Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-22

Der Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 (NCS) wurde von einer Arbeitsgruppe des Sicherheitsverbundes Schweiz (SVS) erarbeitet und präsentiert sich eigenständig aber komplementär zum nationalen Umsetzungsplan. Es handelt sich konkret um 13 Umsetzungsprojekte in sieben von 10 Handlungsfeldern der NCS.

Der Sicherheitsverbund Schweiz[1] hatte zusammen mit seiner Arbeitsgruppe zur Umsetzung der NCS in den Kantonen[2] bereits vor Verabschiedung der Nationalen Cyber-Strategie im April 2018 durch den Bundesrat Handlungsfelder identifiziert, die für die Kantone von besonderer Bedeutung sind und welche sie vertieft bearbeiten wollen. Daraufhin skizzierten die Mitglieder der Arbeitsgruppe verschiedene Umsetzungsprojekte und legten diese in Form eines Entwurfs der Herbstversammlung der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und –direktoren (KKJPD) zur Kenntnisnahme vor. Daraufhin erteilte diese der Arbeitsgruppe des SVS den Auftrag, weitere Konkretisierungsarbeiten vorzunehmen, sodass der Umsetzungsplan in der Frühjahrsversammlung 2019 verabschiedet werden könnte. Die Kantone äusserten somit nicht zuletzt den Willen, in ihrer Dynamik und aus eigener Initiative den Schutz ihrer Bevölkerung vor Cyber-Risiken weiter zu verbessern.

Um die Kohärenz zwischen der nationalen Umsetzungsplanung und dem Umsetzungsplan "Kantone" zu gewährleisten, nahmen einige kantonale Vertreter, die KKJPD und der SVS in seiner Rolle als Schnittstelle zwischen Bund und Kantonen, an den Workshops zur nationalen Umsetzungsplanung teil. Die Koordinationsstelle NCS und die Geschäftsstelle haben ausserdem gemeinsam den Workshop zur Umsetzungsplanung der NCS mit den Kantonen im Februar 2019 organisiert. Die Teilnehmenden überprüften die Umsetzungsprojekte nebeneinander auf Doppelspurigkeiten und konnten diese mit ihren Beiträgen bereichern. Konkret wurden insgesamt vier Projekte sowohl in den nationalen Umsetzungsplan als auch in den Umsetzungsplan der Kantone übernommen.

---

[1] Der Sicherheitsverbund Schweiz geht aus dem sicherheitspolitischen Bericht 2010 hervor. Im Sicherheitsverbund Schweiz sind Bund und Kantone paritätisch vertreten. Die politisch-strategischen Organe (Operative und Politische Plattform1) dienen der Konsultation und Koordination von Entscheiden, Mitteln und Massnahmen in sicherheitspolitischen Fragen und Herausforderungen. In Arbeitsgruppen, in denen auch die kommunale Ebene und die Privatwirtschaft vertreten sein können, werden konkrete Lösungsvorschläge erarbeitet. Siehe auch https://www.svs.admin.ch/

[2] Die Arbeitsgruppe setzte sich aus kantonalen Vertretern aus verschiedenen Disziplinen zusammen (Strafverfolgung, Informationssicherheitsbeauftragte von Kantonen, Vertreter der Schweizerischen Informatikkonferenz (SIK), der KKJPD und aus dem Bereich der Bildung und Forschung).

1. Kompetenzen- und Wissensaufbau

(1) Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen M2 Ausbau und Förderung der Kompetenzbildung	
Zielzustand	Eine proaktive und generelle Stärkung der Cyberkompetenzen ist eminent wichtig. Die kantonalen Verwaltungen und ihre zugehörigen Institutionen sind eine tragende Säule unserer Gesellschaft, ihr Personal muss deshalb zwingend in diesem Bereich geschult werden. Die kantonalen Informatikdienste haben das Umfeld, in dem wir uns bewegen, analysiert und setzen die erforderlichen technischen und organisatorischen Mittel zur Aufrechterhaltung einer sicheren Arbeitsumgebung ein. Vereinzelt wurden bereits Initiativen zum Ausbau der Kompetenzen des Personals ergriffen, bislang jedoch nicht systematisch, obwohl der Mensch unbestritten ein zentraler Faktor der Informationssicherheit ist.
Umsetzungs-verantwortung	Haute école de gestion Arc – Institut de lutte contre la criminalité économique (ILCE) in Zusammenarbeit mit dem Service informatique de l'Entité neuchâteloise, dem Staatssekretariat für Bildung, Forschung und Innovation (SBFI), der Koordinationsstelle NCS und der Schweizerischen Informatikkonferenz (SIK)
Beteiligung	Hochschulen, Wirtschaftsverbände, Fachverbände (Schweizerischen Expertenvereinigung «Bekämpfung der Wirtschaftskriminalität» (SEBWK), Association suisse de la sécurité de l'information (CLUSIS) usw.)
Bestehende Gremien / Prozesse	In diesem Bereich bereits getroffene Massnahmen werden berücksichtigt und wo sinnvoll in das Vorgehen einbezogen.
Instrumente	• Vorschlag eines Ausbildungsprogramms für das Personal der kantonalen Verwaltungen mit klarer und pragmatischer Definition der angestrebten Ziele und Kompetenzen • Langfristige Sicherstellung des Ausbildungssystems zum Thema Cyber für Verwaltungsangestellte • Förderung der landesweiten Verbreitung dieser Ausbildung in allen betroffenen Behörden • Die Inhalte des Ausbildungsprogramms sollten idealerweise durch die Durchführung einer Pilot-Präsenzausbildung validiert werden; dies könnte in Neuenburg erfolgen, sobald das Ausbildungskonzept fertiggestellt ist.

Messbare Leistungsziele	• Erster Bericht; Ausgangslage
	• Ausbildungskonzept mit Zieldefinitionen nach Zielgruppen
	• Umfassendes, auf das Personal der kantonalen Verwaltungen zugeschnittenes Ausbildungsprogramm mit den folgenden Zielen:
	  ○ Entwicklung der Cybergrundkompetenzen aller Angestellten
	  ○ Den Angestellten die nötigen Mittel zur Verfügung stellen, um die Informationsflüsse angemessen steuern zu können, insbesondere jene von oder nach ausserhalb der Organisation

	○ Den Angestellten die Bedeutung von Informationen und damit den Nutzen von Massnahmen zur Sicherstellung gewisser Grundregeln betreffend Speicherung, Bearbeitung und Übermittlung von Informationen verständlich machen ○ Den Angestellten die nötigen Kenntnisse vermitteln, damit sie gute Praktiken im Cyberbereich in ihrem privaten Umfeld vorleben können • Erarbeitung eines didaktischen Instruments, zum Beispiel im E-Learning-Format

2. Bedrohungslage

(2) #MISP[3] – Malware Information Sharing Platform von MELANI für und mit den Kantonen M4 Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage	
Zielzustand	Zur Verbesserung ihrer Fähigkeiten der Beschreibung und Beurteilung von Cyberrisiken erstellen die Kantone einen Bedrohungsradar, für den sie die von MELANI zur Verfügung gestellten Informationen nutzen. Falls nötig integrieren sie darin kantonale Bedrohungsindikatoren. Die Kantone übernehmen in Zusammenarbeit mit dem Bund ein einheitliches Vokabular (Taxonomie), mit dem die Cyber-Bedrohungen schweizweit strukturiert und besser dargestellt werden können. Ergänzend dazu entwickeln sie einen Rahmen für die operative Zusammenarbeit, um Eindringversuche und Malware (Viren) besser abwehren zu können, und binden Nachrichtendienste und Stellen für das proaktive Monitoring der Cyber-Bedrohungen auf kantonaler Ebene ein.
Umsetzungs-verantwortung	MELANI und die Kantone
Beteiligung	Hochschulen, Wirtschaftsverbände, Fachverbände, auf Cyber-Sicherheit spezialisierte private Akteure
Bestehende Gremien / Prozesse	• Cyber-Bedrohungsradar von MELANI • Plattform MISP (Malware Information Sharing Platform) von MELANI
Instrumente:	In Zusammenarbeit mit MELANI: 1. Adoption einer Taxonomie für eine kohärente und homogene Strukturierung und Darstellung der Cyberbedrohungen in der ganzen Schweiz (auf Ebene Bund, Kantone und Gemeinden) 2. Entwicklung eines kantonalen Modells des Cyberbedrohungsradars

[3] MISP = Malware Information Sharing Platform, bezeichnet eine digitale Applikation, welche den Austausch zu Cyberbedrohungen und Informationen erleichtert.

	3. Einführung eines schweizerischen Netzwerks für den Informationsaustausch zu Malware, basierend auf einer MISP-Lösung (Malware Information Sharing Platform) 4. Einführung eines Mindeststandards zur Prüfung der eigenen Vulnerabilität an der im Web exponierten Peripherie der kantonalen Netzwerke mittels regelmässiger Vulnerability Scans[4] 5. Aufbau eines einfachen und effizienten Monitoring- und Analyseprozesses (OSINT – open-source intelligence), der zwischen Bund und Kantonen ausgetauscht werden kann Rahmenbedingung: • Einbindung kantonaler Experten für Cybersicherheit bei der Umsetzung der operativen Massnahmen in den Kantonen
Messbare Leistungsziele:	1. Adoption einer einheitlichen Taxonomie der Cyberbedrohungen durch Bund und Kantone 2. Kantonaler Cyberbedrohungsradar in Betrieb 3. Aktiver Austausch von operativen Informationen zu Malware zwischen den Kantonen 4. Regelmässige Evaluation der Sicherheit ihrer im Internet exponierten peripheren Netzwerkzugangspunkte durch die Kantone 5. Periodische Veröffentlichung von Berichten zum Monitoring der Cyberbedrohungen

3. Resilienzmanagement

(3) Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen M5 Verbesserung der IKT-Resilienz der kritischen Infrastrukturen	
Zielzustand	Für eine Verbesserung der Resilienz (Widerstands- und Regenerationsfähigkeit) haben die Kantone minimale Anforderungen in Bezug auf relevante Prozesse, Aufgaben/Kompetenzen analysiert. Sie verwenden hierfür unter anderem ein Analyse-Tool, das sich an den vom Bundesamt für wirtschaftliche Landesversorgung[5] publizierten Massnahmen zur Verbesserung der IKT-Resilienz in kritischen Teilsektoren orientiert und für ihre Bedürfnisse adaptiert wurde. Sie leiten aus den Erkenntnissen der Analyse weitere Massnahmen ab.
Umsetzungsverantwortung	Stv. Leiter Kantonale Informationssicherheit (Deputy CISO) des Kantons Basel-Stadt in Zusammenarbeit mit dem Sicherheitsverbund Schweiz

[4] Vulnerability Scans sind mit einem Programm möglich, das Computer, Netzwerke und Anwendungen auf bekannte Schwachstellen untersucht.

[5] Bundesamt für wirtschaftliche Landesversorgung; "Minimalstandard zur Verbesserung der IKT-Resilienz", Bern, 2018, abrufbar unter: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Beteiligung	Jede Organisation resp. Betreiber einer kritischen Infrastruktur (KI) ist für die Informationssicherheit selber verantwortlich. Die Verantwortung trägt die Geschäftsleitung. Die Geschäftsprozessverantwortlichen, der Risikomanager, der Informationssicherheitsbeauftrage, der Informatikleiter und ev. der Notfallmanager sind die wichtigsten Ansprechpartner der Geschäftsleitung.
Bestehende Gremien / Prozesse	In der Organisation wird der Business Continuity Management (BCM) Prozess aufgebaut und von einer externen Stelle überprüft. Wichtige Ressourcen innerhalb des BCM sind: • Mitarbeitende • Gebäude und Räume • Informatik- und Telekommunikationsmittel (IKT) und Informationen • Externe Dienstleistende und Informationen
Instrumente:	**Einsatz des Erhebungstools** Mit der Durchführung der Erhebungen zur Einschätzung der eigenen IKT-Resilienz verstärken die Unternehmen ihr Sicherheitsorganisation. Die Erhebung bietet eine Grundlage für die Zuweisung von Verantwortlichkeiten, Kompetenzen und klaren Aufgaben. Ein rascher Indikator bietet der Erfüllungsgrad der empfohlenen Sicherheitsmassnahmen. Bei einem allfälligen Defizit können risikomindernde Massnahmen definiert werden. **Anonyme Übersicht der beteiligten Organisationen** Die Informationen (Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen), die die beteiligten Organisationen dem SVS mitteilen, werden aufbereitet und in anonymisiert. Die Resultate werden definierten Gremien in anonymisierter Form vorgestellt. **BCM-Prozess** Für den BCM-Prozess ist es notwendig, dass alle Geschäftsprozesse dokumentiert sind. Das Risikomanagement, das Notfallmanagement oder. Krisenmanagement und das IT-Notfallmanagement müssen zwingend vorhanden sein. Wichtige Informationen sind die maximale Ausfallzeit und eventuelle Ausweichszenarien, diese Vorgaben werden vom Geschäftsprozessverantwortlichen und von der Geschäftsleitung vorgegeben.
Messbare Leistungsziele:	• Betreiber kritischer Infrastrukturen in der Schweiz haben anhand des ihnen zur Verfügung gestellten Erhebungstools individuell ihre Defizite in Bezug auf die IKT-Resilienz festgestellt und entsprechende Massnahmen getroffen. Messgrössen sind: o Erfüllungsgrad in % o Risikoerhebung (tief, mittel oder hoch o Maximal zu erwartender Schaden in Abhängigkeit der Zeit. • Die Durchführung der Erhebung unter Betreibern kritischer Infrastrukturen hat dazu geführt, dass gezielte Massnahmen ausgeführt wurden und die IKT-Resilienz sich insgesamt verbessert. Die umgesetzten Massnahmen wurden auf ihre Wirksamkeit überprüft. Messgrössen sind: o offene Massnahmen, o Massnahme in Bearbeitung und o umgesetzte Massnahmen • Die Resultate der Erhebung wurden in vordefinierten Gremien bspw. Staatsschreiberkonferenz (SSK), Schweizerische Informatikkonferenz

	(SIK) in anonymisierter Weise vorgestellt. Messgrössen sind: o Übersicht der beteiligten Organisationen o Veranstaltungen, an denen die Resultate vorgestellt worden sind

(4) Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen M7 Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen	
Zielzustand	Mit einem institutionalisierten Erfahrungsaustausch und Dialog fördern die Kantone die Zusammenarbeit zur Stärkung der IKT-Resilienz. Sie nutzen dafür bestehende Netzwerke und erweitern diese wie angebracht. Sie nehmen aktiv an der Arbeitsgruppe Informatiksicherheit der SIK teil. Somit bauen sie beständig gegenseitiges Vertrauen auf, unterstützen sich gegenseitig und koordinieren ihr Vorgehen, nicht zuletzt im Ereignisfall. Sie erstellen gemeinsam hilfreiche Grundlagen (Konzepte, Checklisten, etc.).
Umsetzungs-verantwortung	Arbeitsgruppe Informatiksicherheit der SIK in Zusammenarbeit mit den federführenden, kantonalen Regierungsstellen und deren Informationssicherheitsbeauftragten
Beteiligung	SVS
Bestehende Gremien / Prozesse	• Kantonale Informationssicherheitsbeauftragter • Arbeitsgruppe Informatiksicherheit innerhalb der SIK
Instrumente:	• Kantonale Informatikstrategie • Kantonales Risikomanagementsystem • Kantonale IT-Risikomanagement • Kantonales Ausbildungskonzept • Kantonales Informationssicherheitsmanagementsystem (ISMS)
Messbare Leistungsziele:	• Die Kantone stellen sicher, dass der Kantonale Informationssicherheitsbeauftragte Mitglied der Arbeitsgruppe „Informatiksicherheit“ der SIK ist. Nachweis: Die kantonalen Informatiksicherheitsbeauftragten arbeiten zusammen und vertrauen sich gegenseitig. Sie setzen die Empfehlungen der Arbeitsgruppe in ihren Kantonen um. • Die Kantone stellen sicher, dass ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Informationssicherheit und der Cybersecurity angemessen und stufengerecht geschult und ausgebildet werden. Nachweis: Übersicht der durchgeführten Kampagnen und Schulungen. • Ein **IT-Risikomanagement** (Teil des kantonalen Risikomanagements), das auch die Risiken der kritischen Infrastrukturen enthält, ist umgesetzt. Nachweis: Vorhandenes IT-Risikomanagement inkl. Übersicht der risikomindernden Massnahmen. • Ein der Organisation angepasstes **Informationssicherheitsmanagementsystem** (ISMS) ist eingeführt.

	Nachweis: das ISMS ist von der Leitung genehmigt und wird „gelebt“.

(5) Sensibilisierung der jungen und älteren Menschen für Cyberrisiken	
Zielzustand	Für eine verbesserte Resilienz der Schweiz in Bezug auf Cyberrisiken werden sowohl die junge als auch die ältere Bevölkerungsschicht sensibilisiert. Mit einem verstärkten Bewusstsein für die Bedrohungen aus dem Cyberraum verändern sie ihr Verhalten so, dass sie die Möglichkeiten der Digitalisierung ausschöpfen können ohne vermeidbare Risiken einzugehen. Durch die Vermittlung von bestimmten, zielgruppengerechten Lerninhalten konnten die jungen und älteren Menschen ihr Wissen im Bereich der Digitalisierung und der daraus resultierenden Chancen und Risiken erhöht.
Umsetzungs-verantwortung	Schweizerische Konferenz der kantonalen Erziehungsdirektion (EDK) in Zusammenarbeit mit der Konferenz der kantonalen Sozialdirektorinnen und Sozialdirektoren (SODK) und der Schweizerischen Kriminalprävention (SKP),
Beteiligung	pro senectute, pro juventute, privatim, SVS
Bestehende Gremien / Prozesse	
Instrumente	Die jungen und älteren Menschen in der Schweiz sollen über die Lehrpersonen einerseits und über das Pflegepersonal andererseits auf die Risiken, denen sie im Cyberraum begegnen können, aufmerksam gemacht werden.
Messbare Leistungsziele	• Etablierung und Konsolidierung einer Partnerschaft für die Sensibilisierung der jungen und älteren Menschen • Konzeption von zugeschnittenen Lerninhalten

4. Standardisierung/Regulierung

(6) Umsetzung der Netzwerksicherheitspolicy (NSP) M8 Entwicklung und Einführung von Minimalstandards	
Zielzustand	Die Kantone betreiben ihre Netzte und Systeme sicher, indem sie die Aussenschnittstellen zu ihren Informatiknetzwerken möglichst gut sichern und auch die Tätigkeiten innerhalb des eigenen Netzwerkes permanent überwachen. Mit dieser gemeinsamen Basis erhöhen die Kantone auch die Sicherheit innerhalb gemeinsam genutzter Netzwerke und Applikationen. • Förderung der Zusammenarbeit unter Einhaltung der vordefinierten Standards

	• Aufbau des gegenseitigen Vertrauens durch den Einsatz der definierten Standards • Geeignete Dokumentation (Konzepte, Checklisten, etc.) • Geeignete und sichere Dokumentenablage
Umsetzungs-verantwortung	Konferenz der Kantonsregierungen (KdK)
Beteiligung	Schweizerische Informatikkonferenz SIK, SVS
Bestehende Gremien / Prozesse	• Arbeitsgruppe Informatiksicherheit innerhalb der SIK • Melde und Analysestelle der Informationssicherung MELANI
Instrumente:	• Netzwerk Netzwerk-Sicherheits-Politik (als Basis dient die NSP-SIK 2017) • Orientierung an weiteren bestehenden Standards • Geeignete Prozesse (Change-, Problem-, Incidents- Risiko- und Notfallmanagement) • Einsatz von definierten Standards und Empfehlungen bspw. ISO 2700x, BSI, SANS CSC, oder CIS 20
Messbare Leistungsziele:	• Kantonseigene Netzwerk-Sicherheits-Policy wurde erarbeitet und in Anlehnung an die Vorgaben der SIK (NSP-SIK 2017)[6] umgesetzt. • Definierte und gelebte Standards • Ausgebildetes Personal • Definierte Prozesse (Change-, Problem-, Incident- Risiko-, Notfallmanagement sowie Berichtswesen)

5. Krisenmanagement

(7) Cyber-Übung mit kritischen Infrastrukturen im Gesundheitssektor M17 Gemeinsame Übungen zum Krisenmanagement	
Zielzustand	Die Koordination auf operativer Ebene zwischen Bund, den Kantonen und Vertretern kritischer Infrastrukturen in einer Krisensituation funktioniert. Das Lagebild ist in der Krise aktuell und kann von den betroffenen Stellen eingesehen werden. Das Konzept zur Führung in Krisen mit Cyber-Ausprägungen konnte getestet werden.
Umsetzungs-verantwortung	SVS
Beteiligung	Bundeskanzlei, Gesundheitsdirektorenkonferenz

[6] Die Netzwerksicherheitspolicy der Schweizerischen Informatikkonferenz ist über das Intranet der selbigen für alle Mitglieder abrufbar.

Bestehende Gremien / Prozesse	Allgemeines Krisenmanagement (Führungsabläufe und –prozesse) der Kantone und des Bundes unabhängig vom Szenario SVU19
Instrumente	• Konzept M15 NCS I erweitert um Kantone und KI.
Messbare Leistungsziele	• Anzahl durchgeführter Übungen mit allen betroffenen Organisationen (1 Table Top Übung bis 2020, 1 Stabsrahmenübung bis 2021) • Ein aktuelles und präzises Lagebild war während der Übung jederzeit verfügbar und wurde von den teilnehmenden Akteuren adäquat bewertet (Evaluation) • Die an der Übung teilnehmenden Akteure konnten auf die Unterstützung der Stäbe durch fachspezifisches Wissen zählen (Einschätzung der Akteure der Übungserfahrung, Umfrage) • Die Beteiligten kennen die jeweiligen Zuständigkeiten und Ansprechstellen • Die Beteiligten kennen die Prozesse • Die Übungen wurden ausgewertet und die Lehren fliessen in die Optimierung der Führungsabläufe und –prozesse ein. Dafür wird ein Monitoringplan aufgesetzt. Die Erkenntnisse werden rapportiert.

(8) Schaffung der kantonalen Organisationen für Cyber-Sicherheit	
Zielzustand	Analog zur neu geschaffenen Organisationsstruktur im Cyber-Bereich auf Stufe Bund beabsichtigt diese Massnahme die Schaffung kantonaler Organisationen für Cyber-Sicherheit. Diese kantonale Stelle mit Budgethoheit und Weisungsbefugnis behält zu jeder Zeit den Überblick, repräsentiert den Kanton in Cyber-Belangen, vertritt ihn im KFS und gewährleistet die Schnittstellen im Kanton, zwischen den Kantonen und zum Bund.
Umsetzungs-verantwortung	Federführendes kantonales Departement
Beteiligung	Informationssicherheitsbeauftragte der Kantone, kantonale Führungsstäbe (KFS), Kantonspolizeien, Staatsanwaltschaften, Betreiber kritischer Infrastrukturen, SVS, Cyber-Delegierte/r des Bundes
Bestehende Gremien / Prozesse	Der SVS erarbeitet mit seiner Arbeitsgruppe Umsetzung NCS II mit den Kantonen einen Entwurf, der den Kantonen als Richtlinie und Vorlage zur Schaffung ihrer eigenen kantonalen Organisation für Cyber-Sicherheit zur Verfügung stehen soll.
Instrumente	
Messbare Leistungsziele	• Richtlinie/Vorlage durch die AG des SVS erarbeitet • in jedem Kanton wurde SOLL/IST-Analyse durchgeführt • Erstellung der kantonalen Cyber-Konzepte: Aufgaben, Kompetenzen und Verantwortung sind in einem kantonalen Cyberkonzept definiert • die kantonalen Exekutivbehörden haben zur Schaffung der kantonalen Cyberorganisation Beschluss gefasst

6. Strafverfolgung

Die Koordination und Verantwortung für die Massnahmen im Handlungsfeld Strafverfolgung liegt beim Cyberboard[7].

M18 Lagebild Cyber-Kriminalität	
Zielzustand	Bund (fedpol) und Kantone (KKPKS) haben die technischen Rahmenbedingungen für die Erarbeitung eines nationalen polizeilichen Echtzeit-Lagebilds zur Cyber-Kriminalität geprüft und konzipiert.
Umsetzungs-verantwortung	KKPKS / fedpol
Beteiligung	KKJPD/HPI (PTI), Kantone, MELANI
Bestehende Gremien / Prozesse	• Diese Arbeiten werden in Zusammenarbeit mit dem Programm Harmonisierung der Polizeitechnik und Informatik in der Schweiz (PTI) durchgeführt. • Das Lagebild Cyber-Kriminalität ist als Leistung im Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung, NEDIK aufzunehmen
Instrumente:	• Phänomenologie der Cyber-Kriminalität • HPI-Codes
Messbare Leistungsziele:	Die Strafverfolgungsbehörden des Bundes und der Kantone können sich einen Überblick über die Cybercrime-Aktivitäten und die Lage in der Schweiz machen. (Anzahl national erfasster Phänomene/Lagedarstellungen, erfasster Strafanzeigen, Zuordnung zu Phänomenen und darin angewandte Technologien)

M19 Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämfpung (NEDIK)	
Zielzustand	Bund (fedpol) und Kantone (KKJPD) haben eine Verwaltungsvereinbarung über die Zusammenarbeit und Koordination mit dem nationalen Cyber Competence Center (NC3) im NEDIK erarbeitet.
Umsetzungs-verantwortung	KKPKS / fedpol
Beteiligung	KKJPD, Kantone
Bestehende Gremien / Prozesse	

[7] Das Cyberboard ist ein Koordinationsgremium für die Analyse der Ausgangslage und Bearbeitung von Cybercrime-Meldungen der Polizei und Staatsanwaltschaften auf Bundes- und Kantonsebene.

Instrumente:	Die Aufgaben der ehemaligen Koordinationsstelle zur Bekämpfung der Internetkriminalität, KOBIK, sollen in die Verwaltungsvereinbarung NEDIK einfliessen.
Messbare Leistungsziele:	• Die Verwaltungsvereinbarung ist unterzeichnet. • Das Netzwerk ist operativ

M20 Ausbildung zur Bekämpfung der Cyber-Kriminalität	
Zielzustand	In Zusammenarbeit zwischen der Konferenz der kantonalen Polizeikommandanten (KKPKS) und der Schweizerischen Staatsanwälte-Konferenz (SSK) wurden spezifisch Ausbildungskonzepte für den nachhaltigen Aufbau der erforderlichen Kompetenzen in der Strafverfolgung geschaffen
Umsetzungs-verantwortung	KKPKS / SSK
Beteiligung	SPI, fedpol, Kantone
Bestehende Gremien / Prozesse	Arbeitsgruppe Robert Steiner im Auftrag der KKPKS SPI
Instrumente	• 5-Stufen-Ausbildungsmodell • E-Learning
Messbare Leistungsziele	• E-Learning für Stufe 1 erstellt und zugänglich • Ausbildungsprogramme für Stufe 2 werden durch SPI angeboten • Ausbildungsangebote der Stufen 3-5 werden durch Hochschulen und Universitäten in der Schweiz angeboten.

M21 Zentralstelle Cyber-Kriminalität	
Zielzustand	Die Anpassung des Zentralstellengesetzes (ZentG) zwecks Schaffung einer Zentralstelle Cyber-Kriminalität wurde durch fedpol veranlasst.
Umsetzungs-verantwortung	fedpol
Beteiligung	BJ, NEDIK
Bestehende Gremien / Prozesse	
Instrumente	Leistungskatalog NEDIK
Messbare Leistungsziele	Das angepasste ZentG tritt in Kraft (frühestens 2023)

7. Aussenwirkung und Sensibilisierung

(9) Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS II M28 Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS	
Zielzustand	Die interessierte Bevölkerung im Allgemeinen und die Partner des Sicherheitsverbundes Schweiz im Spezifischen haben die Möglichkeit sich über verschiedene Kanäle zu den Arbeiten der Kantone im Rahmen der NCS II zu informieren. Die Medien- und Öffentlichkeitarbeit erfolgt zielgruppengerecht und ist aktiv und dynamisch. Dabei legen die Stakeholder besonders Wert darauf, die Zusammenarbeit unter den Kantonen und über die Regierungsebenen hinweg zu unterstreichen, aber auch an die Eigenverantwortung zu appellieren. Ein Kommunikationskonzept wurde erarbeitet und umgesetzt.
Umsetzungs-verantwortung	SVS
Beteiligung	SIK, KKJPD
Bestehende Gremien / Prozesse	
Instrumente	• Cyber-Landsgemeinde • Website des SVS • Jahresberichte zur Umsetzung der Projekte aus dem Plan • Medienmitteilungen
Messbare Leistungsziele	• Ein Kommunikationskonzept (Leitlinien, Zuständigkeiten, Prozesse) besteht und wurde umgesetzt. • Verschiedene Kommunikationsprodukte wurden über diverse Kanäle der interessierten Bevölkerung und den Partnern des SVS zielgruppengerecht und zeitnah zur Verfügung gestellt (Anzahl publizierter Kommunikationsprodukte, Resonanz, Reichweite) • Umfrage zum Bekanntheitsgrad