année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Dossier **Dossier: Cyber Defence**

Impressum

Herausgeber

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

Beiträge von

Ackermann, Marco
Ackermann, Nadja
Baltisser, Lena
Lütolf, Lukas
Magnin, Chloé
Porcellana, Diane
Schubiger, Maximilian
Schär, Suzanne

Bevorzugte Zitierweise

Ackermann, Marco; Ackermann, Nadja; Baltisser, Lena; Lütolf, Lukas; Magnin, Chloé; Porcellana, Diane; Schubiger, Maximilian; Schär, Suzanne 2025. ***Ausgewählte Beiträge zur Schweizer Politik: Dossier: Cyber Defence, 2010 - 2024***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 23.08.2025.

Inhaltsverzeichnis

Massnahmen gegen Cyberwar (Mo. 10.3625) 1
Präventive Gefahrenabwehr im Bereich Cyber-Bedrohung (Po. 10.3910) 1
Schutz der digitalen Infrastruktur (Po. 10.4102) 1
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2
Cyber-Landsgemeinden und Konferenzen des Sicherheitsverbunds Schweiz 3
Zweite Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 5
Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund (Mo. 17.3508) 6
Cyberdefence-Kommando (Mo. 17.3507) 7
Aktionsplan Cyber-Defence 9
Meldepflicht bei kritischen Infrastrukturen (Po. 17.3475) 10
Cyberrisiken. Für einen umfassenden, unabhängigen und wirksamen Schutz (Po. 16.4073) 11
Ausbau der Cyberabwehrkompetenzen (Mo. 17.3199) 12
Eine klare Cyber-Gesamtstrategie für den Bund (Po. 18.3003) 13
ICT Empfehlungen Bund (Cyber) 14
Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff? (Po. 19.3136) 14
Cyber-Defence Campus 15
Obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques 15
Institutionnaliser le piratage éthique et améliorer la cybersécurité (Po 20.4594) 15
Modification de loi sur l'armée et de l'organisation de l'armée (OCF 21.061) 16
Massnahmen für einen besseren Schutz gegen Ransomware-Angriffe (Po. 21.4512) 18
Cyberexercices-stratégie générale pour la Suisse (Mo. 22.3836) 19

Abkürzungsverzeichnis

EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
SiK-SR	Sicherheitspolitische Kommission des Ständerates
ETH	Eidgenössische Technische Hochschule
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
SVS	Sicherheitsverbund Schweiz
ISB	Informatiksteuerungsorgan des Bundes
MELANI	Melde- und Analysestelle Informationssicherheit
IKT	Informations- und Kommunikationstechnologien
AdA	Angehörige(r) der Armee
BWL	Bundesamt für wirtschaftliche Landesversorgung
RS	Rekrutenschule
MG	Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
AO	Verordnung der Bundesversammlung über die Organisation der Armee
CYD	Cyber-Defence Campus
NCSC	Nationales Zentrum für Cybersicherheit
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
ICT	Informations- und Kommunikationstechnik, IKT (= Information and communications technology, ICT)
USA	United States of America
KKM SVS	Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz

---

DFF	Département fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
EPF	École polytechnique fédérale
CPS-CN	Commission de la politique de sécurité du Conseil national
RNS	Réseau national de sécurité
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
Militaire	Militaire
OFAE	Office fédéral pour l'approvisionnement économique du pays
ER	École de recrues
LAAM	Loi fédérale sur l'armée et l'administration militaire (Loi sur l'armée)
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)
OOrgA	Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée
CYD	Campus cyberdéfense
NCSC	Centre national pour la cybersécurité
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
TIC	Technologies de l'information et de la communication
USA	United States of America
MCC RNS	Mécanisme de consultation et de coordination du Réseau national de sécurité

Massnahmen gegen Cyberwar (Mo. 10.3625)

Neue Medien

MOTION
DATUM: 02.12.2010
SUZANNE SCHÄR

Die grosse Kammer nahm im Dezember eine Motion der Sicherheitskommission (SiK-NR) des Nationalrats an. Darin wird die Vorbereitung von Gesetzesgrundlagen verlangt, welche die **Sicherung wichtiger ziviler und militärischer Daten(-Netzwerke)** erlauben und regeln. Die Veröffentlichung geheimer Protokolle aus dem Irakkrieg und diplomatischer Depeschen der USA im Oktober 2010 durch die Enthüllungsplattform Wikileaks intensivierten gegen Ende Jahr den öffentlichen Diskurs um die Datensicherheit im Internet. Im Dezember gab der Bundesrat die Einsetzung einer Arbeitsgruppe bekannt, die eine Strategie zur Abwehr von Internetangriffen (Cyber-Defense) zu erarbeiten hat. Bis Ende 2011 soll sie zudem die Bündelung der zwölf dezentralen, mit Cyber-Defense beauftragten Verwaltungsstellen prüfen. [1]

MOTION
DATUM: 15.03.2011
MAXIMILIAN SCHUBIGER

Anfang Juni 2010 hatte der Ständerat ein Postulat Recordon (gp, VD; Po. 10.3136) überwiesen, welches den Bundesrat beauftragt einen Bericht zu erarbeiten, wie er dem Cyberwar zu begegnen gedenke. Ende Juni desselben Jahres wurde von der SiK-NR unter dem Titel **Massnahmen gegen Cyberwar** eine Motion mit ähnlichem Inhalt eingereicht (Mo. 10.3625). Diese beauftragt den Bundesrat mit der Erarbeitung gesetzlicher Grundlagen für Massnahmen zur Sicherung und Verteidigung von Datennetzwerken, die für die Schweiz und für schweizerische Einrichtungen von Bedeutung sind. Vom Nationalrat wurde die Motion in der Wintersession 2010 überwiesen. Nachdem auch der Bundesrat Anfang 2011 die Annahme der Motion beantragte, folgte der Ständerat mit dem gleichen Votum im März 2011. [2]

MOTION
DATUM: 15.03.2011
NADJA ACKERMANN

In diesem Sinne unterstützte der Bundesrat auch eine allgemeingefasste Motion der sicherheitspolitischen Kommission des Nationalrates, die die Regierung beauftragt, eine gesetzliche Grundlage für die **Sicherung und Verteidigung wichtiger Schweizer Datennetzwerke** zu schaffen. Nachdem die Motion von der grossen Kammer 2010 überwiesen worden war, folgte nun auch der Ständerat dem Antrag seiner Kommissionsmehrheit und nahm die Motion an. [3]

Präventive Gefahrenabwehr im Bereich Cyber-Bedrohung (Po. 10.3910)

Innere Sicherheit

POSTULAT
DATUM: 18.03.2011
NADJA ACKERMANN

Konkreter war ein Postulat der FDP-Liberale-Fraktion, welches die Schaffung einer Leit- und Koordinationsstelle für die präventive Gefahrenabwehr im Bereich **Cyber-Bedrohung** vorsieht und vom Nationalrat überwiesen wurde. [4]

Schutz der digitalen Infrastruktur (Po. 10.4102)

Innere Sicherheit

POSTULAT
DATUM: 18.03.2011
NADJA ACKERMANN

Für die Eindämmung der Gefahren, die vom Internet ausgehen, sprach sich auch der Nationalrat aus. So hiess er ein Postulat Darbellay (cvp, VS) gut, welches den Bundesrat beauftragt, ein Konzept zum **Schutz der digitalen Infrastruktur** der Schweiz vorzulegen. In seiner Stellungnahme erklärte der Bundesrat, dass er sich der Bedeutung von Cyber-Bedrohungen bewusst sei und er deshalb beschlossen habe, die Federführung für das Thema Cyber Defense auf Stufe Bund dem VBS zu übertragen. Am 10. Dezember 2010 war für eine befristete Zeit ein Projektleiter in der Person von Divisionär Kurt Nydegger gewählt worden. Ein Strategiepapier zur Cyber Defense soll im Frühling 2012 vorliegen. Im Verlaufe des Jahres zeigte sich, dass Ueli Maurer und seine Spezialisten eine Kooperation mit dem Nato Cooperative Cyber Defence Centre in der estnischen Hauptstadt Tallinn anstreben. [5]

POSTULAT
DATUM: 23.12.2011
SUZANNE SCHÄR

In der Frühlings- und in der Dezembersession nahm der Nationalrat stillschweigend zwei Postulate an, die den Schutz der digitalen Infrastruktur einerseits und den Schutz ihrer Nutzer andererseits forderten. Ein Postulat Darbellay (cvp, VS) wünschte – unter Einbezug aller Sicherheitskräfte, einschliesslich der Armee – die Erarbeitung eines Konzepts zum Schutz der digitalen Infrastrukturen der Schweiz. Das Postulat Schmid-Federer (cvp, ZH) (11.3906) verlangte vom Bundesrat die **Prüfung eines umfassenden Grundlagengesetzes für die Datenverkehrsnetze** (IKT-Grundlagengesetz). [6]

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Bevölkerungsschutz

VERWALTUNGSAKT
DATUM: 27.06.2012
MAXIMILIAN SCHUBIGER

Ende Juni legte der Bundesrat eine **nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken** vor. Eine neu geschaffene Koordinationsstelle innerhalb des eidgenössischen Finanzdepartementes soll die Umsetzung begleiten. In der Strategie wird dargelegt, wie die Bedrohungslage im Cyber-Bereich aussieht, wie die Schweiz, beziehungsweise die Betreiber der kritischen Infrastrukturen, dagegen gerüstet sind, wo die Mängel liegen und wie diese am effizientesten und wirksamsten zu beheben sind. Die Massnahmen reichen dabei von Risikoanalysen zu kritischen ICT-Infrastrukturen bis zu einer stärkeren Einbringung der Schweizer Interessen in diesem Bereich auf internationaler Ebene. Dabei geht der Bundesrat davon aus, dass via elektronische Netzwerke ausgeführte Störungen, Manipulationen und gezielte Angriffe tendenziell zunehmen werden. Der Krisenfall wird durch einen gelungenen Angriff mit erheblichen Konsequenzen beschrieben und verlangt von den involvierten und betroffenen Akteuren ein spezifisches Krisenmanagement. Bis Ende 2017 sollen die verantwortlichen Bundesstellen die Massnahmen im Rahmen ihres Grundauftrags umsetzen. [7]

VERWALTUNGSAKT
DATUM: 27.06.2012
NADJA ACKERMANN

Der Bundesrat verabschiedete am 27. Juni 2012 eine auch durch verschiedene parlamentarische Vorstösse geforderte **nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**. Die Strategie sieht vor, dass die bestehende Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen vertieft wird. Zwar soll zusätzlich zur Melde- und Analysestelle Informationssicherung (MELANI) eine Koordinationsstelle im EFD geschaffen werden, jedoch verzichtet die Regierung auf ein zentrales Steuerungs- und Koordinationsorgan. Die Verantwortung liegt weiterhin bei den Organisationseinheiten, während der Staat nur subsidiäre Aufgaben wie Informationsaustausch und nachrichtendienstliche Erkenntnisse übernimmt. [8]

VERWALTUNGSAKT
DATUM: 15.05.2013
NADJA ACKERMANN

Im Mai 2013 verabschiedete der Bundesrat einen Umsetzungsplan für die im Vorjahr vorgelegte **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken** (NCS). Der bis 2017 laufende **Umsetzungsplan** konkretisiert sechzehn Massnahmen der Strategie und legt die Verantwortlichkeiten fest. Da eine personelle Verstärkung im Fachbereich Cyber nötig ist, beabsichtigte der Bundesrat die Schaffung von 28 Stellen in diesem Bereich. [9]

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. [10]

BERICHT
DATUM: 26.04.2017
MAXIMILIAN SCHUBIGER

Ende April 2017 lag die **Wirksamkeitsüberprüfung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken** wie geplant in Berichtsform vor. Bereits bei der Verabschiedung deren Umsetzungsplans im Jahr 2013 war die Absicht gefasst worden, nach vier Jahren eine Evaluation der NCS vorzunehmen. Dem Bericht konnte entnommen werden, dass die strategische Ausrichtung der NCS richtig gewählt worden war und dass in allen Bereichen funktionierende Prozesse und Strukturen hatten etabliert werden können. Damit könne Spezialwissen gesammelt werden, das die Schweiz besser gegen Cyber-Risiken wappne. Kritisch wurde jedoch auch festgehalten, dass mit der ersten NCS erst quasi ein Fundament gelegt werden konnte, auf dem aufbauend weitere Anstrengungen unternommen werden müssen, um den Schutz im Cyberbereich weiter zu erhöhen.

Im Bericht wurde festgestellt, dass die Schnittstellen zur Armee, also zum Bereich Cyberdefence, noch ungenügend seien. Hier fehle noch eine klarere Abgrenzung und Zuständigkeit zwischen den zivilen Aufgaben der NCS und der Führung durch die Armee, die für den Konfliktfall noch nicht abschliessend geklärt seien. Im Gegensatz hierzu stehen die Schnittstellen zu den Aktivitäten der Kantone (SVS), denen ein besseres Zeugnis ausgestellt werden konnte und wo die Ziele als erreicht deklariert wurden. Insgesamt wurde unterschieden zwischen einer Beurteilung der genannten Schnittstellen und – im Fokus des Berichts – von einzelnen Massnahmen. Die Wirksamkeitsüberprüfung habe gezeigt, dass die in der Umsetzungsplanung beschriebenen Organisationsstrukturen und Prozesse mehrheitlich implementiert werden konnten und dass verschiedene Produkte (Berichte und Konzepte) termingerecht erstellt worden waren. Dies habe «nachweislich zu gestärkten Kapazitäten, breiterem Wissensstand und besserer Koordination in den verschiedenen Bereichen geführt.» Es war also in der Summe ein durchaus positives Zeugnis, das der externe Evaluator hier der NCS ausgestellt hatte. Es zeichnete sich im Laufe des Frühjahres 2017 dann auch ab, dass der Bundesrat eine zweite Strategie NCS anstrebte. [11]

Cyber-Landsgemeinden und Konferenzen des Sicherheitsverbunds Schweiz

Bevölkerungsschutz

INTERKANTONALE ZUSAMMENARBEIT
DATUM: 03.09.2013
MAXIMILIAN SCHUBIGER

Anfang September fand die **erste Konferenz des Sicherheitsverbunds Schweiz** (SVS) statt. An der vom Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) organisierten Konferenz mit Politikern und Vertretern von Polizei, Armee, Feuerwehr, Bevölkerungs- und Zivilschutz standen die Konzeption, Absicht und Perspektiven der sicherheitspolitischen Zusammenarbeit im Verbund zur Diskussion. Eine zentrale Erkenntnis war dabei, dass viele der künftigen Aufgaben im Bereich der öffentlichen Sicherheit nur durch eine gesamtschweizerische Zusammenarbeit bewältigt werden können. Unter der Wahrung des föderalistischen Charakters der Schweiz mit tiefgreifender Autonomie der Kantone soll eine gleichberechtigte Meinungsbildung zwischen Bund und Kantonen eingerichtet werden, so Hans-Jürg Käser (BE, fdp), Präsident der kantonalen Justiz- und Polizeidirektorenkonferenz (KKJPD). Mit regelmässigen Trainings soll in der Schweiz eine nationale Übungskultur etabliert werden, um die Bewältigung komplexer Notlagen zu simulieren. Der KKM SVS wird als geeignetes Instrument betrachtet, um eine bessere Vernetzung der beteiligten Akteure herbei zu führen. [12]

GESELLSCHAFTLICHE DEBATTE
DATUM: 20.03.2014
NADJA ACKERMANN

Im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) auf Stufe der Kantone und der Gemeinden fand im März 2014 in Bern die **zweite Cyber-Landsgemeinde** statt. Ziel des durch den Sicherheitsverbund Schweiz (SVS) organisierten Anlasses war der Austausch über den Umsetzungsstand der Strategie sowie die Koordination des weiteren Vorgehens. Die nächste Cyber-Landsgemeinde soll 2015 stattfinden. [13]

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: 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. [15]

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. [16]

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. [17]

Zweite Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

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. [18]

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. [19]

Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund (Mo. 17.3508)

Äussere Sicherheit

MOTION
DATUM: 19.09.2017
MAXIMILIAN SCHUBIGER

Zeitgleich mit Josef Dittli (cvp, UR) reichte auch Ständerat Eder (fdp, ZG) eine Motion zu Cyber-Fragen ein. Er fokussierte jedoch nicht auf Armeestrukturen, sondern regte generell die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** an. Im Laufe der Überprüfung der NCS solle der Bund Massnahmen in die Wege leiten, um eine solche Organisationseinheit zu schaffen. Eder schwebte eine Koordinationsstelle vor, die bundesweit die Vorgänge im Bereich der Cybersicherheit überwacht und fördert, die jedoch ferner auch eine Weisungsbefugnis gegenüber den Ämtern erhalten solle. Die Notwendigkeit einer solchen Stelle leitete Eder aus früheren parlamentarischen Vorstössen sowie dem Geschäftsbericht des Bundesrates über das vergangene Jahr ab, wo klar geworden sei, dass noch zu wenig für die Cybersicherheit gemacht werde. Wie sein Ratskollege Dittli regte Eder eine Zusammenarbeit mit Wissenschaft und Hochschulen sowie der IT-Branche an.

Der Bundesrat teilte die Auffassung, dass der Cyberbereich eine Koordinationsstelle braucht. Zusammen mit MELANI sei eine solche Stelle jedoch bereits geschaffen worden. Das Know-how sei vorhanden und die geforderte Weisungsbefugnis sei auch bereits erteilt worden. Bei grösseren Cybervorfällen würden departementsübergreifende Task-Forces eingesetzt, um Kräfte zu bündeln. Die Bedrohung werde zunehmen – dessen war sich auch die Regierung sicher – und die Anforderungen an die Durchhaltefähigkeit der zuständigen Stellen steige im Ereignisfall. Ein Koordinationszentrum, wie es in der Motion gefordert wird, sei entsprechend fachlich und personell weiterzuentwickeln. Genau dies werde in der Weiterentwicklung der NCS angestrebt, weswegen der Bundesrat die Ablehnung der Motion beantrage.

Anders sah dies der Ständerat. Die Motion wurde mit 41 zu 4 Stimmen deutlich angenommen. Der Abstimmung ging jedoch eine längere Debatte voraus, die rasch verdeutlichte, dass der Bundesrat allein auf weiter Flur stand. Der Motionär selbst eröffnete die Beratungen mit seiner Erstaunensbekundung: Zwar sage die Regierung, sie wolle die Kompetenzen zur Cyberabwehr verstärken und koordinieren, aber die Motion wolle sie nicht zur Annahme empfehlen. Das passe nicht zusammen und das gehe auch für andere Mitunterzeichnende (22 an der Zahl) nicht auf. Verdeutlichen konnte er sein Anliegen mit eben bekannt gewordenen Angriffen auf zwei Departemente. Die Meinung. dass die Meldestelle MELANI bereits Aufgaben im Cyberbereich wahrnehme, teilte der Motionär nicht. Deren Arbeit stellte er nicht infrage, aber in der noch gültigen Cyberstrategie des Bundes komme das Wort "Cybersecurity-Kompetenzzentrum nicht ein einziges Mal vor." Daraufhin hielt er ein eigentliches Plädoyer für die Sache, man müsse endlich handeln – die beiden ETH stünden bereit. Weitere Redner pflichteten Eder (fdp, ZG) bei. Besonders Vertreter der SP sprachen sich dabei für einen Ausbau der Cyberabwehr aus, durchaus auch zu Lasten von anderen Abwehrprogrammen (Rüstung). Erich Ettlin (cvp, OW) fand die Debatte dann "fast schon langweilig", weil sich alle einig waren. Alle ausser Bundesrat Maurer, der die Regierung vertrat. Sein langes Votum – im Wesentlichen zeigte er die bisher angewendeten Vorgänge und Massnahmen auf und die Tatsache, dass kaum eine Bundesratssitzung ohne Cyber-Thema abgehalten werde – schloss er mit dem Appell, man solle die Regierung und MELANI nicht unterschätzen. Das Plenum wollte jedoch ganz offensichtlich ein Zeichen setzen und die Arbeiten im Cyberbereich dergestalt bündeln, dass eine zentrale Stelle die Koordination übernimmt. [20]

MOTION
DATUM: 07.12.2017
MAXIMILIAN SCHUBIGER

Die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** war im Ständerat kaum bestritten und auch im Vorfeld an die Plenardebatte in der grossen Kammer wurden die Zeichen auf grün gesetzt. Das auf eine Motion Eder (fdp, ZG) zurück gehende Anliegen fand einstimmige Unterstützung in der sicherheitspolitischen Kommission des Nationalrates. Sie kam nach Gesprächen mit Cybersicherheits-Fachpersonen aus der Bundesverwaltung sowie unter Berücksichtigung der bereits laufenden Arbeiten im Bereich der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) und dem entsprechenden Aktionsplan zum Schluss, dass die Motion unterstützt werden soll, denn tiefer greifende Koordination sei im Cyberbereich notwendig. Ein Kompetenzzentrum für Cybersicherheit sei hierzu der richtige Weg.

Kommissionssprecher Glättli (gp, ZH) präzisierte in seiner Einleitung zur Debatte, dass die MELANI nur über beschränkte Personalressourcen verfüge und zudem ihr Auftrag limitiert sei. MELANI, als verwaltungsinterne Koordinationsstelle auch für Cyberkriminalität zuständig, leiste gute Arbeit, so Glättli weiter, es bedürfe aber weiter reichender Kompetenzen für ein eigentliches Kompetenzzentrum. Der anwesende Bundesrat Maurer vertrat auch im Nationalrat die ablehnende Haltung des Siebnerkollegiums: Es werde bereits viel im Cyberbereich unternommen und diverse Expertengruppen würden bald ihre Arbeiten abschliessen. Insofern bat Maurer die Nationalrätinnen und Nationalräte, nicht vorzugreifen. Im Wesentlichen zielten die gegenwärtig angestossenen Prozesse in die gleiche Richtung, wie der Motionär vorgebe, und dies ohne Aufblähung der Verwaltung. Letzteres befürchtete Maurer, falls eine zusätzliche Verwaltungseinheit geschaffen werden müsste. Kommissionssprecher Glättli entgegnete hierauf, dass mit der Motion noch keine operativen Beschlüsse gefasst und die Ausgestaltung und Umsetzung eines solchen Cyber-Kompetenzzentrums Gegenstand weiterer Diskussionen sein würden.
Das Ratsplenum folgte seiner Kommission und hiess die Motion mit 177 zu 2 Stimmen ohne Enthaltungen deutlich gut. [21]

MOTION
DATUM: 28.11.2019
DIANE PORCELLANA

Le Conseil fédéral présente une ébauche de la structure et des tâches du **centre de compétences pour la cybersécurité** dans son rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Trois mesures y sont décrites, afin que l'organisation du centre de compétences réponde aux exigences de centralisation formulées par le Parlement, tout en s'appuyant sur les capacités existantes. Le guichet national devra se créer une aura externe afin d'être perçu comme le guichet unique. Il faudra disposer d'un pool d'experts pour appuyer les offices dans la mise en œuvre des mesures dans le domaine de la cybersécurité. Enfin, pour la réalisation de certaines tâches, le centre de compétences devra collaborer avec les services munis de l'expertise et des capacités nécessaires. [22]

MOTION
DATUM: 10.06.2021
DIANE PORCELLANA

Après l'avoir refusé en 2020, l'Assemblée fédérale a finalement décidé de classer la motion demandant la **création d'un centre de compétence fédéral pour la cybersécurité**, puisque le Conseil fédéral a rempli les objectifs en présentant son rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection contre les cyberrisques.

Cyberdefence-Kommando (Mo. 17.3507)

Äussere Sicherheit

MOTION
DATUM: 25.09.2017
MAXIMILIAN SCHUBIGER

Josef Dittli (fdp, UR) schlug mit seinem Vorschlag, innerhalb der Armee ein **Cyberdefence-Kommando** einzurichten, einen eigentlichen Paradigmenwechsel vor. Bereits seit Jahren war der Bund bestrebt, im Bereich Cyber-Kriminalität neue Wege zu gehen und den sich verändernden technologischen Entwicklungen Rechnung zu tragen, indem beispielsweise die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) lanciert wurde. Eine eigentliche Cyber-Armee wurde jedoch in diesen Prozessen noch nicht konzipiert. Mit der fortschreitenden Digitalisierung und den damit ausgelösten Datenverschiebungen müssen Sicherheitsaspekte im Cyber-Bereich jedoch zunehmend angesprochen sowie entsprechende Massnahmen vorgesehen werden. Dittli wollte innerhalb des VBS und der Armee eine eigene Truppe zur Cyberabwehr aufbauen. Er leitete die Notwendigkeit seines Vorschlags aus dem Verfassungsauftrag an die Armee ab. Ein professionalisiertes Kommando mit 100 bis 150 Cyberspezialisten soll, flankiert von einer 400-600 AdA-starken Cybertruppe, die sensiblen Infrastrukturen schützen. Die Ausbildung dieser Spezialisten soll über eine eigens zu schaffende Cyber-RS erfolgen. Sieben Punkte führte der Motionär an, die eine solche Cyber-Einheit erfüllen können muss: Eigene Systeme jederzeit schützen; eigenständige Cyberoperationen durchführen (z. B. Cyberaufklärung, -verteidigung, aber auch -angriff); den NDB unterstützen; Unterstützungsleistungen weiterer Betreiber kritischer Infrastrukturen; zivile Behörden in Cyberangelegenheiten unterstützen. Dafür soll die Armee einerseits Kooperationen mit dem Forschungsplatz, aber auch dem Hochschulbereich eingehen und andererseits Vorbereitungen treffen, damit eine solche militärische Cyber-Einheit konzipiert werden kann. Dittli schlug also eine

eigentliche Cyber-Armeeeinheit vor, daneben war auch eine Motion von Ständerat Eder (fdp, ZG) hängig, der sich im Cyber-Bereich ein Kompetenzzentrum wünschte. Diese Motion wurde vom Ständerat bereits dem Zweitrat überwiesen.

Der Bundesrat zeigte sich in seiner Antwort auf den Vorstoss skeptisch. Elemente der Zielvorgabe würden gegenwärtig mit einem Aktionsplan Cyberdefence angegangen, dieser erfülle weite Teile der Motion. Bezüglich der Anliegen die Truppe betreffend (Verfügbarkeit, Stärke, Milizprinzip) seien daher die nächsten Schritte in der Umsetzung des Aktionsplans, wie sie bis 2020 vorgesehen sind, abzuwarten. Hinsichtlich der Einrichtung eines eigenen Kommandos zeigte sich die Regierung offener, man müsse aber auch hier abwarten, wie sich solche Leitungsstrukturen in ein Gesamtgefüge integrieren liessen. So sprach sich der Bundesrat noch gegen die Motion aus, hielt sich aber die Möglichkeit offen, bei einer allfälligen Annahme im Erstrat via das VBS zuhanden des Zweitrats noch auf den Motionstext Einfluss zu nehmen.

Die Ratsdebatte wurde mit einem Ordnungsantrag Hêche (sp, JU) eröffnet, der die Motion der zuständigen SiK zur Vorprüfung zuweisen wollte. Hêche wollte nicht mehrspurig fahren und nicht neben den Prozessen um den Aktionsplan des Bundesrates und der zuvor angenommenen Motion Eder (fdp, ZG) zusätzlich auch noch einen Prozess zur Schaffung einer Cyber-Armee anstossen. Der Motionär entgegnete jedoch, dass sich die Ziele der Motion Eder nicht mit denjenigen seiner eigenen überschneiden würden, da er sich eben auf den Bereich Armee beschränke. Im Übrigen hätte sich ja die Regierung offen gegenüber der Motion gezeigt und einzig an der Cyber-RS Anstoss genommen. Der Ordnungsantrag wurde nicht angenommen, damit konnte der Vorstoss materiell behandelt werden.
Der Motionär verteidigte sein Anliegen mit der Einschätzung, dass nicht klar sei, was der Bundesrat und das VBS im Cyber-Bereich erreichen wollen. Zwar werde viel unternommen, auch gerade bezüglich der Rollendefinition der Armee und ihrer Funktionen in der Cyberabwehr, offen sei jedoch, wie die Stärken der Miliz einbezogen werden können. Der Aktionsplan Cyberdefence sei laut Dittli (fdp, UR) „in Ordnung", jedoch sei kaum etwas über seinen Inhalt bekannt. Dass ein wesentlicher Teil seiner Motion bereits in anderen Prozessen umgesetzt wird, begrüsste er, aber das wichtige und titelgebende Anliegen seines Vorstosses, ein Cyber-Kommando in die Armeestrukturen einzubinden, sei eben noch nicht angedacht. Ebenso fehle in der Debatte über die Möglichkeiten, IT-Spezialisten zu finden und auszubilden, die Prüfung einer Cyber-RS. Es gebe schliesslich bereits IT-Spezialisten in den Rechenzentren von Bund und VBS, eine systematische armeenahe Cyber-Ausbildung fehle jedoch komplett. Er sah denn auch einen Steilpass in der geäusserten Bereitschaft der Regierung, im Falle einer Annahme seiner Motion noch Änderungsvorschläge zuhanden der SiK-NR zu machen. Diesen Steilpass müsste der Ständerat „also der Sache zuliebe annehmen". Ratskollege Ettlin (cvp, OW) blies ins gleiche Horn. Es gebe bereits heute monatlich tausende Cyberangriffe auf diverse kritische Strukturen und er finde die Argumentation der Regierung, eine Cyber-RS sei nicht möglich, da sie sich nicht in die bestehenden Ausbildungsmodelle der Armee einfügen lasse, „speziell". Die Annahme neuer Herausforderungen, auch im Bereich (Cyber-)Verteidigung sei wichtig, so der Obwaldner weiter.
Verteidigungsminister Parmelin argumentierte vergeblich mit den bestehenden Arbeiten und der Bereitschaft, den Weg der Cyberabwehr weiter gehen zu wollen. Das Ratsplenum nahm die Motion mit 34 zu 7 Stimmen deutlich an. [23]

MOTION
DATUM: 12.12.2017
MAXIMILIAN SCHUBIGER

Ein **Cyberdefence-Kommando** innerhalb der Strukturen der Armee zu etablieren, stiess bei der SiK des Nationalrates grundsätzlich auf Zustimmung. Jedoch sahen die Sicherheitspolitikerinnen und -politiker noch Präzisierungspotenzial beim Text der Motion Dittli (fdp, UR). So soll statt von einem Kommando von einer «Cyber-Organisation» die Rede sein. Ferner sei der Begriff «Cyber-Bataillon» unzutreffend, weil dadurch suggeriert werde, dass eine autonome Formation errichtet würde. Hingegen sei vorgesehen, dass IT-Spezialisten der Verwaltung und des Militärs zusammen zum Einsatz kommen würden. Schliesslich wollte die Kommission darauf verzichten, eigens eine Cyber-RS durchzuführen. Stattdessen sollten AdA, die ein Talent im Cyber-Bereich hätten, erst später eine armee(fach)spezifische Cyberausbildung erhalten und in einem weiteren Schritt einer Cyber-Einheit zugeteilt werden. Mit diesen Änderungen gelangte die SiK einstimmig ans Ratsplenum.
In der Nationalratsdebatte folgten nur die nötigsten Wortmeldungen. Kommissionssprecher Dobler (fdp, SG) fasste die zentralen Punkte zusammen. Weil die von der Kommission vorgeschlagenen Änderungen vom Bundesrat angeregt worden waren und in der Kommission Einigkeit geherrscht hatte, konnte der St. Galler auf die

Unterstützung seiner Kommissionskolleginnen und -kollegen zählen. Dem Verteidigungsminister blieb nur übrig, die nunmehr von der Regierung mitgetragenen Änderungen zur Annahme zu empfehlen und die Abkehr von der zuvor herrschenden, ablehnenden Meinung bekannt zu geben. In der Folge wurde die Motion im Nationalrat angenommen, wobei sie in der kleinen Kammer aufgrund der vorgenommenen Änderungen nochmals traktandiert werden musste. [24]

MOTION
DATUM: 06.03.2018
MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 des Ständerates war die Beschlussfassung zu einem **Cyberdefence-Kommando** nur noch Formsache. Der Motionär selbst, aber auch die ständerätliche SiK, zeigten sich mit der vom Nationalrat veränderten Fassung einverstanden. Weil der Ständerat selbst zuvor bereits einmal dem Anliegen zugestimmt hatte und nun auch in der Ständekammer seitens des Verteidigungsministers grünes Licht gegeben wurde, galt die Motion schon beinahe als angenommen. Ohne Gegenstimme wurde sie denn auch abgesegnet. [25]

MOTION
DATUM: 10.06.2021
DIANE PORCELLANA

L'Assemblée fédérale a décidé, sur proposition du Conseil fédéral, de classer la motion demandant la **création d'un commandement de cyberdéfense dans l'armée suisse**. En effet, le Conseil fédéral l'a informée qu'avec la révision planifiée en 2023 de la loi du 3 février 1995 sur l'armée et de l'organisation de l'armée, il répondra aux demandes formulées.

Aktionsplan Cyber-Defence

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. [26]

Meldepflicht bei kritischen Infrastrukturen (Po. 17.3475)

Netz und Vertrieb

POSTULAT
DATUM: 13.12.2017
MARCO ACKERMANN

Nationalrätin Graf-Litscher (sp, TG) wies in ihrem Postulat für eine **Meldepflicht bei kritischen Infrastrukturen** darauf hin, dass Infrastrukturen wie Strom und Telekommunikation sehr essentiell für die Schweiz sind und Risiken wie Cyberangriffe, Naturkatastrophen sowie militärische und terroristische Angriffe auf die Infrastruktur grosse Auswirkungen auf das ganze Land haben würden. Sie forderte den Bundesrat dazu auf, darzustellen, wie eine mögliche Meldepflicht bei potenzieller Bedrohung aussehen könnte. Mithilfe einer systematischen Auswertung dieser Meldungen könnte so ein Frühwarn-, Beratungs- und Abwehrsystem aufgebaut werden, welches potenzielle Risiken verringert.
Bundesrat Maurer begrüsste diese Forderung und betonte die geforderte Systematik, die zur Prävention von Risiken führen könne. Durch den Austausch von Erfahrungen unter den Betreibern und den staatlichen Behörden könne das Sicherheitsdefizit der Schweiz in diesem Bereich verringert werden. In der Schweiz seien derzeit wichtige Infrastrukturen anfällig bezüglich diverser Gefahren. Der Nationalrat nahm das Postulat am 13. Dezember 2017 stillschweigend an. [27]

BERICHT
DATUM: 15.12.2019
MARCO ACKERMANN

Im Dezember 2019 legte der Bundesrat einen **Bericht** in Erfüllung des Postulates Graf-Litscher (sp, TG) vor und präsentierte darin **Varianten für die Ausgestaltung von Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen**. Der Bericht erörterte die derzeitige Ausgangslage, verglich Meldepflichten im Ausland und präsentierte nebst der Variante, keine weiteren Meldepflichten einzuführen, drei Varianten für eine Meldepflicht und für Meldestellen in der Schweiz. Bei diesen drei Möglichkeiten würde entweder eine zentrale Meldestelle etabliert, die bisherigen dezentralen Meldestellen in den Sektoren auf- und ausgebaut oder als letzte Variante eine Kombination der beiden Ansätze umgesetzt, wobei eine zentrale Meldestelle einzig für Cybervorfälle und die bestehenden dezentralen Stellen für alle anderen sicherheitsrelevanten Vorfälle zuständig wären. Die vorgeschlagenen vier Varianten sollen in einem nächsten Schritt mit Wirtschaftskreisen, den Kantonen und den zuständigen Behörden vertieft diskutiert werden und im Sommer 2020 zur Erarbeitung einer entsprechenden gesetzlichen Grundlage führen. [28]

POSTULAT
DATUM: 14.09.2020
MARCO ACKERMANN

Im Rahmen des Berichts des Bundesrates über Motionen und Postulate der eidgenössischen Räte 2019 schrieb der Nationalrat im September 2020 das Postulat Graf-Litscher (sp, TG) zur **Ausgestaltung einer Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen** stillschweigend ab. Im November desselben Jahres nahm die SiK-NR bei Beratungen zur Cybersicherheit Kenntnis vom Bericht. [29]

Cyberrisiken. Für einen umfassenden, unabhängigen und wirksamen Schutz (Po. 16.4073)

Äussere Sicherheit

POSTULAT
DATUM: 28.02.2018
MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 wurde die Debatte eines Postulats, das sich der Thematik **Cyberrisiken** widmete und einen **umfassenden, unabhängigen und wirksamen Schutz** für die Schweiz forderte, aufgenommen. Dabei wurde der Bundesrat von Roger Golay (mcg, GE) aufgefordert, einen Bericht über die Anwendung der Nationalen Strategie gegen Cyberrisiken (NCS) zu erstellen. Man habe, so der Postulant, «nämlich bisher nicht viel [davon] wahrnehmen» können. Der Postulant sorgte sich dabei auch um die Kompetenzenverteilung, so wollte er denn auch beantwortet wissen, wie das Nebeneinander von EFD und VBS funktioniere und ob dies nicht Risiken berge. Eine Reihe von weiteren Fragen sollte der Bericht auch noch angehen, so beispielsweise wie hochstehendes Fachwissen in der Schweiz erhalten werden kann und wie die Zusammenarbeit zwischen Wissenschaft und Bund intensiviert werden könnte.
Die bundesrätliche Stellungnahme folgte bereits kurz nach der Einreichung und sie war nicht sehr lang, doch hielt die Regierung fest, dass das Postulat Fragen tangiere, die bereits bekannt seien. Sie würden auch in einer Wirksamkeitsprüfung der NCS diskutiert, ein Dokument, das noch im Frühjahr 2017 erscheinen sollte. Eine weitere Analyse, wie die im Postulat geforderte, sei nicht nötig – es wurde also die Ablehnung des Postulats beantragt.
Golay vertrat seinen Vorstoss, der von 62 Nationarlätinnen und Nationalräten mitunterzeichnet worden war, im Parlament. Seiner Meinung nach war sein Postulat nach wie vor aktuell. Der Nationalrat solle auf diesen Bericht beharren: Gerade im Lichte kürzlich zurück liegender Cyber-Attacken auf bundesnahe Betriebe sei diese Form der Aufklärung gerechtfertigt. Bundesrat Maurer versuchte dem Vorstoss noch entgegenzutreten. Man habe sich im Rahmen eines ähnlichen Vorstosses bereits mit dem Thema auseinander gesetzt. Zudem stand eine Klausur des Bundesrats zum Thema Cybersicherheit an, und überhaupt liefen die Arbeiten diesbezüglich auf Hochtouren. Weiter konnte Maurer in Aussicht stellen, dass bereits mit dem Budget 2019 die Anträge zur Schaffung und Stärkung der Cybersicherheit gestellt werden können. Ein Cyber-Securityzentrum wurde mit 40 neuen Stellen veranschlagt, die man über drei Jahre besetzen will. Angesichts aller bereits angestossenen Vorarbeiten könne das Postulat Golay getrost abgelehnt werden. Relativ knapp, mit 100 zu 93 Stimmen (bei drei Enthaltungen) verwarf das Plenum jedoch diesen Antrag und nahm das Postulat an. [30]

POSTULAT
DATUM: 28.11.2019
DIANE PORCELLANA

Le Conseil fédéral a présenté son **rapport sur l'organisation de la Confédération pour la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques** (SNPC), dans lequel il fournit également une réponse au postulat 18.3003 et à la motion Eder 17.3508. Depuis la transmission des interventions parlementaires, il a déjà adopté le plan de mise en œuvre de la SCNP 2018-2022, déterminé l'organisation de la Confédération dans le domaine des cyberrisques, défini les compétences et les responsabilités de la cyberdéfense militaire et a contribué à la création d'un centre de compétences pour la cybersécurité.
Les sept objectifs stratégiques et les 29 mesures à prendre dans les dix différents champs d'action sont détaillés dans la SNCP 2018-2022. Au sein de l'Administration fédérale, Délégation Cyber du Conseil fédéral surveillera la mise en œuvre de la stratégie. Le délégué de la Confédération à la cybersécurité se chargera, d'une part, de la direction stratégique et d'autre part, il chapeautera le Groupe Cyber – responsable de la coordination des domaines – et le comité de pilotage de la SNCP. Le centre de compétences assumera la direction stratégique de la cybersécurité de la Confédération, du guichet unique national, du service spécialisé de sécurité informatique et du pool de compétences pour la cybersécurité. L'armée formera ses cadres et membres en matière de cybersécurité. Avec les autorités civiles, elle devra définir les conditions-cadres de son soutien lors de cyberincidents et le déroulement de son intervention. Trois projets propices à l'innovation seront mis en œuvre afin de réduire la dépendance à l'égard de prestataires et de fabricants de logiciels et de matériel étrangers. Pour la réalisation, des ressources financières et en personnel supplémentaires seront nécessaires. D'après l'étude du Center for Security Studies de l'EPF de Zurich, les structures dans le domaine de la cybersécurité en Suisse se retrouvent à l'étranger. Aucun des pays étudiés ne possède d'organisation unique pour la réalisation des travaux liés aux cyberrisques et n'a confié à son armée la

responsabilité d'assurer la protection contre ce type de danger. [31]

POSTULAT
DATUM: 10.06.2021
DIANE PORCELLANA

Comme le Conseil fédéral a rendu son **rapport sur l'organisation de la Confédération pour la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques** (SNPC), l'Assemblée fédérale classe donc le postulat.

Ausbau der Cyberabwehrkompetenzen (Mo. 17.3199)

Äussere Sicherheit

MOTION
DATUM: 06.03.2018
MAXIMILIAN SCHUBIGER

Mit 58 Mitunterzeichnenden aller Parteien im Rücken forderte Franz Grüter (svp, LU) den Bundesrat mittels Motion auf, den **Ausbau der Cyberabwehrkompetenzen** voranzutreiben. Innerhalb zweier Jahre sollen alle sicherheitspolitischen Kompetenzen im Bereich Cyberabwehr zudem gebündelt werden und innerhalb der Verwaltung von einer einzigen Stelle koordiniert werden können. Dabei wurde offen gelassen, ob diese Einheit innerhalb der Armee geschaffen oder dem VBS angegliedert werden soll. Jedoch sah der Motionär eine Finanzierung via das Rüstungsbudget vor. Ferner sollte auch bezüglich künftiger Beschaffungen ein Augenmerk auf Cybersicherheit gelegt werden. Grüter schlug damit in die gleiche Kerbe wie Ständerat Dittli (fdp, UR), der seinerseits ein Cyberdefence-Kommando anregte, und Ständerat Eder (fdp, ZG), der die Schaffung eines Kompetenzzentrums für Cyberfragen verlangte. Begründet wurde die Motion mit den neuen Bedrohungsszenarien im digitalen Raum sowie mit der Erfahrung kürzlich stattgefundener Angriffe auf die Computerinfrastruktur von Bund und Wirtschaft. Der Luzerner wollte darüber hinaus ebenfalls – dieses Anliegen deckt sich mit den Bestreben der beiden Motionen aus der kleinen Kammer – die Zuständigkeit neu regeln und nur eine Verwaltungsstelle mit der Aufsicht betrauen, um «Redundanzen, Ineffizienzen und Koordinationsaufwand» reduzieren zu können.
Der Bundesrat, der sich also bereits wiederholt mit ähnlichen Vorstössen konfrontiert sah, beharrte auf der Ablehnung dieser Forderungen. Im Grunde sei er ja nicht gegen einen Ausbau im Cyberbereich, jedoch sollte den Prozessen der NCS nicht vorgegriffen werden, erklärte er. Eine einzige Stelle für diese Oberaufsicht werde geprüft.

Dieser bundesrätlichen Zurückhaltung stand, wie auch in den anderen diesbezüglichen Geschäften, eine wohlwollende Parlamentskammer gegenüber. Im Wissen um die bereits genehmigten anderen beiden Motionen Dittli und Eder hiess der Nationalrat auch die vorliegende Motion gut. Grüter gelang es, Druck aufzubauen, in dem er auf der Einrichtung einer zentralen Koordinationsstelle beharrte. Dabei bot er in der Ratsdebatte bereits Hand zu einer Lösung: Melani könne diese Aufgabe übernehmen, es brauche also nicht einmal eine neue Verwaltungseinheit, schlug er vor. Jedoch müsse dort mehr investiert und sowohl personell als auch finanziell mehr Aufwand betrieben werden. Zudem müsse der Auftrag an Melani neu verfasst werden. Bundesrat Maurer vertrat die ablehnende Haltung der Regierung, auch mit Verweis auf ein kurz zuvor angenommenes SiK-Kommissionspostulat, vergeblich. Die grosse Kammer überwies den Vorstoss mit 134 zu 47 Stimmen und 9 Enthaltungen der Ständekammer. [32]

MOTION
DATUM: 10.09.2018
MAXIMILIAN SCHUBIGER

Die Motion Grüter (svp, LU) beschäftigte im Sommer die ständerätliche SiK. Der **Ausbau der Cyberabwehrkompetenzen** wurde vom Gremium mehrheitlich begrüsst, gleichwohl überwogen Bedenken bezüglich der Motion. Die SiK-SR schlug deswegen ihrem Rat vor, die Motion nicht anzunehmen. Man wollte sich mit diesem Schritt Zeit verschaffen, um bereits in Angriff genommene Projekte weiterzuführen. Namentlich ging es um die beiden überwiesenen Motionen zu einem Cyberdefence-Kommando in der Armee und zu einem Cybersecurity-Kompetenzzentrum. Diese laufenden Massnahmen wurden von der SiK begrüsst, wohingegen die vorliegende Motion widersprüchliche Folgen zu bereits getätigten Beschlüssen hätte. Besonders die angeregte Zentralisierung der Cyberkompetenzen an einer Amtsstelle (innerhalb des VBS) wurde von den Kommissionsangehörigen mehrheitlich abgelehnt. Man vergebe sich dadurch viele bereits erlangte Kenntnisse und die bisherigen Mechanismen innerhalb des EFD und MELANI funktionierten gut. Aus ordnungspolitischer Sicht wurde die Motion zudem abgelehnt, weil es der Regierung und nicht dem Parlament obliege, federführende Stellen innerhalb der Verwaltung zu bestimmen. Diesem Antrag stimmten 10

Kommissionsmitglieder zu, zwei waren dagegen.
Dieser deutlichen Kommissionsmeinung folgte dann auch das Ratsplenum, das die Motion ablehnte und damit den recht deutlichen Beschluss des Erstrates umstiess. Kommissionssprecher Dittli (fdp, UR) und Bundesrat Maurer waren die Einzigen, die sich zu Wort meldeten. Beide betonten die bereits angestossenen Arbeiten und die guten Fortschritte im Cybersicherheitsbereich. Die Regierung erkenne im Vorschlag Grüter keine bessere Lösung, erklärte Maurer. Oppositionslos wurde das Geschäft verworfen. [33]

Eine klare Cyber-Gesamtstrategie für den Bund (Po. 18.3003)

Äussere Sicherheit

POSTULAT
DATUM: 06.03.2018
MAXIMILIAN SCHUBIGER

Angesichts der vielen Vorstösse im Bereich Cyber-Kriminalität und -Abwehr und trotz bereits laufender Projekte (Aktionsplan Cyber-Defence, Nationale Cyber-Strategie) sah die sicherheitpolitische Kommission des Nationalrates in dieser Hinsicht noch Handlungsbedarf. Auch wenn die Arbeiten in der NCS begrüsst würden, brauche es **eine klare Cyber-Gesamtstrategie für den Bund**. Was bisher lanciert wurde, entspreche noch keinem Gesamtkonzept, so die Auffassung der Kommission. Fünf konkrete Aufgaben wurden dem Bundesrat gestellt. Dazu gehörte eine präzise Umschreibung des Auftrags der Armee im Bereich der Cyberverteidigung und des Zuständigkeitsbereichs der zivilen Cyberbehörden. Im Lichte der gewonnenen Erkenntnisse sollte darauf basierend eine Abgrenzung der Kompetenzen vorgenommen und ein entsprechendes Organigramm erstellt werden. Bezüglich Finanzierung sollte man sich ferner Gedanken machen über den Ressourcenbedarf, einschliesslich des Personalbedarfs. Abschliessend wurde vorgeschlagen, dass sich die Schweiz auch am Ausland orientieren möge, wenn es um die Cyberabwehr gehe.
Die Regierung räumte ein, dass längere Zeit unzureichend über dieses Thema nachgedacht und es zeitweise gar unterschätzt worden war. Daher wurde eine solche Gesamtstrategie für unabdingbar erklärt, deutlich unterstützte der Bundesrat also dieses Postulat. Eine «Zerstückelung» des Themas, weil diverse Aktionspläne in unterschiedlichen Departementen erstellt würden, sei nicht wünschenswert.
Im Nationalrat war die Angelegenheit klar, das Postulat wurde angenommen. Kommissionssprecherin Mazzone (gp, GE) und Kommissionssprecher Dobler (fdp, SG) unterstrichen die Wichtigkeit einer koordinierten Vorgehensweise und Dobler äusserte überdies den Eindruck, dass bisher erst wenig geschehen sei, obwohl sich um die 90 Personen in der Bundesverwaltung bereits mit Cyber-Themen befassten. Dies wurde jedoch von Bundesrat Maurer sogleich bestritten. Der Magistrat betonte, dass die Planung weiter fortgeschritten sei, als es vom Vorredner dargestellt worden sei, und er stellte in Aussicht, dass bereits im Budget 2019 erste Positionen für die Umsetzung einer Gesamtstrategie beantragt werden sollten. [34]

POSTULAT
DATUM: 28.11.2019
DIANE PORCELLANA

Le Conseil fédéral a présenté son **concept global de protection et de défense du cyberespace civil et militaire**, dans son rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Une organisation supradépartementale a été privilégiée pour assumer les tâches de cybersécurité, de cyberdéfense et pour la poursuite pénale de la cybercriminalité. Le soutien de l'armée lors de cyberincidents et le déroulement de ses interventions doit encore être défini avec les autorités civiles. Pour assurer la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, les ressources financières ont été augmentées et une soixantaine de postes de travail supplémentaires ont été créés. Enfin, en comparaison internationale, la Suisse possède des structures dans le domaine de la cybersécurité similaires à celles de plusieurs autres pays. Aucun des pays étudiés, à savoir l'Allemagne, la Finlande, la France, Israël, l'Italie et les Pays-Bas, ne possède une organisation unique pour la réalisation des travaux liés aux cyberrisques et n'a confié à son armée la responsabilité d'assurer la protection contre ce type de danger. [35]

POSTULAT
DATUM: 14.09.2020
DIANE PORCELLANA

Sur proposition de la CPS-CN, le **Conseil national a refusé de classer les postulats relatifs à la protection contre les cyberrisques** (Po. 18.3003 et 16.4073). La commission ne souhaitait pas les voir classer, car ils sont en cours de mise en œuvre et de nombreuses questions restent encore sans réponse s'agissant de la Stratégie nationale de protection de la Suisse contre les cyberrisques. [36]

ICT Empfehlungen Bund (Cyber)

Äussere Sicherheit

VERWALTUNGSAKT
DATUM: 27.08.2018
MAXIMILIAN SCHUBIGER

Ende August 2018 gelangte das BWL infolge einer Verwundbarkeitsanalyse zu Cyberrisiken mit Empfehlungen, den sogenannten **IKT-Minimalstandards**, an die Öffentlichkeit. Dabei standen lebenswichtige Branchen im Zentrum des Interesses, namentlich die Stromversorgung, Trinkwasser- und Lebensmittelversorgung sowie auch der Strassen- und Schienenverkehr. Besonders Betreiber von kritischen Infrastrukturen sollen sich an diese Mindeststandards («IKT-Resilienz») halten, sie seien jedoch für alle Unternehmen anwendbar. Über 100 konkrete Handlungsanweisungen in den Bereichen Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen waren zuhanden der Betreiber ausgearbeitet worden. In Kooperation mit dem Verband Schweizerischer Elektrizitätsunternehmen sei bereits ein Standard für die Strombranche erarbeitet worden. Dieser Schritt war im Zuge der 2012 vom Bundesrat lancierten Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) unternommen worden. [37]

Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff? (Po. 19.3136)

Innere Sicherheit

POSTULAT
DATUM: 21.06.2019
MAXIMILIAN SCHUBIGER

«**Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?**», fragte Marcel Dobler (fdp, SG) mit einem im Frühjahr 2019 eingereichten Postulat. Damit griff Dobler Sorgen auf, die bei grösseren IT-Beschaffungen immer wieder geäussert werden. Unter anderem geht es dabei namentlich um ICT-Systeme, die in diversen sensiblen Bereichen eingesetzt werden und die von ausländischen Herstellern produziert und bereitgestellt werden. Solche «digitale[n] Lieferobjekte», die in ihrer Komplexität zu Cyberrisiken führen können, stehen im Fokus seines Vorstosses. Der Bundesrat sollte folglich beauftragt werden, zu prüfen, ob und wie nationale und internationale Standards angewendet werden können, um die Risiken zu vermindern.
Der Bundesrat zeigte sich mit der Stossrichtung des Postulats einverstanden und beantragte dessen Annahme, jedoch seien die Forderungen in einen Bericht aufzunehmen, der bereits mit der Annahme zweier anderer Postulate (Po. 18.3376 und Po. 18.3233) in Auftrag gegeben worden war, erklärte er.
Der Nationalrat sollte sich in der Sommersession 2019 damit befassen, da jedoch auf jegliche Wortmeldungen verzichtet wurde, überwies der Rat das Postulat stillschweigend. [38]

BERICHT
DATUM: 24.11.2021
DIANE PORCELLANA

En exécution des postulats Dobler (19.3135) et (19.3136), le Conseil fédéral a fourni son rapport intitulé «**Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense**». Le rapport détaille les standards existants et les engagements de la Confédération et des exploitant.e.s d'infrastructures critiques y découlant en la matière. Si le domaine de la sécurité des produits est plutôt normé et appliqué, les directives relatives à la gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité sont moins étoffées. La Confédération dispose d'une base légale pour appliquer les standards de sécurité des produits TIC et la gestion des risques de la chaîne d'approvisionnement. Les règles liées au respect des standards de sécurité des TIC pour les infrastructures critiques sont par contre «rares». Pour les standards de sécurité des produits, le rapport appelle à se concentrer sur la mise en œuvre globale

et continue des directives. S'agissant des directives en matière de gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité, les standards se révèlent être des recommandations plutôt que des normes contraignantes. Afin de remédier au manque de directives contraignantes pour les infrastructures critiques, le rapport expose plusieurs solutions: l'élaboration de directives juridiquement contraignantes, les références aux standards dans le domaine de la sécurité des produits ou des directives adressées aux exploitant.e.s d'infrastructures critiques pour une gestion sûre des produits TIC. Le rapport recommande également d'introduire des directives liées à des mesures régulatrices pour la gestion des risques de la chaîne d'approvisionnement. [39]

BERICHT
DATUM: 07.06.2022
CHLOÉ MAGNIN

Après la publication du rapport traitant des deux motions 19.3135 et 19.3136 nommé **«Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense»**, le Conseil fédéral a décrété que les objets devaient être classés. Ceci a été entrepris et finalisé le 7 juin 2022 dans le cadre de l'objet 22.006. [40]

Cyber-Defence Campus

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. [41]

Obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques

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. [42]

Institutionnaliser le piratage éthique et améliorer la cybersécurité (Po 20.4594)

Datenschutz und Statistik

POSTULAT
DATUM: 19.03.2021
DIANE PORCELLANA

La conseillère nationale Judith Bellaïche (pvl, ZH) charge le Conseil fédéral d'étudier comment le **piratage éthique** pourrait être **institutionnalisé** et encouragé dans l'Administration fédérale et les entreprises liées à la Confédération. Le piratage éthique vise à chercher et détecter les failles, afin de renforcer la sécurité du réseau et des systèmes informatiques. Pour ce faire, il faudrait des directives qui définissent le cadre du piratage éthique, notamment le processus pour détecter les failles de sécurité et les tests de robustesse. Toute poursuite à l'encontre des pirates impliqués dans ce type de piratage doit être exclue. Le Centre national pour la cybersécurité devrait accompagner

et soutenir cette démarche.
Le Conseil fédéral a proposé d'accepter le postulat, lequel a été adopté sans discussion par le Conseil national. [43]

BERICHT
DATUM: 29.11.2023
CHLOÉ MAGNIN

Le **rapport** faisant suite au **postulat Bellaiche** (pvl, ZH) a été publié par le Conseil fédéral. Dans ce rapport, le contexte relatif au **piratage éthique** a été rappelé. «La numérisation a rendu l'économie, l'Etat et la population complètement dépendants du fonctionnement et de la sécurité des technologies de l'information et de la communication.» Les codes à l'origine de ces systèmes informatiques sont longs et complexes, laissant place à de possibles vulnérabilités par lesquelles les cyberattaquant.e.s peuvent accéder aux systèmes sans y avoir été invités, pouvant mener à des cyberattaques. Le présent postulat demandait d'analyser la situation du piratage éthique en Suisse. Ce dernier consiste à ce que les cyberattaquant.e.s, au lieu de lancer une cyberattaque contre le système, préviennent l'institution de la vulnérabilité afin que le système soit amélioré et la cybersécurité renforcée.
Dans son rapport, le Conseil fédéral soutient que les chances sont grandes que le recours au piratage éthique gagne encore en importance à l'avenir. En Suisse, les mesures actuelles montrent encore un large potentiel et aucune mesure légale supplémentaire n'est actuellement nécessaire. Au cours des dernières années, le piratage éthique a «grandement progressé en Suisse» et le rapport pointe plusieurs aspects l'expliquant. Premièrement, lors de l'instauration de l'obligation de signalement des vulnérabilités des institutions critiques (22.073), la base légale pour le piratage éthique a été définie par l'Administration. Deuxièmement, l'économie privée a elle aussi promu le piratage éthique en lançant des programmes de primes aux bogues. Le rapport met en lumière que le succès de ces programmes orientera de nouvelles entreprises vers le piratage éthique. Finalement, la Confédération encourage le piratage éthique, ce dernier étant un élément clé de la cyberstratégie nationale.
Ainsi, le NCSC, qui est devenu l'Office fédéral de la cybersécurité le premier janvier 2024, continuera de coordonner et divulguer les vulnérabilités. L'Administration fédérale perpétuera l'élargissement des mesures visant à promouvoir le piratage éthique et la Confédération encouragera le secteur économique à suivre la voie du piratage éthique en mettant en lumière les bienfaits de ce dernier. Le rapport souligne cependant que si après signalement, les vulnérabilités ne sont pas supprimées par les utilisateurs des programmes, même après mise à disposition d'une mise à jour de la part du détenteur du programme, déceler la vulnérabilité ne fait que peu de sens. C'est pourquoi le rapport affirme qu'une collaboration est essentielle. Pour le Conseil fédéral, en promouvant le piratage étique, l'échange sur les vulnérabilités sera renforcé. Et ceci, sans obliger les signalements de vulnérabilités. De plus, «les conditions sont réunies pour que le potentiel important du piratage éthique soit mieux exploité à l'avenir. Si cet objectif est atteint, il est probable que la prévention contre les cyberattaques soit nettement améliorée et que les pouvoirs publics ainsi que les entreprises puissent nettement mieux se protéger qu'aujourd'hui.» [44]

Modification de loi sur l'armée et de l'organisation de l'armée (OCF 21.061)

Militärorganisation

BUNDESRATSGESCHÄFT
DATUM: 01.09.2021
DIANE PORCELLANA

Dans le cadre de la mise en œuvre du développement de l'armée (DEVA) et en exécution de la motion 19.3427, le Conseil fédéral a soumis au Parlement une révision de la **Loi sur l'armée** (LAAM) **et l'Ordonnance sur l'organisation de l'armée** (OOrgA).
En terme d'organisation, comme décidé par l'Assemblée fédérale, la Base d'aide au commandement (BAC) et la Base logistique de l'armée (BLA) ne seront pas réunies sous le commandement du Soutien. Le Conseil fédéral propose que la BAC devienne un commandement Cyber en 2024. En matière d'instruction, les cyberspécialistes devront suivre un stage auprès de partenaires externes afin de développer leurs capacités. Dès le 1er janvier 2022, un cyber bataillon et un état-major spécialisé verront le jour, renforçant les effectifs du personnel dans le domaine de la cyberdéfense. Le Conseil fédéral demande la création d'une autorité du trafic aérien militaire, afin de davantage sécuriser les missions des Forces aériennes. Enfin, le Conseil fédéral aimerait que les recrues puissent également être engagées pour soutenir des événements civils. L'armée devrait être autorisée à fournir des prestations lors d'événements d'importance nationale ou internationale, sans forcément en tirer un avantage majeur

pour l'instruction ou l'entraînement. D'autres modifications concernant notamment les droits et les devoirs des militaires doivent être faites. [45]

BUNDESRATSGESCHÄFT
DATUM: 02.11.2021
DIANE PORCELLANA

La CPS-CN propose, à l'unanimité, d'entrer en matière concernant le projet d'adaptation de la **Loi sur l'armée et l'Ordonnance sur l'organisation de l'armée** du Conseil fédéral. Les adaptations liées à la cyberdéfense ont été saluées. S'agissant de l'autorité de surveillance et de régulation du trafic aérien militaire, la commission a refusé, par 15 voix contre 10, une proposition visant à ce que les enquêtes relatives à l'aviation militaire soient menées par une commission extraparlementaire plutôt que par un service interne de l'autorité. Concernant l'appui de l'armée aux événements civils d'importance nationale ou internationale, la commission a balayé par 15 voix contre 8 et 2 abstentions, une proposition pour limiter strictement ces engagements aux cas où un bénéfice pour l'instruction était avéré. Par 17 voix contre 7, elle a rejeté une proposition visant à empêcher l'engagement de recrues. Enfin, la commission a refusé deux propositions, par 15 voix contre 9, visant à exempter du service militaire le personnel exerçant un taux d'activité d'au moins 50 pour cent et à abaisser le taux à 50 pour cent uniquement pour le personnel médical nécessaire pour assurer le fonctionnement des établissement médicaux civils. [46]

BUNDESRATSGESCHÄFT
DATUM: 15.12.2021
DIANE PORCELLANA

Avec 111 voix contre 80 et avec 179 voix et 12 abstentions, le Conseil national a approuvé **les projets de modification de la Loi fédérale sur l'armée et l'administration militaire** (LAAM) **et de l'Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée** (OOrgA). La conseillère fédérale Viola Amherd a reçu le soutien de la Chambre basse pour la création d'un commandement Cyber et d'un cyber bataillon afin de renforcer la cyberdéfense. Les effectifs en la matière seront donc augmentés. Le Conseil national a également accepté la mise sur pied d'une autorité de surveillance et de régulation du traité aérien militaire, après avoir balayé par 111 voix contre 80 une proposition visant à ce que les enquêtes soient effectuées par une commission extraparlementaire. Si le PS et le PVL jugeaient qu'il serait «abusif» de mettre à disposition gratuitement des soldats sans bénéfice pour leur instruction, l'armée pourra dans le futur soutenir des événements d'importance national ou internationale sans qu'elle en retire un avantage au niveau de l'instruction et de l'entraînement. S'agissant de l'exemption de servir, la proposition visant à exempter les hommes travaillant à moins de 50 pour cent a été rejetée par 109 voix contre 80. Le personnel médical, les membres des services de sauvetage, les policiers ainsi que les gardes-frontières qui ne sont pas nécessaires aux tâches de l'armée pourront être dispensés. Pour répondre aux besoins de l'armée, le service militaire long passera de 280 à 300 jours. [47]

BUNDESRATSGESCHÄFT
DATUM: 18.03.2022
CHLOÉ MAGNIN

Le **projet de modification de l'armée et de son organisation** est passé devant le Conseil des États le premier mars 2022, après son acceptation en décembre par le national. Dans une situation militaire européenne tendue, l'ambiance a parfois été morose en ce mardi de mars sous la coupole fédérale. Les sénateurs et sénatrices ont admis dans leurs discours un besoin de se mettre à jour technologiquement afin de garantir la sécurité du pays. En décidant de suivre la position de la conseillère fédérale Viola Amherd, qui scandait la nécessité de renouveau pour faire face à des cyberattaques, les parlementaires ont approuvé le projet du Conseil fédéral. D'ici 2024, le gouvernement devra ainsi mettre en place la transformation de sa base d'aide au commandement en commandement cyber et augmenter ses effectifs dans le domaine pour passer de 206 à 575 militaires en fonction.
En ce qui concerne le deuxième point discuté, à savoir l'exemption de servir, une plus grande disparité qu'au Conseil national s'est faite ressentir. Il a été décidé que «les personnes travaillant au minimum à 80 pour cent dans le domaine de la santé, pour les services de sauvetage, dans la police, les sapeurs-pompiers et le corps des gardes-frontières, et qui ne sont pas nécessaires aux tâches de l'armée» pourront profiter de cette mesure. Concernant la demande de la gauche – que le personnel médical travaillant dans des institutions publiques à mi-temps puisse aussi profiter de cette mesure, afin de lutter contre le manque de personnel soignant –, la ministre de la défense s'y est opposée. La raison de ce désaccord est relatif au manque d'efficacité que ceci représenterait non seulement pour l'armée mais aussi pour les services de santé publique, si l'armée, exempte de ce personnel professionnel, venait à remplir sa mission de soutien au service de la santé de la population suisse. La requête est de ce fait inenvisageable pour le gouvernement helvétique.
Le projet comprenait aussi la mise en place de mesures afin de renforcer la surveillance

et la participation aux manifestations des services de l'armée. De ce fait, une autorité de surveillance et de régulation de l'espace aérien militaire visant à prévenir les accidents sera créée et les militaires suisses seront plus souvent amenés à participer à des événements civils.
La modification de la loi fédérale sur l'armée et l'administration militaire (LAAM) a été acceptée à l'unanimité.
L'ordonnance de l'Assemblée fédérale sur l'organisation de l'armée (OOrgA) a, elle aussi, été acceptée à l'unanimité. Le 18 mars 2022, les deux chambres ont adopté le texte de loi final. [48]

Massnahmen für einen besseren Schutz gegen Ransomware-Angriffe (Po. 21.4512)

Kriminalität

POSTULAT
DATUM: 08.06.2022
LENA BALTISSER

Im Dezember 2021 reichte Edith Graf-Litscher (sp, TG) ein Postulat zur Prüfung von **Massnahmen für einen besseren Schutz gegen Ransomware-Angriffe** ein. Laut der Postulantin stellten Cyberangriffe über Verschlüsselungstrojaner, sogenannte Ransomware, eine grosse Gefahr für die Wirtschaft und die Verwaltung dar. Besondere Beachtung sollten im Rahmen der auszuarbeitenden Massnahmen die Sicherheitsrichtlinien von Unternehmen mit öffentlichem Auftrag, eine mögliche Meldepflicht für Lösegeldzahlungen bei Cyberangriffen und die engere Zusammenarbeit der betroffenen Unternehmen mit den zuständigen Behörden erhalten. Während der Bundesrat das Postulat zur Annahme beantragte, wurde es von Erich Hess (svp, BE) bekämpft. In der Sommersession 2022 stimmte der Nationalrat dem Postulat mit 87 Ja- zu 86 Nein-Stimmen bei 6 Enthaltungen knapp zu, nachdem sich Judith Graf-Litscher und Bundesrat Maurer für dessen Annahme ausgesprochen hatten. Erich Hess hatte auf ein Votum verzichtet. Gegen das Postulat sprachen sich insbesondere die SVP-, FDP- und Mitte-Fraktion aus. [49]

BERICHT
DATUM: 13.11.2024
LUKAS LÜTOLF

In Erfüllung eines Postulats von Edith Graf-Litscher (sp, TG) veröffentlichte der Bundesrat im September 2024 einen **Bericht zu Massnahmen gegen Ransomware-Angriffe**. Darin betont er, dass die Schweizer Unternehmen und Behörden aufgrund ihrer relativ hohen Zahlungskraft im internationalen Vergleich ein attraktives Ziel für Cyberkriminelle darstellen. Aus diesem Grund gebe es bereits heute zahlreiche rechtliche Vorgaben und behördliche Informationen zur Cybersicherheit sowie Anleitungen und Richtlinien zu IT-Schutzmassnahmen, so die Regierung. Diese Instrumente sollen im Bedarfsfall weiterentwickelt werden. Dabei sei von neuen Vorgaben zu Ransomware abzusehen, denn der Bund könne aufgrund der föderalen Kompetenzzuordnung keine flächendeckenden verbindlichen Schutzvorgaben für kantonale oder kommunale Organisationen mit öffentlichem Auftrag erlassen. Überdies habe die Prüfung einer möglichen Meldepflicht für Lösegeldzahlungen bei Cyberangriffen ergeben, dass eine Förderung des freiwilligen Informationsaustauschs zwischen gefährdeten Unternehmen und der öffentlichen Hand die Resilienz gegenüber Ransomware-Angriffen mehr stärken würde als eine neue Vorschrift. Im Bericht stellte die Regierung daher in Aussicht, diesen Informationsaustausch und die gemeinsame Abwehr von Ransomware-Angriffen durch eine koordinierende Rolle voranzutreiben. Sollten diese Massnahmen nicht die erhoffte Wirkung entfalten, seien bei Angriffen dennoch verbindlichere Massnahmen wie eine anonyme Meldepflicht für Versichernde betroffener Unternehmen, Finanzintermediäre sowie Sicherheitsdienstleistende in Betracht zu ziehen. [50]

Cyberexercices-stratégie générale pour la Suisse (Mo. 22.3836)

Landesverteidigung und Gesellschaft

MOTION
DATUM: 21.09.2022
CHLOÉ MAGNIN

Alors que dans l'ère du numérique les facteurs cybers jouent un rôle de plus en plus important, Marcel Dobler (plr, SG) a souhaité, en déposant une motion, mettre l'accent sur la **planification générale des exercices de sécurité** afin de consolider la résilience du système cyber suisse. Le Conseil fédéral a rejoint Dobler sur l'importance de ces exercices. C'est pourquoi ils sont inscrits sur la SNPC et que les domaines de la finance et de la santé ont déjà été sujets à ces simulations. De plus, afin de garantir une entraide et une gestion collective des complications que l'ère cyber peut engendrer, des exercices à l'échelle internationale ont déjà vu le jour. En conclusion, les objectifs de la motion ont été considérés comme atteints en raison des mesures déjà entreprises sur le territoire helvétique.
28 jours après l'annonce de l'avis négatif du Conseil fédéral, la motion a été retirée. [51]

1) AB NR, 2010, S. 1800 ff.; NZZ, 3.12. und 11.12.10; CdT, 11.12.10.
2) AB NR, 2010, S. 1800 ff.; AB SR, 2010, S. 550; AB SR, 2011, S. 251 f.
3) AB SR, 2011, S. 251 f.
4) AB NR, 2011, S. 531
5) AB NR, 2011, S. 531; SoS, 5.11.11
6) AB NR, 2011, S. 531, 2266.
7) Medienmitteilung VBS vom 27.06.2012
8) NZZ, 28.6.12.
9) BBl, 2013, S. 563 ff.; Medienmitteilung IBS vom 15.5.13 .pdf
10) Jahresbericht Steuerungsausschuss NCS 2013.pdf; Medienmitteilung VBS vom 30.4.14.pdf
11) Medienmitteilung Bundesrat vom 26.04.2017; NCS Bericht Wirksamkeitsueberpruefung
12) Medienmitteilung VBS vom 03.09.2013
13) Medienmitteilung VBS vom 20.3.2014.pdf
14) Medienmitteilung VBS vom 20.3.14.pdf
15) Medienmitteilung BR vom 4.5.17; Medienmitteilung BR vom 5.4.17
16) Medienmitteilung BR vom 26.4.18
17) Medienmitteilung SVS vom 16.5.19; Medienmitteilung SVS vom 28.3.19; Umsetzungsplan SVS Kantone
18) Medienmitteilung Bundesrat vom 26.04.2017
19) Bericht NCS 2018-2022; Medienmitteilung Bundesrat vom 19.04.2018
20) AB SR, 2017, S. 661 ff.; LZ, TA, 20.9.17
21) AB NR, 2017, S. 1994 ff.; Bericht SiK-NR vom 30.10.2017; SGT, TA, TG, 8.12.17
22) Rapport CF du 27.11.19
23) AB SR, 2017, S. 701 ff.; SGT, 26.9.17
24) AB NR, 2017, S. 2138 f.; Bericht SiK-NR vom 30.10.2017
25) AB SR, 2018, S. 110 f.; Bericht SiK-SR vom 30.10.2017; CdT, 7.3.18
26) Aktionsplan Cyberdefence
27) AB NR, 2017, S. 2120 f.
28) Bericht BR vom 15.6.17
29) BBl, 2020, S. 3380; Medienmitteilung SiK-NR vom 17.11.2020
30) AB NR, 2018, S. 87 f.; NZZ, 3.3.18
31) Plan de mise en oeuvre de la SNPC 2018-2022; Rapport CF du 27.11.19
32) AB NR, 2018, S. 217 f.
33) AB SR, 2018, S. 602 ff.; Bericht SiK-SR vom 13.8.18
34) AB NR, 2018, S. 210 f.
35) Rapport CF du 27.11.19
36) BO CN, 2020, p.1483 s
37) BWL (2018). Minimalstandard zur Verbesserung der IKT-Resilienz; Medienmitteilung BR vom 27.8.18
38) AB NR, 2019, S. 1324
39) Rapport du CF du 24.11.21
40) FF, 2022 858
41) Communiqué de presse du DDPS du 7.11.2019; AZ, 20.3.19; LT, 28.11.19; NZZ, 6.12.19
42) Communiqué de presse du DDPS du 11.12.20
43) BO CN, 2021, p. 662
44) Communiqué de presse DFF du 1.1.24; Rapport CF du 29.11.23; LT, 5.12.22
45) Communiqué de presse du CF du 1.9.21; FF, 2021, p.2198s
46) Communiqué de presse CPS-E du 2.11.21
47) BO CN, 2021, p. 2591 ss.; Communiqué de presse du CF du 24.11.21; Communiqué de presse du CF du 24.11.21 (2); CdT, Lib, 16.12.21
48) BO, CE, 2022, pp.27 s.
49) AB NR, 2022, S. 1036; AB NR, 2022, S. 586; Po. 21.4512
50) Bericht BR vom 13.11.24
51) Mo. 22.3836 - Curia Vista