das WEF, Prozesse und Aktivitäten lanciert, die sich um eine Stärkung der Sicherheit im Digitalen Bereich bemühen. Das zentrale Anliegen des WSIS zum Einbezug aller Interessengruppen (Multistakeholder-Ansatz) trägt der Entwicklung Rechnung, dass Normen und Regeln in der digitalen Welt in zunehmendem Masse von privaten globalen Akteuren bestimmt werden und deshalb eine Kooperation zwischen staatlichen und privaten Akteuren von grundlegender Bedeutung ist.
Ausgangslage	Es bestehen verschiedene sektorielle und einige generelle Standards zur Cyber-Sicherheit. In Zusammenarbeit mit der Wirtschaft wurde eine erste Bestandsaufnahme zum Standardisierungs- und Regulierungsbedarf in den verschiedenen Sektoren gemacht. Die Entwicklungen in den internationalen Standardisierungsgremien und im Bereich der Regulierung in anderen Ländern sind bekannt. Auf europäischer Ebene ist die Netzwerk- und Informationssicherheitsrichtlinie der EU (NIS-Richtlinie) beschlossen worden, welche nun von den Mitgliedstaaten umgesetzt wird. Diese sieht die Einführung von Minimalstandards und einer Meldepflicht zu Cyber-Vorfällen vor. Im Bereich der Internet-Gouvernanz sind die für die Schweiz prioritären Gremien, Prozesse und Veranstaltungen identifiziert, die Zuständigkeiten innerhalb des Bundes geklärt und die Koordination mit allen beteiligten Akteuren dank den durch die NCS etablierten Prozesse sichergestellt

Ziele und Handlungsbedarf	Der gestiegenen Bedeutung von IKT-Standardisierungen und -Regulierungen ist Rechnung zu tragen. Verbindliche und überprüfbare IKT-Minimalstandards sind relevant für Sicherheit und Vertrauen in der digitalen Wirtschaft und Gesellschaft und sollen in Zusammenarbeit mit der Privatwirtschaft evaluiert und wo sinnvoll eingeführt werden. Ebenfalls zu prüfen ist, ob und wie eine Meldepflicht für Cyber-Vorfälle eingeführt werden soll. Der internationale Kontext wird bei den Massnahmen berücksichtigt und beeinflusst diese wesentlich, weshalb die Entwicklungen weiterhin verfolgt werden müssen. Die Schweiz bringt deshalb ihre Interessen und Werte in den wichtigsten Prozessen ein.

Massnahmen

8) Entwicklung und Einführung von Minimalstandards

Auf der Basis der durchgeführten Risiko- und Verwundbarkeitsanalysen werden in enger Zusammenarbeit zwischen den Fachbehörden, der Privatwirtschaft und den Verbänden überprüfbare IKT-Minimalstandards evaluiert und eingeführt. Wo vorhanden, werden bestehende Standards verwendet und allenfalls adaptiert. Die zuständigen Behörden prüfen, für welche Organisationen und Tätigkeiten die Standards verbindlich sein sollen. Dabei wird auf den Ergebnissen aus den Verwundbarkeitsanalysen aufgebaut.

9) Prüfung Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung

Zur Verbesserung des Lagebilds zu Cyber-Bedrohungen ist die Einführung einer Meldepflicht für Cyber-Vorfälle zu prüfen und über ihre Einführung zu befinden. Dabei sind zunächst die Fragen zu klären, für wen eine Meldepflicht gelten soll, welche Vorfälle sie betrifft und an wen gemeldet werden müssen und ob eine Meldepflicht im Vergleich zu heute das Lagebild substanziell verbessern kann. Es werden Varianten für die Umsetzung von Meldepflichten in den verschiedenen Sektoren erarbeitet und aufgezeigt, welche gesetzlichen Grundlagen dafür nötig sind. Dies erfolgt unter Einbezug der jeweils zuständigen Behörden, der Privatwirtschaft und der Verbände, in Koordination mit der nationalen Strategie zum Schutz kritischer Infrastrukturen und unter Berücksichtigung der internationalen Entwicklungen. Auf der Basis dieser Abklärungen wird anschliessend über die Einführung einer Meldepflicht entschieden.

10) Globale Internet-Gouvernanz

Die Schweiz soll sich aktiv und koordiniert für ein internationales Regelwerk zur Nutzung und Weiterentwicklung des Internets einsetzen, welches mit den Schweizer Vorstellungen von Freiheit, Demokratie und (Eigen-)Verantwortung, Grundversorgung, Chancengleichheit, Sicherheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist. Diesbezüglich sind die nationalen Interessenträger miteinzubeziehen und ihnen gegenüber die relevanten Entwicklungen aufzuzeigen.

11) Aufbau von Expertise zu Fragen der Standardisierung in Bezug zur Cyber-Sicherheit

Der Bund baut einen Expertenpool zu Fragen der Standardisierung im Bereich Cyber-Sicherheit auf. Der Expertenpool berät die Regulatoren bei der Entwicklung und Umsetzung von themenbezogenen Standards, Regularien oder Leitlinien. Er unterstützt bei Bedarf die Kantone, beobachtet die internationale Entwicklung im Bereich Standardisierung und Regulierung und tauscht sich diesbezüglich mit der Wirtschaft aus. Er trägt so zu einem koordinierten und auf die internationalen Entwicklungen abgestimmten Vorgehen bei.

4.5 Vorfallbewältigung

Übersicht Handlungsfeld	
Beschreibung	Da es keinen vollständigen Schutz gegen Cyber-Vorfälle gibt und mit einer zunehmenden Anzahl gezielter Angriffe zu rechnen ist, welche nicht mit verhältnismässigem Aufwand präventiv zu verhindern sind, ist der Aufbau und Betrieb einer Organisation zur Bewältigung von Vorfällen (Incident-Management) ein Kernelement im Umgang mit Cyber-Risiken. Zur Vorfallbewältigung gehört es, diese so früh wie möglich zu erkennen, die richtigen Gegenmassnahmen zu identifizieren und umzusetzen sowie die Vorfälle zu analysieren und daraus Erkenntnisse für die Verbesserung der Prävention abzuleiten. Um diese Aufgaben wahrzunehmen, braucht es Fachkompetenzen, Analyseinstrumente, eine gut funktionierende Organisation und eine intensive Zusammenarbeit zwischen allen relevanten Stellen. Entscheidend ist der Informationsaustausch zwischen vertrauenswürdigen Partnern über Vorfälle und mögliche Gegenmassnahmen, da Vorfälle oft verschiedene Stellen gleichzeitig betreffen und deshalb schneller und effektiver bewältigt werden können, wenn alle betroffenen Stellen relevante Informationen austauschen.
Ausgangslage	Für die Bewältigung von Cyber-Vorfällen haben viele Organisationen in der Schweiz spezialisierte Teams aufgebaut oder beauftragt. Diese Teams haben unterschiedliche Bezeichnungen (z.B. Security Operations Centers, Computer Emergency Response Teams, Computer Security Incident Response Teams) und jeweils auf den Aufgabenbereich ausgerichteten Kompetenzen. Auch viele Kantone und der Bund verfügen über solche Teams. Die Vorfallbewältigung erfolgt in erster Linie über diese Einheiten. Der Bund betreibt zusätzlich zur Unterstützung der Betreiber kritischer Infrastrukturen die Melde- und Analysestelle Informationssicherung (MELANI). MELANI funktioniert als Anlaufstelle auf staatlicher Ebene und bietet Unterstützung bei der technischen und nachrichtendienstlichen Analyse der Vorfälle, inklusive der dazugehörenden Informationsaustauschplattform. Im Rahmen der NCS 2012-2017 konnten die personellen Kapazitäten von MELANI gestärkt werden, und die Zusammenarbeit mit den spezialisierten Teams inner- und ausserhalb der Bundesverwaltung wurde weiter ausgebaut. Dies ermöglichte es, den Kreis der Firmen mit Zugang zur Plattform für den Informationsaustausch und zur technischen Unterstützung zu vergrössern. Die Dienstleistungen von MELANI bleiben aber auch nach diesem Ausbau fokussiert auf die Betreiber kritischer Infrastrukturen.
Ziele und Handlungsbedarf	Mit der Erweiterung der Zielgruppe der NCS muss auch die Unterstützung bei Vorfällen auf weitere Kreise ausgeweitet werden. Die bisherige Qualität der Unterstützung bei der Erkennung, Bewältigung und Analyse von Vorfällen muss dabei beibehalten werden und der vertrauensvolle Informationsaustausch mit Betreibern kritischer Infrastrukturen weiterhin gewährleistet sein. Die heute schon enge Zusammenarbeit mit den relevanten Kompetenzzentren ist gezielt zu intensivieren, um die beschränkten spezialisierten Ressourcen in der Schweiz möglichst effektiv und effizient zu nutzen.

Massnahmen

12) Ausbau von MELANI als Public-Private-Partnership für Betreiber kritischer Infrastrukturen Die Unterstützung von Betreibern kritischer Infrastrukturen soll weiter ausgebaut werden. Ziel ist, dass alle kritischen Sektoren in den Informationsaustausch eingebunden sind und dieser verstärkt auch sektorübergreifend gepflegt wird. Beim Ausbau des PPP muss sichergestellt sein, dass die Qualität der bisherigen Dienstleistungen erhalten bleibt. Es muss klar definiert werden, welche Mitglieder des geschlossenen Kundenkreises Anspruch auf welche Dienstleistungen haben.
13) Aufbau von Dienstleistungen für alle Unternehmen MELANI erweitert die Zielgruppe und entwickelt Dienstleistungen im Bereich Prävention und Vorfallbewältigung für eine breitere Zielgruppe, welche sich nicht nur auf Betreiber kritischer Infrastrukturen beschränkt. Die Schweizer Wirtschaft und insbesondere kleine und-mittlere Unternehmen sollen durch MELANI unterstützt werden. Die Unterstützung erfolgt subsidiär zu den Angeboten im Bereich Schutz und Vorfallbewältigung, welche auf dem Markt verfügbar sind.
14) Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren Die heute schon enge Zusammenarbeit Abstimmung von MELANI mit weiteren relevanten Stellen in Bund und Kantonen ist weiter zu verstärken. Aufgrund der limitierten Anzahl an verfügbaren Spezialisten in der Schweiz ist die Zusammenarbeit mit ausgewählten Kompetenzzentren gezielt zu intensivieren und besser zu koordinieren, um die beschränkten Ressourcen möglichst effektiv und effizient zu nutzen.

4.6 Krisenmanagement

Übersicht Handlungsfeld	
Beschreibung	Cyber-Vorfälle können gravierende Konsequenzen haben und einzeln oder in Kombination soweit eskalieren, dass ein Krisenmanagement auf nationaler Ebene nötig wird. Entscheidend für die Bewältigung von Krisen sind ein aktuelles, einheitliches und umfassendes Lagebild, die Definition von effizienten Prozessen zur Entscheidungsfindung und die Festlegung einer Kommunikationsstrategie. Das Krisenmanagement ist grundsätzlich szenariounabhängig. Das bedeutet, dass das allgemeine Krisenmanagement (Führungsabläufe und -prozesse) der Kantone und des Bundes auch für Krisen mit Cyber-Ausprägungen gültig bleibt. Wichtig bei solchen Krisen ist aber die Unterstützung der Stäbe durch fachspezifisches Wissen und eine intensive Zusammenarbeit aller kompetenten Stellen aus Bund, Kantonen und Wirtschaft. Nur so ist es möglich, dass alle relevanten Informationen zur Bewältigung der Krise rechtzeitig und in verständlicher Form zur Verfügung stehen. Weil bei der Bewältigung von Krisen keine Zeit verloren gehen darf, müssen die Prozesse im Vornherein geübt und Konzepte zur Führung und Kommunikation ausgearbeitet werden.
Ausgangslage	Für die Bewältigung von Krisen mit Bezug zu Cyber-Risiken wurde gestützt auf die Ergebnisse der Strategischen Führungsübung 2013 ein Konzept des Bundes für das Management von Krisen mit Cyber-Ausprägungen erstellt und in Zusammenarbeit mit den Kantonen und Vertretern der Wirtschaft zu einem Konzept für das nationale Krisenmanagement in diesem Bereich erweitert. Das Konzept wurde getestet und die Übungen ausgewertet. Als entscheidendes Element und wichtigste Herausforderung bei der Bewältigung von Krisen mit Cyber-Ausprägungen wird die Verfügbarkeit eines möglichst präzisen und aktuellen Lagebilds bewertet.

Ziele und Handlungsbedarf	Die Übungen haben gezeigt, dass die Fähigkeiten zur Koordination auf operativer Ebene und zur Beschreibung der Lage ausgebaut werden müssen. MELANI soll als Informationsdrehscheibe funktionieren und als Fachorgan für Cyber-Aspekte in bestehende oder ad-hoc eingesetzte Stäbe integriert werden. Die Zusammenarbeit mit den Kantonen und der Wirtschaft muss zudem weiterhin geübt werden.

Massnahmen
15) Integration von MELANI in die Krisenstäbe des Bundes Für die Bewältigung von Cyber-Krisen werden die bestehenden Krisenstäbe (Bundesstab ABCN und BWL-Krisenstab) genutzt oder ad-hoc Krisenstäbe gebildet. MELANI ist als Fachorganisationen in die Stäbe zu integrieren und muss über die Fähigkeiten verfügen, bei einer Krise mit Cyber-Aspekten die fachliche Koordination zu übernehmen und Empfehlungen zuhanden des Krisenstabes abzugeben. Dabei ist auch zu klären, welche Weisungsbefugnisse im Fall einer Krise auf Stufe Fachorganisation nötig sind.
16) Gemeinsame Übungen zum Krisenmanagement In gemeinsamen Übungen von Bund, Kantonen und Vertretern kritischer Infrastrukturen wird das Krisenmanagement in Bezug auf die Cyber-Aspekte getestet. Dabei sind sowohl Cyber-Aspekte in generelle Übungen einzubeziehen, als auch spezifische Übungen zur Bewältigung von Krisen mit Cyber-Ausprägungen durchzuführen.Die Übungen werden ausgewertet und fliessen in die Optimierung der Führungsabläufe und -prozesse ein.

4.7 Strafverfolgung

Übersicht Handlungsfeld	
Beschreibung	Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftätern neuartige Tatmuster mit enormem Schadenspotenzial für Gesellschaft und Wirtschaft. Zeit und Raum erlangen eine neue Bedeutung, klassische Rechtsbegriffe wie Tatort, Tatzeit und örtliche Zuständigkeiten ebenfalls. Cyber-Kriminalität überschreitet territoriale Grenzen, und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Je stärker die digitale Vernetzung ist, desto grösser wird die Gefahr, dass Cyber-Vorfälle zwar in der virtuellen Welt beginnen, aber ihre schädigende Wirkung in der realen Welt entfalten. Vor dem Hintergrund dieser Entwicklung ist es dringend angezeigt, auch in der Strafverfolgung nach neuen Lösungsansätzen zu suchen. Es gilt gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern die Interoperabilität und Reaktionsfähigkeit zu verbessern, die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben.

Ausgangslage	Im Rahmen der NCS wurden in Zusammenarbeit mit den Kantonen zwischen 2012-17 nachstehende Ziele erreicht: - ein konsolidiertes Konzept «Fallübersicht und Koordination interkantonaler Fallkomplexe» wurde erstellt; - Massnahmen zur einheitlichen Erfassung, Koordination und Verbreitung von Lageinformationen wurden definiert; - polizeiliche Massnahmen zur Bestimmung der örtlichen und sachlichen Zuständigkeit wurden definiert; - eine phänomenbezogene Erfassung und Analyse der Cyber-Kriminalität wurde eingeführt. Testbetrieb mit vier kantonalen Polizeikorps und der BKP seit Ende 2016). Das gesamtschweizerische Lagebild und die interkantonale Fallkoordination sind lediglich zwei Teilaspekte der Herausforderung Cyber-Kriminalität. Wichtige Aspekte wie die eigentlichen Ermittlungen, die nationalen Strukturen und die stufengerechte Ausbildung sind noch zu klären. Deshalb erarbeitet die Konferenz der Kantonalen Polizeikommandanten (KKPKS) das nationale Dispositiv „Cyber-Crime und IT-Forensik“. Dort werden diese organisatorischen und infrastrukturellen Fragen in ihrer Gesamtheit angegangen und die Allokation der hierfür notwendigen Ressourcen vollzogen.
Ziele und Handlungsbedarf	Das gesamtschweizerische Dispositiv zur Bekämpfung der Cyber-Kriminalität der KKPKS und der dazugehörige Umsetzungsplan sollen alle vom Lagebild, der Ausbildung, über die Koordination bis zur Ermittlung reichenden Aspekte der Bekämpfung der Cyberkriminalität umfassen. 

Massnahmen

17) Lagebild Cyber-Kriminalität
Bund (fedpol) und Kantone (KKPKS) prüfen und konzipieren die technischen Rahmenbedingungen für die Erarbeitung eines nationalen polizeilichen Echtzeit-Lagebilds zur Cyber-Kriminalität. Diese Arbeiten werden in Zusammenarbeit mit dem Programm Harmonisierung der Polizeiinformatik (HPI) durchgeführt.

18) Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDK)
Bund (fedpol) und Kantone (KKJPD) erarbeiten eine Verwaltungsvereinbarung über die Zusammenarbeit und Koordination zwischen dem nationalen Cyber Competence Center (NC3) und den regionalen Cyber Competence Centren (RC3) im NEDK.

19) Ausbildung zu Cyber-Kriminalität
In Zusammenarbeit zwischen der Konferenz der kantonalen Polizeidirektoren (KKPKS) und der Schweizerischen Staatsanwälte-Konferenz (SSK) werden spezifisch Ausbildungskonzepte für den nach den nachhaltigen Aufbau der erforderlichen Kompetenzen in der Strafverfolgung geschaffen.

20) Zentralstelle Cyber-Kriminalität
Fedpol veranlasst die Anpassung des Zentralstellengesetzes (ZentG) zwecks Schaffung einer Zentralstelle Cyber-Kriminaliät.

4.8 Cyber-Defence

Übersicht Handlungsfeld	
Beschreibung	Grossangelegte oder sehr gezielte Cyber-Angriffe auf kritische Infrastrukturen der Schweiz können die Sicherheit der Bevölkerung und der Wirtschaft gefährden. Neben einer breiten Palette an Massnahmen, die den Schutz vor Cyber-Risiken stärken, braucht es deshalb über alle Lagen auch Fähigkeiten und Ressourcen, um laufende Angriffe zu unterbinden und die dafür verantwortlichen Akteure zu identifizieren. Bei Angriffen, welche das Funktionieren kritischer Infrastrukturen gefährdet, müssen nötigenfalls aktive Gegenmassnahmen ergriffen werden können, um deren Betrieb sicherzustellen. Die Cyber-Defence umfasst daher jene Massnahmen, die generell der Verteidigung kritischer Systeme und der Abwehr von Angriffen im Cyberraum über alle Lage, also bis zu Konflikt- und Kriegszeiten dienen.
Ausgangslage	Mit dem NDG und dem revidierten MG verfügt der Bund, namentlich das VBS über die notwendigen Rechtsgrundlagen zum Ausbau und Ergreifen aktiver Massnahmen und Gegenmassnahmen im Rahmen der Cyber-Defence. Die Entwicklung von Cyber-Angriffen über die letzten Jahre und ihre wachsende Komplexität bindet jedoch zunehmend Ressourcen über längere Zeiträume. Dies führt zur Gefahr, dass gleichzeitig laufende Angriffe nicht zeitgerecht entdeckt werden, da die wenigen verfügbaren Spezialisten mit der Verfolgung anderer Vorfälle absorbiert sind. Auch erschweren die knappen Ressourcen die notwendige, durchgehende Nachbearbeitung von Vorfällen. In seinem „Plan d'Action Cyberdéfense" (PACD) hat das VBS den Handlungs- und Ressourcenbedarf im Bereich Cyber-Defence festgestellt, die Aufträge der verschiedenen Stellen (insbesondere auch der Armee) definiert und beschrieben welche Massnahmen zur Bewältigung der Aufgaben getroffen werden.
Ziele und Handlungsbedarf	Der Nachrichtendienst muss mittels einer systematischen Informationsbeschaffung und -auswertung in der Lage sein, neue Angriffsmuster möglichst frühzeitig zu entdecken. Weiter muss er eine möglichst genaue Feststellung der Urheberschaft von erfolgten Angriffen (Attribution) vorzunehmen können, damit die Handlungsfreiheit der politischen Behörden und der Strafverfolgungsbehörden gewahrt wird. Bei Angriffen auf kritische Infrastrukturbetreiber, muss der Nachrichtendienst unter Einbezug unterstützender Einheiten in der Lage seinen Auftrag im Rahmen des NDG zu erfüllen. Die Armee spielt als strategische Reserve zur subsidiären Unterstützung ziviler Verwaltungseinheiten und im Falle der Mobilmachung eine entscheidende Rolle. Sie muss daher die Einsatzbereitschaft über alle Lagen im Bereich der Cyber-Defence gewährleisten können.

Massnahmen

21) Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution
Das vorhandene Spezialwissen und die Fähigkeiten zur Informationsbeschaffung zwecks Früherkennung von Cyber-Angriffen und zur Identifikation der Urheberschaft werden weiterentwickelt, die Zusammenarbeit dazu zwischen Bund und Kantonen gestärkt und der Informationsaustausch mit der Wirtschaft ausgebaut. Der Nachrichtendienst des Bundes führt vertiefte Akteurs- und Umfeldanalysen durch, nutzt und entwickelt technische Hilfsmittel, die Fernmeldeüberwachung und Methoden der *Human Intelligence*. Erfolgte Cyber-Angriffe werden so systematisch aufgearbeitet und verfolgt.

22) Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gem. NDG und MG

Das VBS (NDB und Armee) verfügen über genügend qualitative und quantitative Kompetenzen und Kapazitäten um gegebenenfalls Angriffe auf Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft, Staat und Armee unerlässlich sind (kritische Infrastrukturen) zu stören, zu verhindern oder zu verlangsamen.

23) Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum

Die Armee stellt im Rahmen der Umsetzung WEA sicher, dass sie über genügend Mittel, Ressourcen und Fähigkeiten verfügt, ihren Auftrag nach MG in der ausserordentlichen Lage im Cyber-Raum wahrzunehmen. Die Armee verfügt über die Bereitschaft, als strategische Reserve subsidiär zivile Behörden zu unterstützen. Dazu bildet sie ihre Kader und Armeeangehörige entsprechend aus.

4.9 Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik

Übersicht Handlungsfeld	
Beschreibung	Der Cyber-Raum hat eine neue Dimension der Aussensicherheitspolitik geschaffen. Der Cyber-Raum wird von staatlichen Akteuren zunehmend zur Machtprojektion und für die Erreichung politischer Ziele, nachrichtendienstliche Vorhaben sowie militärische Zwecke genutzt. Nebst dem Einsatz von Cyber-Mitteln in konventionellen bewaffneten Konflikten, werden Auseinandersetzungen vermehrt auch im digitalen Raum ausgetragen. Entsprechend ist die internationale Zusammenarbeit sowohl auf diplomatischer als auch auf technisch-operativer Ebene zur Reduktion von Cyber-Risiken unabdingbar. Die Wahrung der aussen- und sicherheitspolitischen Interessen der Schweiz muss auch im Cyber-Raum sichergestellt werden. Die Schweiz engagiert sich daher sowohl auf diplomatischer als auch auf technisch-operativer Ebene für die Stärkung der internationalen Kooperation zur Minimierung von Cyber-Risiken.
Ausgangslage	Bereits in der NCS von 2012 wurde die Bedeutung der internationalen Kooperation hervorgehoben. Die Prozesse und Strukturen für eine koordinierte und kohärente Cyber-Aussensicherheitspolitik sind geschaffen worden. Auch in der 2016 vom Bundesrat verabschiedeten Strategie „Digitale Schweiz“ werden sicherheitspolitische Überlegungen berücksichtigt. In den relevanten internationalen Prozessen wird die Schweiz als aktive, verlässliche und vertrauenswürdige Partnerin wahrgenommen und auch gehört. Die Schweiz hat sich stark in der Entwicklung und Umsetzung von ersten vertrauensbildenden Massnahmen zwischen Staaten im Cyber-Bereich engagiert. Multilaterale Prozesse mit Bezug zur Cyber-Sicherheit gestaltet sie aktiv mit und vertieft die Kooperation mit ausgewählten Ländern und Organisationen.
Ziele und Handlungsbedarf	Für die Minimierung von Cyber-Risiken ist eine kohärente Cyber-Aussensicherheitspolitik unabdingbar. Deren übergeordnetes Ziel ist ein freier, offener und sicherer Cyber-Raum. Die Schweiz bedient sich zur Wahrung ihrer Interessen gegenüber Staaten und internationalen Organisationen sowie zur Förderung von Frieden, Stabilität und internationaler Sicherheit verschiedener Instrumente. Sie setzt sich *erstens* für die Anerkennung, Einhaltung und Durchsetzung des Völkerrechts im Bereich Cyber-Sicherheit ein und trägt zur Klärung der Frage bei, wie bestehendes Völkerrecht im Cyber-Raum angewendet wird. *Zweitens* engagiert sich die Schweiz aktiv für die zwischenstaatliche Vertrauensbildung. Und *drittens* unterstützt und entwickelt sie Initiativen zum Ausbau nationaler Fähigkeiten und zum Aufbau von Kapazitäten in Drittstaaten. Bei letzterem soll auch sichergestellt werden, dass möglichst alle interessierten Akteure an den internationalen Diskussionen zur Förderung der Cyber-Sicherheit teilnehmen können. Bei allen Aktivitäten gilt ein Augenmerk auch der Förderung der Schweiz und des internationalen Genfs als Plattform für Diskussionen zur Cyber-Aussensicherheitspolitik.

Massnahmen

24) Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik

Die Schweiz setzt sich im Bereich Cyber-Aussensicherheitspolitik für die Entwicklung eines Regelwerkes zur verantwortungsvollen Nutzung der Informations- und Kommunikationstechnologien ein. Dies tut sie im Rahmen der UNO, der OSZE und weiterer relevanter internationaler Fora.

Sie setzt sich für eine Stärkung der Anerkennung des Völkerrechts ein und trägt zur Klärung von spezifischen Fragen zu dessen Anwendung bei (z.B. UNO-Expertengruppe und Folgeprozesse, Tallinn-Prozess und weitere).

Die Schweiz vertritt den Grundsatz, dass dieselben Menschenrechte, die offline gelten, auch online anwendbar sind. Sie setzt sich deshalb dafür ein, dass der Schutz der Menschenrechte auch im Rahmen sicherheitspolitischer Interaktionen im Cyber-Raum gewährleistet ist.

Die Schweiz engagiert sich ferner in der OSZE und in anderen relevanten Fora für die Umsetzung und Weiterentwicklung von vertrauensbildenden Massnahmen.

Schliesslich beteiligt sie sich aktiv an den Diskussionen zur Schnittstelle zwischen Cyber-Sicherheit und Rüstungskontrolle und fördert den Aufbau von Know-How und Kapazitäten in diesem Themenbereich.

25) Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit

Durch die Zusammenarbeit und den Austausch mit anderen Staaten, internationalen Organisationen oder spezialisierten Forschungszentren (z.B. Cooperative Cyber Defence Centre of Excellence) soll die Schweiz ausländisches Know-How nutzen, um die nationalen Fähigkeiten zur Risikominimierung auszubauen.

Die Schweiz unterstützt Projekte und Initiativen zum Aufbau von Kapazitäten im Bereich Cyber-Sicherheit in anderen Staaten (z.B. Expertenaustausch zum Aufbau von Institutionen und Cyber-Aussensicherheitsstrukturen, Durchführung von Workshops zu internationalen Prozessen, Unterstützung des Global Forum on Cyber-Expertise).

26) Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussen-Sicherheitspolitik

Die Schweiz führt mit ausgewählten Ländern Konsultationen zu Cyber-Aussensicherheitspolitik durch, insbesondere zur Bedrohungslage und zu Trends. Sie gestaltet multilaterale Dialoge aktiv mit (z.B. Sino-European Cyber-Dialog).

4.10 Aussenwirkung und Sensibilisierung

Übersicht Handlungsfeld	
Beschreibung	Die rasche Entwicklung und Zunahme von Cyber-Risiken führt in der Bevölkerung und in der Wirtschaft zu Verunsicherungen. Es ist für Einzelpersonen und Unternehmen schwierig, einzuschätzen, welchen Cyber-Risiken sie ausgesetzt sind und welche Schutzmassnahmen für sie sinnvoll sind. Neben der Schwierigkeit, die Cyber-Risiken für sich selber abschätzen zu können, bleibt auch oft unklar, welche Unterstützung vom Staat erwartet werden kann. Das breite Portfolio der NCS und die dezentrale Umsetzung machen es für Aussenstehende schwierig, zu verstehen, welche Massnahmen der Staat trifft, um den Schutz der Schweiz vor Cyber-Risiken zu verbessern. Die aktive Kommunikation über die ergriffenen Massnahmen und die erzielten Fortschritten gehört deshalb zu den Aufgaben der Strategieumsetzung. Zusätzlich zur Kommunikation über die NCS soll der Bund auch zur Sensibilisierung gegenüber Cyber-Risiken beitragen. Die Information der Bevölkerung über Cyber-Risiken und mögliche Schutzmassnahmen trägt zur Prävention und zur Verbesserung der Resilienz bei und hilft, Verunsicherungen zu mindern.
Ausgangslage	Die Resultate der NCS wurden der Öffentlichkeit bisher über die Jahresberichte, die jährlichen Tagungen (NCS-Tagung und Cyber-Landsgemeinde) und die Website vermittelt. Rückmeldungen aus Bevölkerung, Wirtschaft und Politik haben aber gezeigt, dass der Informationsbedarf über die vorhandenen Instrumente nicht genügend abgedeckt wird. Neue Vorfälle haben ebenfalls gezeigt, dass es weiterhin nötig ist, die Allgemeinheit für Cyber-Risiken zu sensibilisieren und auf grundlegende Schutzmöglichkeiten aufmerksam zu machen.
Ziele und Handlungsbedarf	Die Information der Öffentlichkeit über die Umsetzung der NCS soll künftig aktiver erfolgen, so dass über den Kreis der Fachpersonen hinaus bekannt wird, welche Massnahmen der Bund zum Schutz der Schweiz vor Cyber-Risiken umsetzt. Im Sinne der Prävention soll der Bund zudem verstärkt dazu beitragen, Bevölkerung, Wirtschaft und Politik für Cyber-Risiken zu sensibilisieren und über mögliche Schutzmassnahmen zu informieren.

Massnahmen
27) Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS Die Kommunikationsleitlinien, Zuständigkeiten und Prozesse sind in einem Konzept festgehalten. Es wird dabei auch die Balance zwischen Vertraulichkeit und Informationsbedürfnis erörtert. Die Umsetzung des Konzepts über Medien- und Öffentlichkeitsarbeit soll zielgruppengerecht erfolgen und aktiv vorangetrieben werden.
28) Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness) Der Bund will mithelfen, die Öffentlichkeit für Cyber-Risiken zu sensibilisieren. Er verstärkt die Kommunikation zu Cyber-Risiken und nutzt die bestehenden Kapazitäten der in diesem Bereich bereits aktiven Vereinen, Verbände und Behörden.

5 Umsetzung der Strategie

Dieses Kapitel ist noch in Erarbeitung. Es wird eine Übersicht zur Organisationsstruktur der NCS beinhalten. Die Grundelemente dieser Organisation sind:

- Zentrale Steuerung der NCS-Umsetzung durch ein zu schaffendes Kompetenzzentrum Cyber-Risiken im Bund
- Beschreibung der Zusammenarbeit dieses Kompetenzzentrums mit weiteren Stellen (z.B. Armee, Behörden der Strafverfolgung, Kantone, kritische Infrastrukturen) zur Umsetzung der NCS
- Begleitung der Umsetzung durch externe Fachleute
- Zuteilung der Verantwortung für die Umsetzung der Massnahmen

Die Details zur Umsetzung der Massnahmen werden in einem separaten Umsetzungsplan erläutert. Dieser definiert die Zuständigkeiten der verschiedenen Bundesstellen, beschreibt die nötigen Kooperationen und legt messbare Leistungsziele fest. Der Umsetzungsplan ist aktuell in Arbeit.

6 Abkürzungsverzeichnis

7 Glossar