Nationales Forschungsprogramm NFP 86 «Digitale Resilienz kritischer Infrastrukturen»

Ausschreibung

Inhaltsverzeichnis

Was sind Nationale Forschungsprogramme (NFP)?

Die im Rahmen der Nationalen Forschungsprogramme durchgeführten Forschungsprojekte leisten einen Beitrag zur Bewältigung gesellschaftlicher Herausforderungen von nationaler Bedeutung.

Gestützt auf Art. 10 Abs. 2 Buchst. c des Bundesgesetzes über die Förderung der Forschung und der Innovation vom 14. Dezember 2012 (FIFG) bestimmt der Bundesrat die Fragestellungen und Schwerpunkte, die in den NFP untersucht werden sollen. Die volle Verantwortung für die Durchführung der Programme wird dem Schweizerischen Nationalfonds (SNF) übertragen. In Art. 3–9 der Verordnung zum Bundesgesetz über die Förderung der Forschung und der Innovation vom 29. November 2013 (V-FIFG) werden die NFP und ihre Lancierung beschrieben. Gemäss dieser Rechtsgrundlage können zwei verschiedene Verfahren zur Lancierung eines NFP führen:

1. Offene Ausschreibungsrunden
2. Thematisch definierte Ausschreibungsrunden

Die in diesem NFP behandelte Fragestellung ergibt sich aus letzterer und steht mit den aktuellen Strategien des Bundes sowie den Prioritäten der Bundesverwaltung im Einklang. Im Vergleich zum offenen Ausschreibungsverfahren hat dieses NFP eine kürzere Laufzeit, ein geringeres Budget und eine stärkere Verbindung zwischen Forschenden und der Bundesverwaltung zum Ziel. Die wissenschaftliche Begutachtung und die Förderentscheide erfolgen unabhängig von politischen Instanzen und im Einklang mit den Grundsätzen der wissenschaftlichen Exzellenz und der akademischen Freiheit.

Am 1. Juli 2025 beauftragte das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) den SNF, die Machbarkeit eines NFP zum Thema «Digitale Resilienz kritischer Infrastrukturen» zu prüfen und ein Programmkonzept zu erarbeiten, in dem die Ziele und die wichtigsten zu behandelnden Forschungsfragen definiert werden. Auf der Grundlage dieses Programmkonzepts beschloss der Bundesrat am 20. März 2026, das FP 86 «Digitale Resilienz kritischer Infrastrukturen» zu lancieren. Die Mitglieder der Leitungsgruppe wurden am 24. März 2026 vom Nationalen Forschungsrat des SNF gewählt. Die Leitungsgruppe hat diese Ausschreibung ausgearbeitet und ist für die strategische Leitung des Programms zuständig.

1 Zusammenfassung

Die Ausschreibung lädt zur Einreichung von Vorschlägen für Forschungsvorhaben ein, die im Nationalen Forschungsprogramm «Digitale Resilienz kritischer Infrastrukturen » (NFP 86) durchgeführt werden. Am 20. März 2026 hat der Schweizer Bundesrat das Programm in Auftrag gegeben, um die Widerstandsfähigkeit der kritischen Infrastrukturen der Schweiz gegenüber Cyberangriffen und anderen digitalen Störungen zu stärken. Damit werden Forschungsvorhaben gefördert, welche die Wissensbasis zu Schwachstellen und Risiken erweitern, technisch realisierbare und gesellschaftlich akzeptable Lösungen entwickeln und Steuerungs- und Koordinationsmechanismen für eine agile kollektive Cyberabwehr vorschlagen.

Das NFP 86 umfasst vier Forschungsschwerpunkte:

- Im Forschungsschwerpunkt «Daten» wird untersucht, welche Daten als relevante Cybersicherheitsdaten gelten und wie der Zugriff auf diese Daten sowie deren Aufbereitung, Schutz und Austausch zwischen Wissenschaft, Behörden und Betreibern kritischer Infrastrukturen verbessert werden können.

- Im Forschungsschwerpunkt «Bewährte Verfahren» wird untersucht, welche organisatorischen, technischen und betrieblichen Verfahren als Stand der Technik gelten und wie diese in den verschiedenen Sektoren der kritischen Infrastruktur der Schweiz übernommen, getestet, angepasst und übertragen werden können.

- Im Forschungsschwerpunkt «Anreize» werden die wirtschaftlichen, regulatorischen, verhaltensbezogenen und institutionellen Rahmenbedingungen untersucht, die Investitionen in die Cybersicherheit beeinflussen, und Wege aufgezeigt, wie organisatorische Entscheidungen mit der Resilienz auf Systemebene in Einklang gebracht werden können.

- Im Forschungsschwerpunkt «Kollektive Verteidigung» wird untersucht, wie Betreiber, Anbieter, Behörden, Regulierungsbehörden, Forschende und Nutzer:innen ihre Zuständigkeiten, den Informationsaustausch, die Risikobewertung und gemeinsame Reaktionen vor, während und nach Cybervorfällen koordinieren können.

Das NFP 86 dient der Förderung interdisziplinärer Forschung und umfasst transdisziplinäre Elemente, die für Eigentümer und Betreiber kritischer Infrastrukturen, Sicherheitsfachleute, Behörden, Regulierungsbehörden, Versicherungsgesellschaften, Forschende sowie Nutzer:innen kritischer Dienste von praktischer Bedeutung sind. Projekte müssen nicht-akademische Partner:innen einbeziehen, zum Wissensaustausch auf Programmebene beitragen und Ergebnisse hervorbringen, die in die Politik, die Regierungsführung, die organisatorische Praxis, die technische Umsetzung, die Ausbildung und die öffentliche Entscheidungsfindung einfliessen können.

Das Gesamtbudget des Programms beträgt 5 Millionen Franken, wovon 4,25 Millionen Franken für die Forschung vorgesehen sind. Es wird erwartet, dass etwa fünf bis zehn Projekte in den vier Forschungsschwerpunkten gefördert werden. Die Projektbudgets müssen zwischen 300 000 und 800 000 Franken liegen, und die Forschungsprojekte dürfen 18 bis 36 Monate dauern. Eine Mitfinanzierung durch andere Finanzierungsquellen (z. B. von nicht-akademischen Projektpartnern) wird ausdrücklich begrüsst.

Interessenbekundungen müssen bis zum 24. November 2026, 17:00 Uhr Schweizer Zeit, eingereicht werden und Gesuche sind bis zum 19. Januar 2027, 17:00 Uhr Schweizer Zeit, einzureichen. Die endgültigen Förderentscheide des Forschungsrats werden spätestens im August 2027 erwartet. Die Forschungsarbeiten im Rahmen der geförderten Projekte müssen bis zum 1. November 2027 beginnen.

2 Einleitung

2.1 Hintergrund und Problemstellung

Die Digitalisierung unserer modernen Gesellschaft bietet viele Vorteile, birgt aber auch Risiken.[1] Während sich die Digitalisierung kritischer Infrastrukturen beschleunigt hat, hat die Sicherheit der zugrunde liegenden Systeme nicht immer Schritt gehalten. Diese kritische Infrastruktur betrifft mittlerweile viele Lebensbereiche, darunter die Energieversorgung, das Gesundheitswesen, den öffentlichen und gewerblichen Verkehr, die Logistik, das Bauwesen, die Kommunikation, die Landwirtschaft sowie die Wasserversorgung und Abwasserentsorgung. Allein in der Schweiz sind Millionen von Geräten – mehr als das Land Einwohner:innen hat – mit dem Internet verbunden. Leider wurde die Sicherheit bei den meisten vernetzten Geräten nicht von Anfang an berücksichtigt – entweder, weil Bedrohungen und Schwachstellen noch nicht bekannt waren, oder weil die entsprechenden Schutzmassnahmen für Einzelpersonen und Organisationen als zu aufwendig, komplex oder kostspielig eingeschätzt wurden. Unterdessen nehmen Cyberangriffe auf kritische Infrastrukturen zu, auch in der Schweiz. Spitäler kamen zum Stillstand, Ransomware-Angriffe beeinträchtigten den öffentlichen Verkehr und in öffentlichen Verwaltungen kam es zu Datenschutzverletzungen. Diese Ereignisse verdeutlichen die zunehmende Anfälligkeit der digitalen Infrastruktur der Schweiz. Da sich die Digitalisierung immer weiter beschleunigt, werden die Fähigkeiten und Ressourcen böswilliger Akteure immer umfangreicher. Ein Ende der Zunahme von Zahl, Vielfalt und Ausmass der versuchten Cyberangriffe ist nicht in Sicht.

Wie jedes andere Land steht auch die Schweiz aufgrund ihrer besonderen Merkmale vor ganz eigenen Herausforderungen und Chancen. Das Land ist klein und weist einen hohen technischen Entwicklungsstand auf. Gleichzeitig trägt die Aufsplitterung der Zuständigkeiten zwischen Bund, Kantonen und Gemeinden zur Trennung zwischen staatlichen Stellen und privaten Betreibern bei, was koordinierte Massnahmen erschwert. Zudem werden die Kosten für Cybersicherheit – wie in vielen anderen Ländern auch – als Hindernis für Innovationen angesehen, obwohl das Risiko von Angriffen weit verbreitet ist.

Dieses NFP soll die Widerstandsfähigkeit der kritischen Infrastrukturen der Schweiz[2] gegenüber Cyberangriffen stärken. Dies beginnt mit der Schaffung einer solideren Wissensgrundlage über Schwachstellen und Risiken im Hinblick auf die derzeitige digitale Resilienz der kritischen Infrastrukturen des Landes, umfasst aber auch die Ermittlung technisch realisierbarer und gesellschaftlich akzeptabler Lösungen sowie den Vorschlag umfassender Strategien zur Umsetzung dieser Lösungen, um die digitale Widerstandsfähigkeit der kritischen Infrastrukturen des Landes zu stärken. Darüber hinaus zielt das Programm darauf ab, die nationale Koordination und Steuerung im Bereich der Cybersicherheit zu verbessern.

---

[1] C. Herley und P. C. Van Oorschot. *SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit*. IEEE Symposium on Security and Privacy (SP) 2017, S. 99–120. https://ieeexplore.ieee.org/document/7958573

[2] Weitere Informationen zur Definition kritischer Infrastrukturen in der Schweiz finden Sie beim Bundesamt für Bevölkerungsschutz (BABS): https://www.babs.admin.ch/de/die-kritischen-infrastrukturen

2.2 Nationales und internationales Forschungsumfeld

Die Schweiz ist zwar äusserst innovativ, doch fehlen ihr die Ressourcen, um Ideen in die industrielle Produktion umzusetzen. Zwar entstehen Fachgemeinschaften, und die Zusammenarbeit zwischen Wirtschaft, Wissenschaft und Staat nimmt zu, doch die Schweiz benötigt nach wie vor strengere gesetzliche Regelungen, mehr Ressourcen und einen intensiveren Datenaustausch. In anderen Ländern wurde die Cybersicherheit bereits deutlich früher zu einer nationalen Priorität – sowohl in der Forschungsförderung als auch bei der staatlichen Fachkompetenz. In Deutschland beispielsweise wurde das BSI bereits 1991 gegründet, während die ersten Schritte zum Aufbau des Schweizer NCSC erst im Jahr 2020 unternommen wurden. Dennoch kann die Schweiz dank ihrer politischen Rahmenbedingungen und ihrer führenden Forschungsteams eine Schlüsselrolle auf internationaler Ebene im Bereich der Cyberresilienz spielen.

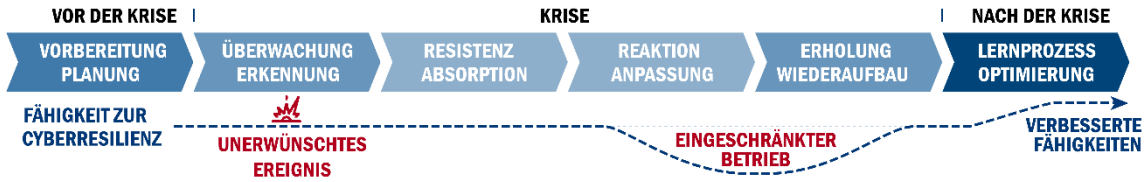
Digitale Resilienz ist auch ein wichtiges internationales Thema. So wurde beispielsweise im Jahr 2025 in Saudi-Arabien vom Global Cybersecurity Forum (GCF) und dem Weltwirtschaftsforum (WEF) das Centre for Cyber Economics (CCE) ins Leben gerufen – eine Plattform, auf der Stakeholder eine fundierte Entscheidungsfindung im Bereich der Cyberresilienz unterstützen. Die Länder verfolgen unterschiedliche Strategien: Die USA und China haben ihren Schwerpunkt auf eine Sicherheitspolitik verlagert, die andere Länder durch Vorschriften und Beschränkungen ins Visier nimmt, während andere Nationen den Schwerpunkt auf die Wirtschaft legen.

3 Ziele des Nationalen Forschungsprogramms

Das übergeordnete Ziel des NFP 86 ist es, die Widerstandsfähigkeit der Schweiz gegenüber Cyberangriffen langfristig zu stärken, indem in den Aufbau einer agilen und technologisch fortschrittlichen kollektiven Verteidigung investiert wird. Konkret geht es darum, die Fähigkeit kritischer Infrastrukturen zu verbessern, digitalen Störungen wie Cyberangriffen oder Systemausfällen standzuhalten, sich anzupassen und sich davon zu erholen, um so sicherzustellen, dass der Betrieb effektiv fortgesetzt werden kann. Dazu gehört nicht Erhöhung der Zahl und des Anteils der Angriffe, die kritische Infrastrukturen abwehren oder unbeschadet überstehen können, sondern auch die Reaktion auf erfolgreiche Angriffe und deren Eindämmung (Grafik 1).

Das NFP 86 wird die Widerstandsfähigkeit der kritischen Infrastrukturen der Schweiz in sensiblen Sektoren wie Gesundheitswesen, Verkehr, Landwirtschaft, Trinkwasserversorgung und Abwasserentsorgung verbessern, indem es bestehende Schutzmassnahmen bewertet und validiert sowie neuartige präventive Ansätze entwickelt, die über rein technische Massnahmen hinausgehen. Um die nationale Cyberinfrastruktur ganzheitlich und langfristig zu stärken, ist es wichtig, den Austausch relevanter Informationen zwischen den beteiligten Akteuren – darunter Behörden, Unternehmen und Hochschulen – zu fördern. Die zukünftige Forschung im Bereich der Cybersicherheit benötigt kontinuierlich realistische und aktuelle Sicherheitsdaten. Daher ist es von entscheidender Bedeutung, Koordinations- und Steuerungsmechanismen zu ermitteln und zu stärken, die der fragmentierten digitalen Landschaft gerecht werden. Die derzeitigen Prozesse müssen besser verstanden, bewertet und gegebenenfalls angepasst werden. Dazu gehören nicht nur der Einsatz von Abwehr- und Schutzmechanismen, sondern auch die kontinuierliche Sicherheitsüberprüfung kritischer Infrastrukturen sowie strukturierte Reaktionen auf Vorfälle. Es bedarf einer schlüssigen Theorie für eine effektive Resilienz-Praxis, die alle Bereiche und Arten kritischer Infrastrukturen umfasst. Um der steigenden Zahl von Cyberangriffen entgegenzuwirken, sind strategisches Denken und etablierte Prozesse erforderlich.

Das Verständnis der umfassenderen sozialen und wirtschaftlichen Dynamiken, die die Cybersicherheit und die damit verbundenen Investitionsanreize prägen, ist nach wie vor begrenzt. Um die digitale Resilienz auf nachhaltige und kostengünstige Weise zu stärken, müssen wirksame Investitionen ermittelt werden. Zudem geht es darum, in einem von Unsicherheit geprägten Umfeld in Organisationen und miteinander verflochtenen Systemen zu verstehen, wie Entscheidungen im Rahmen regulatorischer und verhaltensbezogener Einschränkungen getroffen werden. Da Angriffe immer raffinierter werden, ist es zunehmend unhaltbar, sich darauf zu verlassen, dass Versicherungen die Folgen abfedern. Investitionen in die Sicherheit können zudem Geschäftsmodelle unterstützen und Erträge generieren, die ihre Kosten ausgleichen. Es ist ein gemeinsamer Ansatz im Bereich der Verteidigung erforderlich, der alle Stakeholder, Akteure sowie die Anfälligkeit gegenüber Angriffen auf die Lieferkette und Software-Monokulturen berücksichtigt. Dieser muss agil genug sein, um sich rasch an ein sich schnell wandelndes Umfeld anzupassen – und zwar in einem globalen Kontext, in dem die Staaten zunehmend bestrebt sind, eine Form der digitalen Selbstbestimmung zu erlangen. Zudem sehen sich alle westlichen Staaten mittlerweile mit hybrider Kriegsführung konfrontiert, was eine Untersuchung der menschlichen Reaktionen auf Angriffe und Vorfälle erfordert, um sich auf Angriffe vorzubereiten, bei denen Menschen die nationale Infrastruktur angreifen.



Grafik 1: Reaktion auf einen erfolgreichen Angriff und Umsetzung von Massnahmen zur Stärkung der digitalen Resilienz.[3] Das NFP 86 zielt darauf ab, durch eine hochmoderne, agile und kollektive Cyberabwehr zu verhindern, dass Cyberangriffe erfolgreich sind, und, falls es doch zu Angriffen kommt, deren Folgen zu begrenzen und die Strategie rasch anzupassen, um zu verhindern, dass künftige Angriffe erfolgreich sind.

4 Forschungsschwerpunkte

Das NFP 86 zielt darauf ab, die Cyberresilienz kritischer Infrastrukturen in der Schweiz zu verbessern, wobei der Schwerpunkt insbesondere auf interdisziplinären und transdisziplinären Forschungsaktivitäten im breiteren Ökosystem der Cybersicherheit liegt. Im Mittelpunkt des Programms stehen die folgenden vier Forschungsthemen, die nicht nur technische Aspekte, sondern auch Sozial- und Geisteswissenschaften sowie die rechtlichen und regulatorischen Rahmenbedingungen abdecken. Von den Projekten wird erwartet, dass sie bei ihrer Konzeption sowohl technische als auch nicht technische Aspekte berücksichtigen, um dem interdisziplinären Anspruch des Programms gerecht zu werden. Das NFP 86 bittet um Beiträge zu den folgenden Forschungsschwerpunkten:

4.1 Daten

Um den aktuellen Stand der Cybersicherheit zu evaluieren, Schwachstellen und Sicherheitslücken zu identifizieren, technische Lösungen zu erforschen und die Bemühungen zu koordinieren, sind Daten erforderlich. Forschende haben in der Regel keinen Zugang zu Daten von Betreibern kritischer Infrastrukturen und können daher bestimmte Experimente und Forschungsarbeiten nicht durchführen oder

[3] In Anlehnung an Araujo, M.S.d.; Machado, B.A.S.; Passos, F.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Appl. Sci.* **2024**, *14*, 2116. https://doi.org/10.3390/app14052116

passen ihre Lösungen letztendlich zu stark an einzelne Datenpunkte an. Staatliche Einrichtungen verfügen zwar über Daten, können diese jedoch nicht einfach an beliebige Interessent:innen oder gar untereinander weitergeben. Ebenso zögern Unternehmen, Daten weiterzugeben, da sie befürchten, damit Sicherheits- oder Geschäftsstrategien preiszugeben oder ihre Schwachstellen einzugestehen. Es sind methodisch fundiertere und praxisorientiertere Ansätze sowie möglicherweise gesetzliche Regelungen erforderlich, um den Austausch relevanter und verwertbarer Daten zwischen Wissenschaft, Industrie und Behörden zu erleichtern und zu intensivieren. Die Entwicklung von Governance-Rahmenwerken, die Transparenz und Sicherheitsanforderungen in Einklang bringen, wie die Berücksichtigung rechtlicher Vorgaben wie der Datenschutzpflichten gemäss dem neuen Bundesdatenschutzgesetz (BDSG-neu), Vertraulichkeitsvorschriften sowie die Ermittlung von unterstützenden Mechanismen, einschliesslich geeigneter Rechtsgrundlagen, Anonymisierungsstandards und Haftungsregelungen, ist daher eine Priorität dieses Programms.

Dieser Forschungsschwerpunkt befasst sich mit den rechtlichen, regulatorischen, vertraglichen und technischen Rahmenbedingungen, unter denen *relevante Daten abgerufen, weitergegeben und genutzt werden können* für Forschung, operative Tätigkeiten und öffentliche Entscheidungsfindung in der Schweiz.

Beispiele für Fragestellungen, mit denen sich Projekte in diesem Forschungsschwerpunkt befassen könnten, sind unter anderem:

- *Welche rechtlichen und regulatorischen Rahmenbedingungen ermöglichen oder schränken derzeit den Datenaustausch zwischen Behörden, Betreibern kritischer Infrastrukturen und Forschenden ein, und wie könnten diese reformiert oder ergänzt werden, auch im Hinblick auf Haftungsregelungen?*
- *Welche Governance-Modelle und institutionellen Regelungen können einen kontrollierten, sicheren und rechtskonformen Datenaustausch zwischen den Anspruchsgruppen ermöglichen, auch über die Grenzen zwischen dem öffentlichen und dem privaten Sektor hinweg?*
- *Welche Bedingungen müssen erfüllt sein, damit Daten zu Vorfällen und Schwachstellen unter Einhaltung der Datenschutzanforderungen weitergegeben werden können? Ist eine Anonymisierung oder Pseudonymisierung erforderlich, und wenn ja, welche Standards wären ausreichend – auch im Rahmen der Echtzeitreaktion auf Vorfälle – und wie lässt sich die Einhaltung dieser Standards in der Praxis überprüfen?*
- *Welche Mechanismen – darunter isolierte Forschungsumgebungen und vertrauenswürdige Drittanbieter – könnten Forschenden einen realistischen Zugang zu Betriebsdaten ermöglichen, ohne dabei Sicherheits- oder Vertraulichkeitsverpflichtungen zu gefährden?*
- *Wie und unter welchen Bedingungen lässt sich der Datenaustausch zwischen den Bundes- und Kantonsbehörden in der Schweiz umsetzen, und welche gesetzlichen oder regulatorischen Änderungen wären dafür erforderlich?*
- *Inwiefern könnten internationale Datenströme und grenzüberschreitende Daten zu Sicherheitsvorfällen die rechtlichen Rahmenbedingungen für den Datenaustausch in der Schweiz beeinflussen, und wie lassen sich die schweizerischen Rechtsvorschriften an EU-Rechtsakte wie die EU-Datenverordnung (Verordnung 2023/2854) oder die NIS-2-Richtlinie (Richtlinie 2022/2555) anpassen, ohne die Souveränität zu beeinträchtigen?*

4.2 Bewährte Verfahren

Sowohl staatliche Einrichtungen als auch Unternehmen führen Sicherheitslösungen oft nur zögerlich ein, da sie vermeintliche Einstiegshürden sehen oder sich der Vorteile nicht bewusst sind. Prozesse müssen getestet und angepasst werden; zwar schreiben Rahmenwerke wie ISO 27001 vor, wie dies

zu geschehen hat, doch viele der derzeitigen als bewährt geltenden Richtlinien, Standards und Verfahren im Bereich der Cybersicherheit werden nicht gründlich getestet. Der Umgang mit der Komplexität der Lieferkette, den Risiken von Software-Monokulturen und der steigenden Zahl von Cyberangriffen erfordert strategisches Denken und etablierte Prozesse, darunter kontinuierliche Sicherheitstests und eine strukturierte Reaktion auf Vorfälle. Es ist zudem unklar, inwieweit sich Verfahren aus einem Bereich oder einer Art kritischer Infrastruktur auf andere übertragen lassen. Darüber hinaus fehlt eine schlüssige Theorie für wirksame Massnahmen zur Stärkung der Resilienz.

Dieser Forschungsschwerpunkt befasst sich damit, *welche bewährten Verfahren dem aktuellen Stand der Technik entsprechen* und wie sie umgesetzt werden können, um eine Wissensbasis aufzubauen, die den sektorübergreifenden Transfer von Resilienz-Praktiken unterstützt und als Leitfaden für die künftige Umsetzung in der Schweiz dient.

Beispiele für Fragestellungen, mit denen sich Projekte in diesem Forschungsschwerpunkt befassen könnten, sind unter anderem:

- *Anhand welcher Kriterien und Kennzahlen sollten die Wirksamkeit und die Rentabilität der derzeitigen Verfahren bzw. Lösungen evaluiert werden?*
- *Welche organisatorischen und technischen Massnahmen tragen derzeit am meisten zur Prävention, Erkennung, Reaktion, Aufrechterhaltung des Betriebs und zur Wiederherstellung in den kritischen Infrastrukturen der Schweiz bei?*
- *Wie lassen sich erfolgreiche Cybersicherheitspraktiken aus einem Sektor der kritischen Infrastruktur (z. B. Energie) systematisch auf andere Sektoren (z. B. Gesundheitswesen oder Verkehr) übertragen?*
- *Wie lassen sich bewährte Verfahren für Beschaffung, Konfiguration, Patching, Überwachung, Tests und Krisenmanagement an Organisationen unterschiedlicher Grösse und Struktur anpassen?*
- *Welche Rahmenkonzepte für das Risikomanagement in der Lieferkette sind am wirksamsten, um die Exposition gegenüber Hardware- und Softwarerisiken zu verringern?*
- *Welche Rolle spielen Unternehmenskultur, Führung und Kommunikation bei der erfolgreichen Einführung und Aufrechterhaltung bewährter Verfahren im Bereich der Cybersicherheit?*

4.3 Anreize

Viele wirksame Lösungen für Verteidigung und Schutz werden aufgrund der vermeintlich hohen Kosten nur widerwillig umgesetzt. Unternehmen betrachten Cybersicherheit als Kostenfaktor ohne greifbaren Ertrag und gehen manchmal davon aus, dass die Folgen von Angriffen aufgrund unterschätzter Wahrscheinlichkeiten weniger kostspielig sind – obwohl die zunehmende Raffinesse der Angriffe solche Annahmen infrage stellt. Sicherheit kann Geschäftsmodelle unterstützen und Einnahmen generieren, welche die Investitionen ausgleichen. Uns fehlen Methoden, um das soziale und wirtschaftliche System rund um die Cybersicherheit sowie die Anreize für Investitionen zu analysieren. Für eine bezahlbare und nachhaltige Resilienz ist ein besseres Verständnis des Kosten-Nutzen-Verhältnisses sowie der Art und Weise erforderlich, wie Investitionsentscheidungen trotz Unsicherheiten in Organisationen und zwischen voneinander abhängigen Systemen getroffen werden.

Dieser Forschungsschwerpunkt befasst sich mit *der Frage, welche Anreize Investitionen in die Sicherheit fördern und wie diese verstärkt werden können*, wobei der Schwerpunkt auf den wirtschaftlichen, regulatorischen, verhaltensbezogenen und institutionellen Rahmenbedingungen liegt, die Investitionsentscheidungen im Bereich der Cybersicherheit beeinflussen.

Beispiele für Fragestellungen, mit denen sich Projekte in diesem Forschungsschwerpunkt befassen könnten, sind unter anderem:

- *Welche wirtschaftlichen, verhaltensbezogenen, regulatorischen und organisatorischen Faktoren erklären gemeinsam die anhaltende Unterfinanzierung im Bereich der Sicherheit in kritischen Infrastrukturen? Wie lässt sich der Wert von Sicherheit und Resilienz (einschliesslich finanzieller, operativer und systemischer Vorteile, wie etwa der Verhinderung von Kettenausfällen) quantifizieren und in Kennzahlen übersetzen, die als Grundlage für die Entscheidungsfindung der Unternehmensleitung dienen?*
- *Wie lässt sich ein Rahmenkonzept zum «Wert der Resilienz» mithilfe von Entscheidungsschnittstellen (z. B. Dashboards, Simulationen, Darstellungen) und Instrumenten operationalisieren, um Investitionsentscheidungen in einem von Unsicherheit geprägten Umfeld zu unterstützen?*
- *Wie würde ein praktisches, adaptives Instrument zur Entscheidungsfindung bei Sicherheitsinvestitionen aussehen, das die Dynamik von Bedrohungen, die Risikoexposition von Organisationen und branchenübergreifende Wechselwirkungen berücksichtigt?*
- *Welche Kombinationen aus regulatorischen und Anreiz-basierten Mechanismen können die Sicherheitsinvestitionen von Organisationen mit den Resilienzzielen auf Systemebene in Einklang bringen, dabei sektorübergreifende Wechselwirkungen berücksichtigen und einen durch Compliance-Anforderungen bedingten Minimalismus vermeiden?*

4.4 Kollektive Verteidigung

Kritische nationale Infrastrukturen sind keine monolithischen Systeme, sondern bestehen vielmehr aus einer Vielzahl von Hardware- und Softwarekomponenten, Diensten und den Menschen, die diese warten. Angriffe auf einzelne Bestandteile können Auswirkungen auf grössere Teile kritischer Infrastrukturen haben, doch den Betreibern sind diese Auswirkungen häufig nicht bewusst. Eine wirksame Widerstandsfähigkeit erfordert daher eine Form der kollektiven Verteidigung, die alle Beteiligten berücksichtigt, insbesondere die Lieferkette. Da vergangene Vorfälle gezeigt haben, dass die Bevölkerung gezielt für Angriffe ausgenutzt werden kann, muss dieser Aspekt auch auf die Endnutzer:innen sowie die Nutzniessenden kritischer Dienste ausgedehnt werden. Ausgehend vom Bewusstsein für gegenseitige Abhängigkeiten brauchen wir Forschungsarbeiten zu der Frage, wie der Austausch zwischen allen Beteiligten, und der gemeinsame Risikobewertungs-Prozess verbessert werden kann.

Dieser Forschungsschwerpunkt befasst sich mit *der Frage, wie wir eine kollektive Verteidigung unter Einbeziehung aller Beteiligten erreichen können,* wobei der Schwerpunkt darauf liegt, wie diese im Schweizer Kontext organisiert werden kann, wie Wechselwirkungen verstanden und gesteuert werden können und wie interdisziplinäre Ansätze technische, organisatorische, rechtliche und soziale Dimensionen bei heterogenen Akteuren in einer sich rasch wandelnden Bedrohungslandschaft miteinander verbinden können.

Beispiele für Fragestellungen, mit denen sich Projekte in diesem Forschungsschwerpunkt befassen könnten, sind unter anderem:

- *Wie lassen sich Wechselwirkungen innerhalb und zwischen kritischen Infrastrukturen für ein kollektives Risikomanagement identifizieren, abbilden und priorisieren?*
- *Welche Formen der Koordination, des Informationsaustauschs und der gemeinsamen Entscheidungsfindung sind zwischen Betreibern, Lieferanten, Regulierungsbehörden und Einsatzkräften am wirksamsten? Welche Formen der strategischen und opportunistischen Zusammenarbeit bieten die beste Grundlage für die kollektive Verteidigung kritischer Infrastrukturen? Lässt sich beispielsweise das Modell «Team von Teams» auf CNIs anwenden?*

- *Wie lässt sich das Double-Loop-Lernen auf CNIs anwenden? Wie lassen sich Erkenntnisse aus Vorfällen, Übungen und Beinaheunfällen erfassen und analysieren, um kollektive Verteidigungsstrategien zu entwickeln, agilere Reaktionen auf Informationen und Frühwarnsignale zu formulieren und die Steuerung zu verbessern (z. B. Zuständigkeitsverteilung, Weiterentwicklung von Fähigkeiten und Kapazitätsausbau)?*
- *Welche Rolle sollten Behörden, Branchenaufsichtsbehörden und internationale Organisationen bei der Koordination der nationalen Cyberabwehr spielen, und wie lassen sich diese im Schweizer Kontext stärken?*
- *Welche Massnahmen können ergriffen werden, um die Bürger:innen als zusätzliche Verteidigungsebene («Sensoren») zu befähigen und zu unterstützen, beispielsweise durch Sensibilisierung für Social Engineering und Desinformation als Angriffsvektoren gegen kritische Infrastrukturen, durch die Einbindung der Bürger:innen bei der Bereitstellung von Informationen oder Frühwarnsignalen sowie durch Anreize für den Zugang zu und den Austausch von relevanten Daten und die Überprüfung ihrer Gültigkeit (mithilfe von KI oder gegenseitiger Verifizierung, Gemeinschaftsaktivitäten usw.)?*

5 Implementierung und erwartete Ergebnisse

5.1 Implementierung

Um die erwarteten Ergebnisse zu erzielen, kommen folgende Implementierungsmöglichkeiten infrage:

- Stärkung der Interaktion zwischen den Stakeholdern durch projektbezogene Forschung, Öffentlichkeitsarbeit auf Programmebene, Partnerschaften mit bestehenden Initiativen sowie sektorübergreifende Massnahmen.
- Einrichtung von Kanälen für den Datenaustausch und der damit verbundenen rechtlichen und administrativen Rahmenbedingungen (einschliesslich Datenschutzbestimmungen, Anonymisierungsstandards, zulässiger Verwendungszwecke, Vertraulichkeitsverpflichtungen und Haftungsregeln), wobei diese als erwartete Programmergebnisse und nicht als selbstverständliche Voraussetzungen betrachtet werden.
- Unterstützung bei der Umsetzung von Arbeitsabläufen, Leitfäden, Protokollen und Methoden zur Cyberresilienz für kontinuierliche Tests, die Reaktion auf Vorfälle, die Wiederherstellung und die Anpassung, ergänzt durch offizielle Richtlinien und Vorschriften, wo dies erforderlich ist.
- Erstellung einer Reihe von Ergebnissen, darunter praxisorientierte Publikationen, Lehr- und Schulungsmaterialien, begutachtete wissenschaftliche Publikationen, FAIR-konforme Datensets, validierte Tools und öffentliche Kommunikation über verschiedene Medien hinweg; gegebenenfalls Entwicklung von pilotgetesteten Produkten oder Lösungen.
- Aktive Einbindung akademischer Projektteams in berufliche und nicht-akademische Umgebungen, um den Dialog über den Datenaustausch und einen konstruktiven Austausch mit Anwender:innen zu fördern.
- Förderung der direkten Einbindung von Stakeholdern in Forschungsprojekte durch Praxispartnerschaften und Mitfinanzierungsvereinbarungen, die Anreize, Risiken in der Lieferkette und im Zusammenhang mit Monokulturen sowie menschliche Faktoren berücksichtigen.
- Entwicklung von Massnahmen zur Öffentlichkeitsarbeit und zum Aufbau von Partnerschaften in Verbindung mit rechtlichen Rahmenbedingungen, die den beteiligten Stakeholdern durch Vertraulichkeitsgarantien und klare Regeln zur Nutzung der weitergegebenen Informationen durch Forschungsteams und Behörden einen angemessenen Schutz bieten.

5.2 Erwartete Ergebnisse

Das NFP 86 zielt durch die Erarbeitung von praxisorientiertem Wissen, validierten Instrumenten, Governance-Modellen und Koordinationsmechanismen für kritische Infrastrukturen darauf ab, die digitale Resilienz in der Schweiz zu stärken. Zu den möglichen Ergebnissen gehören unter anderem:

- Umsetzung einer hochmodernen, agilen kollektiven Cyberabwehr und Entwicklung einer Theorie für effektive Praktiken unter Einbeziehung von Erkenntnissen aus vergangenen Vorfällen zur Stärkung der Resilienz.
- Verbesserte Kommunikation und Zusammenarbeit zwischen Wissenschaft, Praxis und anderen Anspruchsgruppen, wobei Forschungsergebnisse von nicht-akademischen Akteuren, insbesondere von Eigentümern und Betreibern kritischer Infrastrukturen, aktiv genutzt werden.
- Verstärkter Austausch relevanter Daten zu Betrieb, Vorfällen und Schwachstellen zwischen den Beteiligten, z. B. Forschenden, Betreibern kritischer Infrastrukturen und staatlichen Stellen.
- Fortschritte bei der Umsetzung und Einführung von Leitfäden, Vorschriften, Protokollen und Strategien zur Erprobung von Verteidigungsmassnahmen, zur Priorisierung von Investitionen und zur Koordination von Massnahmen zur Stärkung der Cyberresilienz.
- Einstellungs- und Verhaltensänderungen bei Eigentümern, Betreibern und Endnutzer:innen kritischer Infrastrukturen, um sie für Social Engineering, Desinformation und hybride Bedrohungen zu sensibilisieren.
- Ausbildung einer neuen Generation von Führungskräften im Bereich digitaler Transformation mit umfassender Expertise im Bereich Cyberresilienz, die über rein technisches Wissen hinausgeht.

6 Merkmale des NFP und Anforderungen an die Forschung

6.1 Lösungsorientierter Ansatz

Alle Projekte sollen sich an den Forschungsschwerpunkten 1, 2, 3 oder 4 orientieren, im Idealfall an mehr als einem. Zudem müssen die Projekte lösungsorientiert und praxisnah sein. Die Forschungsgesuche sollten eine Erörterung der praktischen Bedeutsamkeit des Projekts sowie konkrete Vorschläge für die praktische Umsetzung der Projektergebnisse enthalten. Das NFP 86 fördert keine Grundlagenforschung, die keine praxisorientierten Ergebnisse hervorbringt. Die Gesuchstellenden sollten öffentlichkeitswirksame Massnahmen vorschlagen, um den Austausch mit den Stakeholdern zu fördern.

6.2 Interdisziplinärer Forschungsansatz

Wie oben dargelegt, ist Cybersicherheit ein vielschichtiges Problem, das zahlreiche Stakeholder betrifft. Der Erfolg des vorgeschlagenen Programms hängt entscheidend von der engen Zusammenarbeit zwischen Fachleuten aus verschiedenen Disziplinen ab, darunter unter anderem Vertreter:innen der folgenden Bereiche:

- Cybersicherheit (Daten-/Informationssicherheit, Systemsicherheit, Softwaresicherheit, angewandte Kryptographie)
- Verhaltensforschung (Vertrauenswürdigkeit, benutzerfreundliche Sicherheit, Sicherheitserziehung/-schulung)
- Recht, Regulierung und öffentliche Politik (Datenschutz und Privatsphäre, Haftungsregelungen, Vertragsrecht, Regulierungsgestaltung und öffentliches Recht im Bereich kritischer Infrastrukturen)
- Sozioökonomie (Anreize, Lieferkette)

Daher müssen **alle Projekte sowohl die technischen als auch die nicht technischen Dimensionen der digitalen Resilienz inhaltlich berücksichtigen**, einschliesslich – soweit relevant – menschlicher, rechtlicher und organisatorischer Aspekte. Die Gesuchstellenden müssen in einem eigens dafür vorgesehenen Abschnitt des Gesuchs ausdrücklich darlegen, wie dies umgesetzt wird.

6.3 Elemente der transdisziplinären Forschung

Da das Programm darauf abzielt, Wissen und Lösungen zu generieren, welche relevant und anwendbar sind und der Realität der kritischen Infrastrukturen der Schweiz entsprechen, **müssen alle Projekte mindestens eine:n nicht-akademische:n Partner:in einbeziehen**. Diese:r Partner:in muss in einem für kritische Infrastrukturen relevanten Sektor oder einer entsprechenden Funktion tätig sein, dort Dienstleistungen erbringen, diesen regulieren, unterstützen oder anderweitig direkt daran beteiligt sein. Dazu können Betreiber, Dienstleister, Behörden, Regulierungsbehörden oder andere relevante Akteure gehören, deren Tätigkeit sich auf die Resilienz, die Kontinuität oder die Sicherheit kritischer Infrastrukturdienste auswirkt.

Der Erfolg des NFP 86 hängt von einem zeitnahen Wissensaustausch, der konkreten Einbindung der Anspruchsgruppen und der Umsetzung der Forschungsergebnisse in praxistaugliche Verfahren ab. Von den Gesuchstellenden wird erwartet, dass sie darlegen, wann und wie der bzw. die nicht-akademischen Partner:innen im Verlauf des Projekts einbezogen werden, damit diese Einbindung konkret, zeitnah und sinnvoll ist und nicht nur rein formeller Natur bleibt. Die wichtigsten im NFP 86 berücksichtigten Anspruchsgruppen sind in der folgenden Tabelle zusammengefasst:

Anspruchsgruppe	**Rolle im NFP 86**
Betreiber kritischer Infrastrukturen	Entscheidungsverantwortliche, die für die Resilienzstrategie, die Ressourcen und die Steuerung zuständig sind
Anbieter und technische Personal	Sie führen Dienste aus, warten Systeme, bearbeiten Störungen und stellen technisches Wissen und Daten bereit.
Sicherheitsfachpersonen und weitere Expert:innen	Sie schätzen Bedrohungen ein, entwickeln und testen Abwehrmassnahmen und setzen Forschungsergebnisse in operative Sicherheitsverfahren um.
Mitarbeitende in kritischen Bereichen und Nutzer:innen	Sie nutzen kritische Systeme, um Dienste bereitzustellen und tragen dazu bei, die Benutzerfreundlichkeit, Arbeitsabläufe und Akzeptanz zu bewerten.
Kund:innen, Auftraggeber:innen und Bürger:innen	Sie sind auf kritische Dienste angewiesen und können von Ausfällen, Desinformationen, Social Engineering usw. betroffen sein.
Versicherungsgesellschaften	Sie beeinflussen die Preisbildung, die Übertragung von Cyberrisiken und die Offenlegungspraxis und tragen zur Gestaltung von Investitionsanreizen bei.
Juristische Fachpersonen, Gesetzgeber und Regulierungsbehörden	Sie legen Rechtsgrundlagen, Vertraulichkeitsvorschriften, Haftungsmodelle, Regulierungsinstrumente und politische Rahmenbedingungen fest.
Politische Entscheidungsträger:innen und Behörden	Sie nutzen die Ergebnisse für öffentliche Entscheidungen, Koordinationsaufträge, Krisenvorsorge und Massnahmen zur Stärkung der Resilienz.
Sicherheitsforschende und wissenschaftliche Partner:innen	Sie erarbeiten Erkenntnisse, Methoden, Rahmenwerke, Werkzeuge, FAIR-konforme Datensets und interdisziplinäre Schulungsangebote.

Forschungspläne müssen eine überzeugende Umsetzungsstrategie enthalten: Gesuchstellende werden gebeten, klar formulierte und umsetzbare Projektergebnisse zu definieren, die realistisch in der Praxis, der Politik, der Verwaltung, in organisatorischen Prozessen oder im Rahmen der technischen Implementierung umgesetzt werden können.

6.4 Datenzugang, Datenmanagement und offene Forschungsdaten

Die Ergebnisse öffentlich finanzierter Forschung sollten der Öffentlichkeit so weit wie möglich kostenlos zugänglich sein. Der SNF setzt sich durch Open Science (snf.ch) für dieses Ziel ein. Bei den meisten Förderangeboten müssen Forschende ihrem Gesuch einen Data Management Plan (DMP) beifügen. Gleichzeitig erwartet der SNF, dass die im Rahmen von SNF-geförderten Projekten generierten Daten in digitalen FAIR-Datenbanken öffentlich zugänglich sind (wobei sichergestellt sein muss, dass die Daten auffindbar, zugänglich, interoperabel und wiederverwendbar sind), sofern keine rechtlichen, ethischen, urheberrechtlichen oder sonstigen Probleme bestehen.

7 Einreichungs- und Evaluationsverfahren

7.1 Allgemeine Bedingungen

Rechtliche Grundlage: Die Gesuche müssen den in dieser Ausschreibung dargelegten Bestimmungen entsprechen. Darüber hinaus und sofern in dieser Ausschreibung keine spezifischen Bestimmungen festgelegt sind, gelten das Beitragsreglement des SNF sowie das Allgemeine Ausführungsreglement zum Beitragsreglement. Es ist nur eine einzige Ausschreibung vorgesehen; sollten sich jedoch erhebliche thematische Lücken ergeben, kann eine zweite Ausschreibung veröffentlicht werden.

Koordinierte Forschungs- und Programmaktivitäten: Die NFP haben zum Ziel, einen Beitrag zur Bewältigung drängender Herausforderungen von nationaler Bedeutung zu leisten. Zu diesem Zweck koordiniert und steuert die Leitungsgruppe die Auswahl der Projekte, die Durchführung der Forschungsarbeiten sowie weitere programmspezifische Aktivitäten wie regelmässige Programmtreffen und den Austausch mit den Stakeholdern. Die Leitungsgruppe wird während der gesamten Laufzeit des Programms in kontinuierlichem Austausch mit den wichtigsten Stakeholdern stehen und deren Beteiligung an den durchgeführten Programmaktivitäten sicherstellen. Ziel ist es, die Qualität der Forschung sicherzustellen, Synergien zu ermöglichen und die Ergebnisse der Projekte an die entsprechenden Zielgruppen weiterzugeben. Mit der Einreichung eines Forschungsgesuchs im Rahmen des NFP 86 erklären sich die Gesuchstellenden bereit, an den Programmaktivitäten teilzunehmen, mit der Leitungsgruppe und dem Programmmanagement zusammenzuarbeiten und zu den gemeinsamen Ergebnissen des Programms beizutragen.

Projektbeginn: Die Forschungsarbeiten zu den bewilligten Projekten müssen spätestens am 1. November 2027 aufgenommen werden.

Projektdauer: Die Forschungsprojekte im Rahmen des NFP 86 müssen eine Dauer von mindestens **18** Monaten und höchstens **36** Monaten aufweisen.

Projektbudget: Der für ein Projekt beantragte Beitrag muss unabhängig von der Anzahl beteiligter Forschenden oder Projektdauer zwischen **CHF 300’000** und **CHF 800’000** liegen. Zusätzliche Fördermittel aus anderen Förderquellen sind ausdrücklich willkommen (Artikel 18 des Beitragsreglements des SNF sowie Ziffer 1.20 des Allgemeinen Ausführungsreglements zum Beitragsreglement).

Saläre: Die Saläre der Gesuchstellenden werden im Rahmen des NFP 86 nicht finanziert. Gesuchstellende, die Doktorierende mit Projektmitteln des NFP 86 anstellen möchten, müssen sicherstellen, dass deren Finanzierung für die gesamte verbleibende Dauer des Doktorats gewährleistet ist, einschliesslich allfälliger Zeiträume nach Abschluss des durch das NFP 86 finanzierten Projekts.

Sie müssen zudem darlegen, wie die Doktorarbeit zum Projekt beiträgt und wie die relevanten Ergebnisse der Dissertation in den Programmschlussbericht einfliessen werden.

Sprache des Gesuchs: Interessenbekundungen und Gesuche sind auf Englisch einzureichen.

7.2 Zulassungsbedingungen für Gesuchstellende und Projektpartner:innen

Gesuchstellende: Die Gesuchstellenden müssen die Anforderungen gemäss Art. 10 des Beitragsreglements des SNF erfüllen. Gesuchstellende mit Doktorat müssen dieses mindestens vier Jahre vor dem Eingabetermin des Gesuchs erworben haben. Gesuchstellende ohne Doktorat müssen nachweisen, dass sie mindestens drei Jahre lang hauptberuflich in der Forschung tätig waren.

Gesuchstellende müssen in der Lage sein, die volle Verantwortung für die Durchführung eines Forschungsprojekts und die Leitung der daran beteiligten Mitarbeitenden zu übernehmen. Interessenkonflikte und Unvereinbarkeiten werden gemäss den Bestimmungen des SNF zu Ausstand und Interessenkonflikten geprüft. Familienangehörige, Personen in einer persönlichen Beziehung oder Personen, deren Unabhängigkeit aus anderen Gründen infrage stehen könnte, dürfen im selben Projekt nicht wissenschaftlich zusammenarbeiten; dies gilt insbesondere bei hierarchischen Abhängigkeiten.

Anzahl der Projekte: Gesuchstellende dürfen im Rahmen dieser Ausschreibung nur ein Gesuch einreichen und an keinem weiteren Gesuch für dieses NFP als Projektpartner:in beteiligt sein. Nicht-akademische Projektpartner:innen können sich an mehreren Gesuchen beteiligen. Ein Gesuch für NFP 86 kann unabhängig von der Anzahl beantragter oder bereits laufender SNF-Förderungen eingereicht werden, sofern die Bestimmungen der jeweiligen Förderinstrumente eingehalten werden. Während des Evaluationsverfahrens dürfen Gesuchstellende keine identischen oder wesentlich ähnlichen Gesuche in einem anderen Förderinstrument des SNF mit überlappenden Förderzeiträumen zur Evaluation eingereicht haben (vgl. Art. 17 des Beitragsreglements).

Förderberechtigung von Projektpartner:innen: Projektpartner:innen sind Forschende und/oder nicht-akademische Akteure, die einen Teilbeitrag zum Forschungsprojekt leisten, ohne für das Projekt verantwortlich zu sein. Sie sind gemäss dem Beitragsreglement des SNF und dem Allgemeinen Ausführungsreglement zum Beitragsreglement förderberechtigt. Gesuchstellende, die das geplante Forschungsvorhaben in Zusammenarbeit mit einer kommerziell ausgerichteten Einrichtung durchführen möchten, müssen gegenüber dem SNF nachweisen können, dass die Grundsätze der Forschungsfreiheit, der Forschungsunabhängigkeit und der Publikationsfreiheit gewahrt bleiben. Wie bei den Gesuchstellenden werden auch die Saläre der Projektpartner:innen nicht aus Mitteln des NFP 86 finanziert. Der für Projektpartner:innen aufzuwendende Anteil am Gesamtbudget sollte in der Regel 20 Prozent nicht überschreiten. Die Projektpartner:innen dürfen die vom SNF erhaltene Förderung nicht als selbst eingeworbenen Beitrag bezeichnen.

Grenzüberschreitende Forschungsprojekte: Eine Zusammenarbeit mit Forschungsgruppen in anderen Ländern ist zulässig, sofern sie einen erheblichen Mehrwert schafft, der sich nur grenzüberschreitend erzielen lässt, das Forschungsvorhaben inhaltlich oder methodisch wesentlich bereichert oder unverzichtbare Kompetenzen einbringt. Der für mitgesuchstellende Forschende aus dem Ausland beantragte Förderanteil darf in der Regel höchstens 30% des beantragten Forschungsbudgets betragen. Für Mitgesuchstellende aus dem Ausland werden die Ansätze und Normen für Saläre des jeweiligen Landes *mutatis mutandis* angewendet, wobei die Höchstsätze des SNF die Obergrenze darstellen. Vor der Einreichung eines Gesuchs mit grenzüberschreitender Komponente ist der Programmmanager des NFP 86 zu kontaktieren.

7.3 Einreichungsverfahren

Die Einreichung der Gesuche für dieses NFP besteht aus einem zweistufigen Verfahren: Zunächst ist eine Interessensbekundung (Expression of interest) einzureichen, die nicht evaluiert wird, anschliessend ein Gesuch, das begutachtet wird.

Bitte beachten Sie, dass alle Gesuchstellenden und Projektpartner:innen ihre Personendaten, einschliesslich ihres CVs, im Portal **selbst** erfassen müssen. Erst danach können Sie Ihre Interessensbekundung einreichen**.** Laden Sie darum **frühzeitig** alle Gesuchstellenden und Projektpartner:innen als Mitwirkende auf das Gesuch ein, damit diese genug Zeit haben, um falls nötig ein Benutzerkonto zu erstellen und ihre Daten im SNF-Portal zu erfassen.

Nach Ablauf der Eingabefrist für die Interessenbekundung ist eine Gesuchseinreichung für dieses NFP nicht mehr möglich.

7.3.1 Online-Einreichung über das SNF-Portal

Um ein Gesuch über das SNF-Portal einzureichen, müssen sich die Gesuchstellenden und Projektpartner:innen mit einer SWITCH edu-ID anmelden. Für die erstmalige Anmeldung steht eine Schritt-für-Schritt-Anleitung zur Verfügung: (Ein SNF-Portal-Benutzerkonto erstellen).

Lebenslauf (CV): Die Gesuchstellenden müssen ihren Lebenslauf (CV) anhand der auf dem SNF-Portal verfügbaren Vorlage erstellen. Weitere Informationen finden sich auf der CV-Webseite und auf dem SNF-Portal.

7.3.2 Interessenbekundung

Die Vorlage für das Gesuch wird bereits in der Phase der Interessenbekundung im SNF-Portal zur Verfügung gestellt.

Die Gesuchstellenden müssen bis zum **24. November 2026**, 17:00 Uhr Schweizer Zeit, über das SNF-Portal eine Interessenbekundung einreichen. Diese umfasst Angaben zur Person, die Zusammensetzung des Projektteams sowie eine kurze Zusammenfassung des geplanten Projekts (max. 4 000 Zeichen). Die Projektpartner:innen bestätigen ihre Beteiligung am Projekt, indem sie ihre Angaben in das SNF-Portal eingeben. Die Interessenbekundung und die darin enthaltenen Informationen dienen dem SNF zur Organisation des bevorstehenden Evaluationsverfahrens. In der Phase findet keine Evaluation oder Vorauswahl statt.

Die Interessenbekundung wird am 25. November angenommen. Danach können die Gesuchstellenden ihr Gesuch auf dem SNF-Portal weiterbearbeiten und einreichen.

7.3.3 Gesuche

Die Frist für die Einreichung der Gesuche endet am 19. Januar 2027 um 17:00 Uhr Schweizer Zeit.

Die Gesuche müssen online über das SNF-Portal eingereicht werden. Zusätzlich zu den administrativen Angaben der Gesuchstellenden und Projektpartner:innen, die direkt im SNF-Portal zu erfassen sind, müssen folgende Dokumente hochgeladen werden:

- **Projektplan und Literaturverzeichnis** (im PDF-Format): Die Gesuchstellenden müssen die im SNF-Portal bereitgestellte Vorlage verwenden. Der Projektplan darf nicht länger als 15 Seiten sein (ohne Literaturverzeichnis).

Bitte beachten Sie, dass formelle Unterstützungsschreiben der nicht akademischen Projektpartner:innen zu einem späteren Zeitpunkt eingereicht werden müssen.

7.4 Evaluationsverfahren

Die Geschäftsstelle des SNF prüft vor der Weiterleitung des Gesuchs zur wissenschaftlichen Begutachtung, ob die persönlichen und formellen Voraussetzungen erfüllt sind. Gesuche, die diese Voraussetzungen nicht erfüllen, werden vom SNF nicht berücksichtigt. Solche Entscheide werden den Gesuchstellenden in Form einer anfechtbaren Verfügung mitgeteilt.

Die Leitungsgruppe kann eine Vorprüfung der Gesuche durchführen und diejenigen von der weiteren Behandlung ausschliessen, die nicht den Zielen und dem thematischen Rahmen des NFP 86 entsprechen. Der SNF teilt den Gesuchstellenden solche Entscheide in Form einer anfechtbaren Verfügung mit.

Die für das weitere Verfahren ausgewählten Gesuche werden von nationalen und internationalen Expert:innen begutachtet. Gestützt auf diese externen Evaluationen sowie auf die nachstehend aufgeführten Evaluationskriterien beurteilt die Leitungsgruppe die Gesuche und erarbeitet eine Förderempfehlung. Während der Evaluationsphase können zudem Ad-hoc-Expert:innen beigezogen werden, die spezifische Expertise einbringen und das Evaluationspanel ergänzen. Bei der Ausarbeitung ihrer Empfehlung berücksichtigt die Leitungsgruppe die Zusammensetzung und Kohärenz in Bezug auf die Programmziele sowie die transparente und konsistente Anwendung der Evaluationskriterien. Die endgültigen Förderentscheide werden vom Nationalen Forschungsrat getroffen.

7.5 Evaluationskriterien

Die Gesuche werden anhand folgender Kriterien beurteilt:

- **Übereinstimmung mit den Zielen des NFP 86 und Relevanz für dessen Forschungsfragen:** Die Gesuche müssen sich in den übergeordneten Rahmen des Programms einfügen und den in dieser Ausschreibung festgelegten Programmzielen entsprechen;

- **Wissenschaftliche Qualität des Forschungsprojekts:** Die Gesuche müssen internationalen Standards hinsichtlich wissenschaftlicher Qualität, Relevanz, Aktualität und Originalität, Eignung der Methoden sowie der Machbarkeit genügen;

- **Interdisziplinäre Integration:** Kohärenz und Mehrwert der Verknüpfung technischer Fachkenntnisse mit Erkenntnissen aus nicht-technischen Disziplinen, einschliesslich gegebenenfalls menschlicher, rechtlicher und organisatorischer Aspekte, um komplexe Wechselwirkungen und systemische Risiken zu bewältigen;

- **Praktische Bedeutsamkeit:** Die Glaubwürdigkeit einer strukturierten Umsetzungsstrategie, die Relevanz der aufgeführten Anspruchsgruppen sowie die Qualität und der Mehrwert der Einbindung der nicht akademischen Partner:innen müssen überzeugend dargelegt werden. Die Art der Zusammenarbeit, Zuständigkeiten und Zeitpläne, sowie die getroffenen Massnahmen zur Erzielung umsetzbarer Ergebnisse für die Governance oder die Praxis sind klar zu beschreiben;

- **Wissenschaftliche Qualifikationen der Gesuchstellenden und geeignete Infrastruktur:** Die Gesuchstellenden müssen über einen ausgewiesenen wissenschaftlichen Leistungsausweis auf dem Gebiet des Gesuchs verfügen und in der Lage sein, das Forschungsprojekt erfolgreich durchzuführen. Für das Projekt müssen angemessene personelle Ressourcen und eine geeignete Infrastruktur zur Verfügung stehen.

8 Programmbudget und Zeitplan

8.1 Programmbudget

Es wird erwartet, dass im Rahmen des NFP 86 etwa fünf bis zehn Projekte in allen vier Forschungsschwerpunkten gefördert werden.

Projekte	Forschungsschwerpunkt 1: Daten	CHF 4 250 000
	Forschungsschwerpunkt 2: Bewährte Verfahren	
	Forschungsschwerpunkt 3: Anreize	
	Forschungsschwerpunkt 4: Kollektive Verteidigung	
Wissensaustausch und -synthese		CHF 300 000
Projekt- und programmübergreifende Koordination		CHF 150 000
Wissenschaftliche Evaluation, Unterstützung und Leitung		CHF 300 000
Gesamtbudget		**CHF 5 Mio.**

8.2 Zeitplan

Die einzelnen Projekte des NFP 86 dürfen maximal eine Laufzeit von 36 Monaten haben.

Veröffentlichung der Ausschreibung	22. September 2026
Frist für die Einreichung von Interessenbekundungen	24. November 2026
Frist für die Einreichung der Gesuche	19. Januar 2027
Endgültiger Förderentscheid zu den Gesuchen	Spätestens im August 2027
Beginn der Forschungsarbeiten	Spätestens am 1. November 2027
Ende der Forschungsarbeiten	November 2031
Veröffentlichung der Programmsynthese	Mitte 2032

9 Organisation und Beteiligte

Leitungsgruppe des NFP 86

- Prof. Dr. Pascal Felber, ordentlicher Professor für Informatik, Fachbereich Informatik, Universität Neuenburg (Präsident)
- Dr. Eva Cellina, in der Schweiz zugelassene Rechtsanwältin und Dozentin, Digital Law Center, Rechtsfakultät, Universität Genf
- Dr. Fabian Muhly, stellvertretender Leiter des Bereichs Verteidigungsökonomie/Cyberabwehr, Militärakademie an der ETH Zürich
- Prof. Dr. Martina Angela Sasse, Professorin am Lehrstuhl Human-Centred Security, Horst-Görtz-Institut für IT-Sicherheit, Ruhr-Universität Bochum (Deutschland)

Vertreter der Schweizer Bundesverwaltung

- Dr. Bernhard Tellenbach, Leiter Cyberdefence, armasuisse Wissenschaft und Technologie

Delegierter des Forschungsrats für das Programmkomitee Thematische und lösungsorientierte Forschung (TSOR)

- Prof. Dr. Patrick Eugster, ordentlicher Professor für Informatik,
  Computer Science Institute, Università della Svizzera italiana

Programm-Manager

- Dr. Martin Christen, Schweizerischer Nationalfonds, Bern

Programmassistentin

- Julien Jauquier, Schweizerischer Nationalfonds, Bern

10 Kontaktpersonen

Bei Fragen zur Einreichung der Interessenbekundungen und Gesuche wenden Sie sich bitte an den Programm-Manager Martin Christen: nrp86@snf.ch oder +41 31 308 22 22.

Bei Fragen zu Salären und förderfähigen Kosten wenden Sie sich bitte an den Finanzleiter Roman Sollberger: roman.sollberger@snf.ch oder +41 31 308 22 22.

Für technische Unterstützung zum SNF-Portal und zur elektronischen Einreichung besuchen Sie bitte das SNF-Support-Portal: https://snsf-ch.atlassian.net/servicedesk

Hotline: Tel. +41 31 308 22 00 (Deutsch/Français/English)