année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

# Ausgewählte Beiträge zur Schweizer Politik

Prozess **Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**

# Impressum

**Herausgeber**

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

**Beiträge von**

Ackermann, Nadja
Schubiger, Maximilian

**Bevorzugte Zitierweise**

Ackermann, Nadja; Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, 2012 - 2017*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 12.10.2024.

# Inhaltsverzeichnis

**Allgemeine Chronik** 1
**Grundlagen der Staatsordnung** 1
Rechtsordnung 1
Äussere Sicherheit 1
Innere Sicherheit 1
**Landesverteidigung** 2
Bevölkerungsschutz 2

# Abkürzungsverzeichnis

| | |
|---|---|
| **EFD** | Eidgenössisches Finanzdepartement |
| **SVS** | Sicherheitsverbund Schweiz |
| **MELANI** | Melde- und Analysestelle Informationssicherheit |
| **NCS** | Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken |

| | |
|---|---|
| **DFF** | Département fédéral des finances |
| **RNS** | Réseau national de sécurité |
| **MELANI** | Centrale d'enregistrement et d'analyse pour la sûreté de l'information |
| **SNPC** | Stratégie nationale de protection de la Suisse contre les cyberrisques |

# Allgemeine Chronik

## Grundlagen der Staatsordnung

### Rechtsordnung

#### Äussere Sicherheit

**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. [1]

#### Innere Sicherheit

**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. [2]

**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. [3]

## Landesverteidigung

### 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. [4]

**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. [5]

---

1) Medienmitteilung Bundesrat vom 26.04.2017; NCS Bericht Wirksamkeitsueberpruefung
2) NZZ, 28.6.12.
3) BBl, 2013, S. 563 ff.; Medienmitteilung IBS vom 15.5.13 .pdf
4) Medienmitteilung VBS vom 27.6.12.
5) Jahresbericht Steuerungsausschuss NCS 2013.pdf; Medienmitteilung VBS vom 30.4.14.pdf