année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**24.04.2024**
Thema	**Keine Einschränkung**
Schlagworte	**Cyberkriminalität**
Akteure	**Keine Einschränkung**
Prozesstypen	**Anderes**
Datum	**01.01.1965 - 01.01.2023**

Impressum

Herausgeber

Année Politique Suisse
Institut für Politikwissenschaft
Universität Bern
Fabrikstrasse 8
CH-3012 Bern
www.anneepolitique.swiss

Beiträge von

Ackermann, Nadja
Bühlmann, Marc
Ehrensperger, Elisabeth
Hirter, Hans
Porcellana, Diane
Schubiger, Maximilian

Bevorzugte Zitierweise

Ackermann, Nadja; Bühlmann, Marc; Ehrensperger, Elisabeth; Hirter, Hans; Porcellana, Diane; Schubiger, Maximilian 2024. ***Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, Anderes, 1994 - 2020***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 24.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
ETH	Eidgenössische Technische Hochschule
EU	Europäische Union
MROS	Meldestelle für Geldwäscherei
SVS	Sicherheitsverbund Schweiz
SISA	Swiss Internet Security Alliance
ISB	Informatiksteuerungsorgan des Bundes
MELANI	Melde- und Analysestelle Informationssicherheit
IKT	Informations- und Kommunikationstechnologien
MERCOSUR	Gemeinsamer Markt des Südens
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
CYD	Cyber-Defence Campus

DFF	Département fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
EPF	École polytechnique fédérale
UE	Union européenne
MROS	Bureau de communication en matière de blanchiment d'argent
RNS	Réseau national de sécurité
SISA	Swiss Internet Security Alliance
UPIC	Unité de pilotage informatique de la Confédération
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
TIC	Technologies de l'information et de la communication
MERCOSUR	Marché commun du Sud
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération (à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)
CYD	Campus cyberdéfense

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Rechtsordnung

ANDERES
DATUM: 26.04.2017
MAXIMILIAN SCHUBIGER

Nach der Veröffentlichung der Wirksamkeitsüberprüfung der ersten nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken beschloss der Bundesrat, dass er eine Nachfolgestrategie ausarbeiten möchte. Noch während des letzten Jahres im Zyklus der ersten NCS wurde also die **2. NCS-Strategie** lanciert. Der Schutz vor Cyberkriminalität aller Art sei nach wie vor wichtig, so die Regierung in ihrer Medienorientierung. Vorfälle sowohl in der Schweiz als auch im Ausland zeigten, dass auch kritische Strukturen angegriffen würden und dass Cyber-Angriffe auch für politische Zwecke eingesetzt würden. Die Beurteilung der ersten Strategie 2012–2017 habe gemäss Bundesrat zur Erkenntnis geführt, dass erst ein Fundament habe gelegt werden können, der Schutz jedoch noch ausgebaut werden müsse.
So wurde die Verwaltung beauftragt, eine Nachfolgestrategie für die Jahre 2018 bis 2023 auszuarbeiten, die innert eines Jahres der Regierung unterbreitet werden sollte. Aufbauend auf geschaffenen Strukturen und Prozessen soll der Schutz vor Cyber-Risiken weiter verstärkt werden. Dafür sollen die 30 Stellen weiterhin finanziert und unbefristet verlängert werden. Die Federführung der Arbeiten lag beim ISB. [1]

Äussere Sicherheit

ANDERES
DATUM: 18.04.2018
MAXIMILIAN SCHUBIGER

Pünktlich, wie vom Bundesrat gefordert und per Frühling 2018 angekündigt, konnte die **2. NCS verabschiedet** werden. Im April wurde das Papier, das aufzeigt, wie der Bund gemeinsam mit den Kantonen, der Wirtschaft und der Wissenschaft Cyber-Risiken entgegentreten will und welche Handlungsvorgaben für den angestrebten Zeitraum von fünf Jahren gefasst wurden, vom Bundesrat verabschiedet. Aufbauend auf der ersten Umsetzung der NCS wurden sieben Ziele definiert; sie reichen vom Aufbau von Kompetenzen und Wissen bis zu Massnahmen der Cyber-Abwehr, die durch die Armee sichergestellt werden soll. Diese insgesamt 29 Massnahmen wurden in zehn Handlungsfeldern angelegt, wobei auch neue Aspekte abgedeckt werden. So wurde die Verwaltung beauftragt, im Bereich „Standardisierung und Regulierung" aktiv zu werden, um in Kooperation mit der Wirtschaft Mindeststandards für die Cyber-Sicherheit zu etablieren. Ferner sollen sogenannte Cyber-Vorfälle fortan systematisch registriert werden, wofür die Einführung einer Meldepflicht geprüft werden soll. Auch diese Strategie wird in regelmässigen Abständen überprüft, nötigenfalls angepasst und spätestens 2022 aktualisiert. Nur falls es die Bedrohungslage erfordert, wird eine vorzeitige Aktualisierung ins Auge gefasst, nicht jedoch ohne die betroffenen Stellen vorgängig anzuhören. Für die Realisierung und Anwendung der neuen Strategie soll ein Umsetzungsplan erarbeitet werden. Fünf Herausforderungen wurden bereits erkannt: Es braucht zunächst eine klare Verteilung der Verantwortlichkeiten und Kompetenzen innerhalb der Bundesverwaltung. Zweitens muss geprüft werden, ob die geltende Rechtsetzung allenfalls angepasst werden muss, und falls dem so ist, müssen Gesetzesrevisionen über die üblichen Prozesse in die Wege geleitet werden, was unter Umständen viel Zeit in Anspruch nehmen kann. Als drittes gilt es, die Zusammenarbeit mit den Partnern aus der Wirtschaft und den Hochschulen, aber auch den Kantonen, zu definieren. Viertens braucht es messbare Leistungsziele, um den Umsetzungsfortschritt der Strategie nachvollziehen und transparent beurteilen zu können. Die allfällige vorzeitige Aktualisierung bedarf, fünftens, klarer Vorgaben und Kriterien: Die Umstände für eine Anpassung müssen ebenso wie die Verantwortlichkeiten festgelegt werden. [2]

Datenschutz und Statistik

ANDERES
DATUM: 11.04.2014
NADJA ACKERMANN

Im April 2014 sorgte die Aufdeckung einer **Sicherheitslücke bei der weitverbreiteten Verschlüsselungssoftware Open SSL** für Aufregung. Durch das „**Heartbleed**" genannte Leck konnten Kriminelle an sensible Daten wie Passwörter gelangen. Betroffen waren viele Dienstleistungsanbieter wie Krankenversicherer, Banken, Webshops, Google und Yahoo. Nachdem die Sicherheitslücke wohl zwei Jahre bestanden hatte, konnte sie bei den betroffenen Banken in der Schweiz innerhalb eines Tages geschlossen werden. [3]

Innere Sicherheit

ANDERES
DATUM: 04.05.2017
MAXIMILIAN SCHUBIGER

Der **Sicherheitsverbund Schweiz** (SVS) hat im ersten Halbjahr 2017 **zwei Veranstaltungen** durchgeführt. Anfang April fand zum fünften Mal die Cyber-Landsgemeinde statt. In Bern trafen sich etwa 100 Vertrererinnen und Vertreter von Bund und Kantonen, um über die NCS zu diskutieren. Im Fokus standen dabei die Cyberkriminalität und Cybersicherheit.

Die NCS stand auch bei der dritten Konferenz des SVS im Zentrum der Aufmerksamkeit. Rund 400 Personen waren für diesen Anlass zusammengekommen, bei dem ebenfalls der Schutz vor Cyberrisiken sowie die Sicherheit im Cyberbereich thematisiert wurden. Da die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken Ende 2017 auslief, stellte sich die Frage nach der künftigen Ausgestaltung der Cyber-Abwehr. Der Verteidigungsminister hatte dabei Gelegenheit, die neue Cyberverteidigungsstrategie vorzustellen, die das VBS erarbeitete. [4]

ANDERES
DATUM: 26.04.2018
MAXIMILIAN SCHUBIGER

2018 fand die **sechste Cyber-Landsgemeinde des Sicherheitsverbundes Schweiz** statt. Die Nachfolgearbeiten der ersten NCS standen dabei im Zentrum: Im Zuge der Aufarbeitung der 16 Massnahmen aus der ersten Strategie wurde den Teilnehmenden aus Bund, Kantonen und der Privatwirtschaft aufgezeigt, welche Themen für die NCS II relevant sein werden; gleichzeitig wurden sie in die Erarbeitung dieser Nachfolgestrategie involviert. Weitere Themen waren die Entwicklung und Einführung von Minimalstandards im IKT-Bereich, neue Arten der Cyberkriminalität und die Schwierigkeiten, diese zu erkennen und zu bekämpfen, die Reduktion von IKT-Verwundbarkeiten und, damit zusammenhängend, eine verbesserte Resilienz. Als Herausforderung galten ferner auch die Bedeutung einer korrekten Erkennung und Einschätzung der Bedrohungen aus dem Cyberraum und die geeignete Handhabung dieser Gefährdung. [5]

ANDERES
DATUM: 26.05.2019
MAXIMILIAN SCHUBIGER

Im März 2019 fand die **7. Cyber-Landsgemeinde des Sicherheitsverbundes Schweiz** statt. Im Zentrum der Veranstaltung und des Interesses stand die im April des Vorjahres vom Bundesrat verabschiedete zweite Nationale Strategie zum Schutz vor Cyberrisiken (NCS). Auf dem Programm der Konferenz stand eine Reihe von Themen aus der Umsetzungsagenda, beispielsweise die Risikoanalyse zur Verbesserung der IKT-Resilienz oder die Ausgestaltung einer übergreifenden Austauschplattform zu aktuellen Bedrohungen aus dem Cyber-Raum. Die institutionalisierte Einbindung der Kantone in die Organisationsstruktur für Cyber-Sicherheit auf Stufe Bund stellte gar eines der Kernthemen dar, mit denen sich der SVS über die vergangenen Jahre beschäftigt hatte.

Im Mai stand ferner die **vierte Konferenz des Sicherheitsverbundes Schweiz** an. Der Fokus des Zusammentreffens verschiedener Akteure lag auf der Zusammenarbeit zwischen staatlichen Sicherheitsorganen und privaten Unternehmen. Mit Verweis auf die bisherigen Erfahrungen wurde festgehalten, dass auch staatliche Sicherheitsakteure auf private Dienstleister zurückgreifen. Diese hätten die Kapazitäten, um die staatlichen Organe zu ergänzen, wurde betont. In Anwesenheit von Bundesrätin Karin Keller-Sutter konnten die Kantone Erfahrungen austauschen, aber auch ihre Vorstellungen äussern. So pochte Regierungsrat Norman Gobbi (TI, lega) auf eine flexible Gesetzgebung, die dem Subsidiaritätsprinzip gerecht werde und den Kantonen in den betreffenden Feldern ihre Kompetenzen überlässt. [6]

Kriminalität

ANDERES
DATUM: 07.10.1994
HANS HIRTER

Die 1991 vom Bundesrat beantragte **Strafrechtsrevision** in bezug auf strafbare Handlungen gegen das Vermögen und auf Urkundenfälschung konnte **abgeschlossen** werden. In der Differenzbereinigung schloss sich der Nationalrat weitgehend den Entscheiden der kleinen Kammer an. [7]

ANDERES
DATUM: 08.05.2014
NADJA ACKERMANN

Trotz eines leichten Rückgangs war auch im Jahr 2013 die Anzahl der gemeldeten, verdächtigen Vermögenswerte hoch. Ihr Umfang belief sich auf knapp drei Milliarden CHF, wobei insgesamt 30 Verdachtsmeldungen Summen von über 10 Millionen CHF betrafen. Meist handelte es sich bei der mutmasslich begangenen Vortat zur **Geldwäscherei** um Betrug, wobei eine Zunahme von Computerbetrugsfällen verzeichnet wurde. Die Abnahme der Fälle erlaubte eine vertiefte Analyse der eingegangenen Verdachtsmeldungen und raschere und besser fundierte Meldungen an die Strafverfolgungsbehörden. Dies hielt der im Mai 2014 veröffentlichte Jahresbericht der Meldestelle für Geldwäscherei (MROS) fest. [8]

ANDERES
DATUM: 11.09.2014
NADJA ACKERMANN

Im September 2014 gründeten Vertreter der Wirtschaft die branchenübergreifende **Swiss Internet Security Alliance** (SISA), um die Sicherheit von Schweizer Online-Angeboten auch in Zukunft zu gewährleisten. Der Verein, dem unter anderem Swisscom, UBS, Switch und PostFinance angehören, folgt dem Ruf nach einer verstärkten Zusammenarbeit bei der Bekämpfung der Internetkriminalität. Zu diesem Zweck bietet SISA einen kostenlosen Swiss Security Check an, der Problemstellen aufdecken soll. [9]

Institutionen und Volksrechte

Regierungspolitik

ANDERES
DATUM: 14.11.2018
MARC BÜHLMANN

Auch **2018** trafen sich die Partei- und Fraktionsspitzen der Regierungsparteien mit Vertretungen der Landesregierung zu den **Von-Wattenwyl-Gesprächen**. Die Gespräche finden seit Jahren jeweils vor den Parlamentssessionen statt und sollen informelle Diskussionen zu wichtigen aktuellen politischen Themen erlauben.
Anfang Februar tauschten sich die Präsidien der Regierungsparteien mit dem Bundespräsidenten Alain Berset, mit Bundesrätin Doris Leuthard und Bundesrat Ignazio Cassis sowie Bundeskanzler Walter Thurnherr über den Strommarkt und die Europapolitik aus. Im Zentrum der Diskussion standen dabei die im Rahmen der Revision des Stromversorgungsgesetzes anvisierte Planung der Versorgungssicherheit mit Strom sowie die geplanten Schritte zu den Beziehungen mit der EU. Intensive Debatten habe es zur Frage der dynamischen Rechtsübernahme bei einem allfälligen Rahmenabkommen gegeben, liess sich der Medienmitteilung entnehmen.
Bei den Gesprächen vor der Frühlingssession wurde der Bundespräsident von Bundesrat Ueli Maurer und erneut vom Bundeskanzler begleitet. Thema war die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), deren Verantwortung beim EFD lag. Die Gesprächsteilnehmenden waren sich einig, dass es hier Zusammenarbeit zwischen allen Departementen und in den Bereichen Cyber-Sicherheit, Cyber-Strafverfolgung und Cyber-Defense brauche. Erneut wurde zudem über die Beziehungen zur EU diskutiert. Die Regierung präsentierte die umstrittene Schiedsgerichtslösung zur Streitbeilegung und bekräftigte ihren Willen, die flankierenden Massnahmen zur Personenfreizügigkeit aufrecht erhalten zu wollen. Der Bundesrat informierte zudem über den Stand der Agrarpolitik 2022 (AP22+). Der dafür verantwortliche Bundesrat, Johann Schneider-Ammann war nicht anwesend, weil er auf einer Reise in die Mercosur-Staaten war.
Ende August fanden die Gespräche – wie einmal pro Jahr üblich – in Form einer Klausur statt. Der Bundesrat trat in corpore an und die einzelnen Magistratinnen und Magistraten stellten die Schwerpunkte ihrer Departemente und die Jahresziele 2019 vor. Auch in Klausur waren die Verhandlungen über ein institutionelles Abkommen mit der EU wichtiges Diskussionsthema.
Dies galt auch für die Gespräche vom 9. November. Erneut war deshalb neben Bundespräsident Alain Berset und Bundeskanzler Walter Thurnherr auch Aussenminister Ignazio Cassis anwesend, begleitet von Johann Schneider-Ammann, der über die Herausforderungen der Aussenhandelspolitik etwa auch aufgrund der Neuorientierung der Handelspolitik der USA berichtete. Beim Rahmenabkommen betonten alle Parteien, dass die roten Linien eingehalten werden müssten. Auch der

Migrationspakt war Gegenstand der Gespräche.

Ende September 2018 hatte Nationalrätin Sibel Arslan (basta, BS) eine Interpellation eingereicht (Ip. 18.3953), mit der sie anfragte, weshalb die Nicht-Regierungsparteien (GP, GLP, BDP), die immerhin rund 16 Prozent der Wählerinnen und Wähler vertreten, nicht zu den Gespräche eingeladen werden. Der Bundesrat schaffe hier eine Zweiklassengesellschaft und überdies hätten die Gespräche keine rechtliche Grundlage. In seiner Antwort – kurz nach den letzten von-Wattenwyl-Gesprächen vom 9. November – machte der Bundesrat deutlich, dass für ihn der Austausch mit allen Parteien von Bedeutung sei, dass es aber für die Regierungsparteien und ihre Bundesrätinnen und Bundesräte die Möglichkeit für einen vertieften Dialog geben müsse, um politische Spielräume ausloten zu können. Die nicht an den Gesprächen beteiligten Fraktionen werden nachträglich mit den Unterlagen für die Gespräche bedient. [10]

Landesverteidigung

Landesverteidigung

ANDERES
DATUM: 11.12.2020
DIANE PORCELLANA

L'introduction d'une **obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques** sera soumise à consultation. Avec cette décision, le Conseil fédéral matérialise la mesure formulée dans la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 et fait écho au postulat d'Edith Graf-Litscher (ps, TG). Pour ce faire, le DFF est chargé de soumettre un projet de loi déterminant les types d'incidents à signaler, les délais et les concernés par l'obligation. Les dispositions concrètes relatives à l'obligation de déclarer figureront dans des actes législatifs distincts en fonction de la situation spécifique des secteurs concernés. Si les adaptations législatives devaient être saluées lors de la consultation et approuvées par la suite, les données récoltées dans le cadre de l'obligation permettraient de diffuser des alertes rapides, de renforcer la sécurité et une meilleure évaluation des menaces. [11]

Landesverteidigung und Gesellschaft

ANDERES
DATUM: 07.11.2019
DIANE PORCELLANA

Le **Campus cyberdéfense** (CYD), fruit du partenariat entre le DDPS et l'ETH, a été inauguré. Ce partenariat fait partie du plan d'action pour la cyberdéfense et de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Outre la création de synergies entre l'industrie militaire, le monde académique et les communautés de hackers, la plateforme permettra d'anticiper, d'identifier et d'évaluer les tendances technologiques, commerciales et sociétales du cyberespace. [12]

Militärorganisation

ANDERES
DATUM: 09.11.2017
MAXIMILIAN SCHUBIGER

Seit einigen Jahren arbeitet der Bund, gemeinsam mit mehreren weiteren Akteuren, an verschiedenen Programmen zur Bewältigung neuer Bedrohungen aus dem digitalen Raum. Diesen als „Cyber-Risiken" umschriebenen, im Zuge der Digitalisierung vermehrt auftretenden Komplikationen und/oder Angriffen wird unter anderem auch mit einer Cyber-Strategie begegnet. Diese Strategie wird dezentral umgesetzt, wobei die Melde- und Analysestelle Informationssicherung (MELANI) eine zentrale Rolle innehat. Damit ist aufgrund des Kooperationsmodells bei MELANI zwischen ISB und NDB direkt auch der Nachrichtendienst des Bundes involviert. Innerhalb des VBS hat aber auch die Armee den Auftrag, sensible IT-Infrastrukturen und Systeme zu schützen. Dafür wurde bis anhin auf die Nutzung sicherer Netze vertraut, gerade auch im militärischen Tagesbetrieb. Zur Informations- und Objektsicherheit wurde zudem innerhalb des Verteidigungsdepartementes eine gleichnamige Stelle eingerichtet. Um nun der weiteren Entwicklung im Cyberbereich zu begegnen, wurde ein **Aktionsplan Cyber-Defence** ausgearbeitet. Diese auf Anregung von Departementsvorsteher Guy Parmelin 2016 lancierte Massnahme soll bis 2020 umgesetzt werden und die bereits laufenden Vorgänge im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken ergänzen.

Der Aktionsplan Cyber-Defence ist ein rein auf das VBS bezogenes Strategiepapier, das mit einer Standortbestimmung im Sommer 2016 angestossen worden war und im folgenden Herbst eine Strategie hervorgebracht hatte, deren Umsetzungsplan im Sommer 2017 verabschiedet wurde. Gemäss dem Aktionsplan ist dieser vorerst als

Orientierungshilfe anzusehen, er bedeute jedoch einen zwingenden ersten Schritt, weil eine Anpassung an neue „Herausforderungen im Cyber-Raum ein wichtiges Thema unserer Sicherheitspolitik geworden ist."
Als operative Ziele wurden drei Bereiche definiert. Das VBS soll erstens seine eigenen Systeme und Infrastrukturen jederzeit schützen und verteidigen können. Zweitens soll es möglich werden, militärische und nachrichtendienstliche Operationen im Cyber-Raum durchzuführen. Ferner sollen drittens zivile Behörden im Falle von Cyber-Angriffen unterstützt werden können. Diese Zielvorgaben verlangen jedoch eine genügende Ausstattung mit finanziellen, aber auch personellen Ressourcen – ein Unterfangen, das auf der politischen Bühne auszutragen sein wird.

Die Rekrutierung von geeignetem Milizpersonal beispielsweise mittels neu zu schaffender Cyber-RS, wie im Parlament inzwischen gefordert wurde, wurde im Aktionsplan als nicht zielführend beschrieben. Im Papier ist von einem Bedarf von 166 Stellen die Rede, wovon etwa 100 neu zu schaffen wären. Bezüglich Finanzierung wurden keine präzisen Zahlen genannt, eine Schätzung geht jedoch von etwa 2 Prozent des Jahresbudgets des VBS aus. Ob der gesamte Bereich der Cyber-Abwehr, also auch ausserhalb des VBS und der Armee, durch ein Cybersecurity-Kompetenzzentrum organisiert werden könnte, wurde im Aktionsplan nicht genauer ausgeführt. Unter der Bezeichnung „CYD-Campus" wurde jedoch eine Plattform zur vertieften Zusammenarbeit skizziert, deren Entwicklung noch abgewartet werden muss. [13]

Bevölkerungsschutz

ANDERES
DATUM: 20.03.2014
MAXIMILIAN SCHUBIGER

Am 20. März 2014 fand die **zweite Cyber-Landsgemeinde** des Sicherheitsverbundes Schweiz (SVS) in Bern statt. Ziel dieses Treffens von rund 70 Vertretern von Bund und Kantonen war es, über den aktuellen Stand der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) zu informieren. Seit Ende 2013 befassen sich vier paritätisch zusammengesetzte Arbeitsgruppen mit der Umsetzung einzelner Massnahmen der Strategie in den Kantonen. Ziel dieser Massnahmen ist es, mittels konkreter Produkte die Kantone zu unterstützen, ihre Widerstandsfähigkeit zu erhöhen und Cyber-Risiken zu reduzieren. Drei Arbeitsgruppen erarbeiten in den Bereichen Risikoanalyse und Präventionsmassnahmen, Incident Management und Krisenmanagement Konzepte, Prozesse und fördern den Zugang zu Expertenwissen. Die vierte Arbeitsgruppe dokumentiert Straffälle und erstellt ein Konzept zur Koordination von interkantonalen Fallkomplexen. Der Sicherheitsverbund Schweiz koordiniert in Zusammenarbeit mit der Koordinationsstelle NCS, die beim Informatiksteuerungsorgan des Bundes angesiedelt ist, die Umsetzung der Strategie auf Stufe der Kantone und der Gemeinden. [14]

ANDERES
DATUM: 30.04.2014
MAXIMILIAN SCHUBIGER

Per Ende April 2014 lag der **Jahresbericht 2013 des Steuerungsausschusses der nationalen Strategie zum Schutz vor Cyber-Risiken** (NCS) vor. Bei vielen der 16 gefassten Massnahmen, vor allem in den Bereichen Prävention und Reaktion, wurden Ende 2013 bereits erste Meilensteine erreicht. So wurden die notwendigen Schritte zur Erstellung eines Lagebildes, das über die Cyber-Bedrohungen Auskunft geben wird, eingeleitet. In den beteiligten Verwaltungseinheiten beim Bund wurden auch nötige, neue Organisationsstrukturen geschaffen, um Cyber-Bedrohungen rasch erkennen zu können und die Handlungsfähigkeit zu erhöhen. Es wurden Grundlagen für die Zusammenarbeit geschaffen sowie einheitliche Methoden unter den beteiligten Stellen etabliert, damit im Falle von Cyber-Angriffen optimal reagiert und Schäden und Auswirkungen möglichst gering gehalten werden können.
Im Rahmen der Mitte 2012 gestarteten NCS verfolgt der Bundesrat drei strategische Ziele: die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich, die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen sowie eine wirksame Reduktion von Cyber-Risiken. Die Koordination der Umsetzungsarbeiten übernahm die bei der Melde- und Analysestelle Informationssicherung (MELANI) angesiedelte Koordinationsstelle NCS. Dort werden die Umsetzungsarbeiten überwacht und für den Einbezug aller Beteiligten gesorgt. Zusammen mit den verantwortlichen Bundesämtern wurden die Meilensteine und der Zeitplan für die jeweiligen Massnahmen definiert und in einer Roadmap festgehalten. [15]

Bildung, Kultur und Medien

Medien

Neue Medien

ANDERES
DATUM: 05.06.2000
ELISABETH EHRENSPERGER

Im Mai hatte der Virus **„I love you"** einen grossen Teil der Kommunikation in der Bundesverwaltung für einen Tag lahmgelegt; zwischen 400 und 500 Personalcomputer waren laut Bundesamt für Informatik infiziert und deren Festplatten vollständig gelöscht worden. Der Virusangriff habe die Verwaltung damit rund eine Mio Fr. gekostet. Über mögliche durch „I love you" in der Privatwirtschaft verursachte Schäden hielt sich diese aus Imagegründen – um nicht heikle Lücken in ihrem Sicherheitsdispositiv preisgeben zu müssen – bedeckt. [16]

ANDERES
DATUM: 24.10.2000
ELISABETH EHRENSPERGER

Im Versuch, gegen **illegale Inhalte im Internet** anzukämpfen, verabschiedete die Bundespolizei (Bupo) im April Verhaltensgrundsätze, die abgestützt auf ein Rechtsgutachten des Bundesamts für Justiz den Providern als private Anbieter elektronischer Dienstleistungen eine aktive Rolle beim Kampf gegen illegale Websites-Inhalte zuteilten. So sollten Provider, die den Nutzerinnen und Nutzern den Zugang zum Internet verschaffen, bei Erhalt eines Hinweises der Strafverfolgungsbehörden illegale Netzinhalte sperren. Das Gutachten baute auf einem Bundesgerichtsentscheid von 1999 auf, das einen Buchhändler mit der Begründung verurteilt hatte, bei Rassendiskriminierung und harter Pornographie seien nicht nur der Autor, sondern auch weitere Verbreiter strafbar. Das Positionspapier der Bupo drohte, eine einvernehmliche Lösung mit den Providern zu verhindern. Da nach wie vor zahlreiche rechtliche Fragen offen standen, liess der Verband Inside Telecom (VIT), Vertreter der Provider, ein Zweitgutachten erstellen. Die Professoren Marcel Niggli, Franz Riklin und Günter Stratenwerth orteten eine eklatante Rechtsunsicherheit, welche die Dringlichkeit gesetzlicher Regelungen spiegelten. Der Unmut der Provider über das Bupo-Papier gründete insbesondere in den Befürchtungen, einerseits eine eigene Überwachungspolizei aufbauen zu müssen und andererseits durch allzu strenge nationale Gesetze einen Standortnachteil im internationalen Umfeld zu erleiden. [17]

---

1) Medienmitteilung Bundesrat vom 26.04.2017
2) Bericht NCS 2018-2022; Medienmitteilung Bundesrat vom 19.04.2018
3) AZ, 11.4.14
4) Medienmitteilung BR vom 4.5.17; Medienmitteilung BR vom 5.4.17
5) Medienmitteilung BR vom 26.4.18
6) Medienmitteilung SVS vom 16.5.19; Medienmitteilung SVS vom 28.3.19; Umsetzungsplan SVS Kantone
7) AB NR, 1994, S. 1250; AB NR, 1994, S. 329 ff.; AB NR, 1994, S. 869 ff.; AB SR, 1994, S. 1074; AB SR, 1994, S. 14 ff.; AB SR, 1994, S. 430 f.; AB SR, 1994, S. 582; AB SR, 1994, S. 775; AB SR, 1994, S. 880; BBl, 1994, III, S. 256 ff.
8) Lit. Fedpol 2014; Medienmitteilungen Fedpol vom 8.5.14.pdf
9) Medienmitteilung NCSC (damals Melani) vom 11.9.14
10) Ip. 18.3953; Medienmitteilung BR vom 2.2.18; Medienmitteilung BR vom 31.8.18; Medienmitteilung BR vom 4.5.18; Medienmitteilung BR vom 9.11.18
11) Communiqué de presse du DDPS du 11.12.20
12) Communiqué de presse du DDPS du 7.11.2019; AZ, 20.3.19; LT, 28.11.19; NZZ, 6.12.19
13) Aktionsplan Cyberdefence
14) Medienmitteilung VBS vom 20.3.14.pdf
15) Jahresbericht Steuerungsausschuss NCS 2013.pdf; Medienmitteilung VBS vom 30.4.14.pdf
16) NF, 5.6.00.
17) BZ, 10.5.00; 24h, 16.5.00; Presse vom 16.5. und 24.10.00; NZZ, 19.5.00.