Programme national de recherche PNR 86 « Résilience numérique des infrastructures critiques »

Mise au concours

Table des matières

Que sont les programmes nationaux de recherche (PNR) ?

Les travaux de recherche menés dans le cadre des programmes nationaux de recherche sont des projets de recherche qui contribuent à relever les défis sociétaux d'importance nationale.

Sur la base de l'article 10, alinéa 2, lettre c de la Loi fédérale sur l'encouragement de la recherche et de l'innovation du 14 décembre 2012 (LERI), le Conseil fédéral choisit les questions et les axes prioritaires qui doivent faire l'objet de recherches dans le cadre des PNR, et confie au Fonds national suisse de la recherche scientifique (FNS) l'entière responsabilité de la mise en œuvre de ces programmes. Les articles 3 à 9 de l'Ordonnance relative à la Loi fédérale sur l'encouragement de la recherche et de l'innovation du 29 novembre 2013 (O-LERI) décrivent les PNR et leur lancement. À partir de cette base juridique, deux procédures distinctes peuvent conduire au lancement d'un PNR :

1. Appels à projets ouverts
2. Appels thématiques

Le thème abordé par le présent PNR est issu du deuxième type de processus et s'inscrit dans le cadre des stratégies fédérales actuelles et des priorités de l'administration fédérale. Par rapport au processus des appels à projets ouverts, le présent PNR vise à réduire la durée, à diminuer le budget et à renforcer les liens entre les équipes de recherche et l'administration fédérale. L'évaluation scientifique et les décisions d'octroi sont menées en toute indépendance vis-à-vis des autorités politiques et conformément aux principes d'excellence scientifique et de liberté académique.

Le 1er juillet 2025, le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI) a chargé le FNS d'évaluer la faisabilité de la mise en œuvre d'un PNR sur le thème « Résilience numérique des infrastructures critiques », et d'élaborer un concept de programme définissant les objectifs et les principaux enjeux de recherche. À partir de ce concept de programme, le Conseil fédéral a décidé, le 20 mars 2026, de lancer le PNR 86 « Résilience numérique des infrastructures critiques ». Les membres de son comité de direction ont été élus par le Conseil national de la recherche du FNS le 24 mars 2026. Le comité de direction a élaboré cette mise au concours et supervise la gestion stratégique du programme.

1 Résumé

Des requêtes peuvent être soumises pour des projets de recherche qui seront menés dans le cadre du Programme national de recherche « Résilience numérique des infrastructures critiques » (PNR 86). Ce programme a été mis en place sur décision du Conseil fédéral suisse le 20 mars 2026 afin de renforcer la résilience des infrastructures critiques de la Suisse face aux cyberattaques et autres perturbations numériques. Il financera des travaux de recherche visant à améliorer les connaissances sur les vulnérabilités et les risques, à mettre au point des solutions techniquement viables et socialement acceptables, et à proposer des mécanismes de gouvernance et de coordination pour une cyberdéfense collective agile. Le PNR 86 comprend quatre domaines de recherche :

- Le domaine de recherche « Données » déterminera ce qui constitue des données pertinentes en matière de cybersécurité et comment améliorer l'accès à ces données, leur gestion, leur protection et leur partage entre le monde universitaire, les pouvoirs publics et les opérateurs d'infrastructures critiques.

- Le domaine de recherche « Bonnes pratiques » évaluera les pratiques organisationnelles, techniques et opérationnelles pouvant être considérées comme à la pointe de la technologie, et examinera comment les adopter, les tester, les adapter et les transférer dans l'ensemble des secteurs des infrastructures critiques suisses.

- Le domaine de recherche « Mesures incitatives » étudiera les conditions économiques, réglementaires, comportementales et institutionnelles qui influencent les investissements en matière de cybersécurité, et identifiera les moyens d'aligner les décisions organisationnelles avec la résilience au niveau du système.

- Le domaine de recherche « Défense collective » examinera la possibilité pour les opérateurs, les fournisseurs, les autorités, les régulateurs, les chercheuses et chercheurs, les utilisatrices et utilisateurs de coordonner leurs responsabilités, l'échange d'informations, l'évaluation des risques et les réponses conjointes avant, pendant et après des cyberincidents.

Le PNR 86 financera la recherche interdisciplinaire et intégrera des éléments de recherche transdisciplinaire présentant un intérêt pratique pour les propriétaires et exploitants d'infrastructures critiques, les professionnels de la sécurité, les pouvoirs publics, les autorités de régulation, les assureurs, les chercheuses et chercheurs et les utilisatrices et utilisateurs de services critiques. Les projets doivent associer des partenaires non-académiques, contribuer à l'échange de connaissances au niveau du programme et produire des résultats pouvant être mis à profit dans les domaines de la politique, de la gouvernance, des pratiques organisationnelles, de la mise en œuvre technique, de la formation et de la prise de décision publique.

Le programme dispose d'un budget total de 5 millions de francs suisses, dont 4,25 millions sont consacrés à la recherche. Il devrait permettre de financer entre cinq et dix projets dans ces quatre domaines de recherche. Le budget des projets doit être compris entre 300 000 et 800 000 CHF, et la durée des projets de recherche peut varier de 18 à 36 mois. Le cofinancement par d'autres sources de subsides est explicitement encouragé.

Les manifestations d'intérêt doivent être soumises au plus tard le 24 novembre 2026 à 17 h, heure locale suisse, et les requêtes de projet au plus tard le 19 janvier 2027 à 17 h, heure locale suisse. Les décisions d'octroi finales du Conseil national de la recherche du FNS devraient être rendues au plus tard en août 2027. Les travaux de recherche liés aux projets financés doivent débuter au plus tard le 1er novembre 2027.

2 Introduction

2.1 Contexte et définition du problème

La numérisation de notre société moderne présente de nombreux avantages, mais comporte également des risques.[1] Alors que la numérisation des infrastructures critiques s'est accélérée, la sécurité des systèmes sous-jacents n'a pas toujours suivi le rythme. Ces infrastructures essentielles touchent désormais de nombreux domaines de notre vie, notamment l'approvisionnement énergétique, les soins de santé, les transports publics et commerciaux, la logistique, le bâtiment, les communications, l'agriculture, l'approvisionnement en eau et l'assainissement. La Suisse compte à elle seule des millions d'appareils connectés à Internet, soit davantage d'appareils connectés qu'elle ne compte d'habitant·es. Malheureusement, la sécurité n'a pas été intégrée dès le départ dans la plupart de ces appareils connectés, soit parce que les menaces et les vulnérabilités n'étaient pas connues, soit parce que les mesures de protection sont trop fastidieuses, complexes ou coûteuses à mettre en œuvre pour les particuliers et les organisations. Par ailleurs, les cyberattaques visant les infrastructures critiques se multiplient, y compris en Suisse. Des hôpitaux ont été paralysés, des ransomwares (ou rançongiciels) ont perturbé les transports publics et des fuites de données ont eu lieu au sein des administrations publiques. Ces événements mettent en évidence la fragilité croissante du tissu numérique suisse.
À mesure que la numérisation s'accélère, les compétences et les moyens dont disposent les acteur·trices malveillant·es ne cessent de se renforcer. L'augmentation du nombre, de la diversité et de l'ampleur des tentatives d'attaques semble sans fin. Comme tout pays, la Suisse doit faire face à des défis et bénéficie de possibilités qui lui sont propres, en raison de ses caractéristiques uniques. Ce pays est petit et présente un niveau élevé de développement technique. En parallèle, la fragmentation des responsabilités entre la Confédération, les cantons et les communes accentue la séparation entre les pouvoirs publics et les opérateurs privés, ce qui complique la mise en place de réponses coordonnées. De plus, comme dans de nombreux autres pays, les coûts liés à la cybersécurité sont considérés comme un frein à l'innovation, alors même que le risque d'attaques est très répandu.

Ce PNR vise à renforcer la résilience des infrastructures critiques suisses[2] face aux cyberattaques. Cette consolidation commence par la mise en place d'une base de connaissances plus solide sur les vulnérabilités et les risques liés à la résilience numérique actuelle des infrastructures critiques du pays, mais implique également d'identifier des solutions techniquement viables et socialement acceptables, ainsi que de proposer des stratégies globales visant à mettre en œuvre ces solutions, et ainsi à renforcer la résilience numérique des infrastructures critiques du pays. En outre, le PNR vise à améliorer la coordination et la gouvernance nationales dans le domaine de la cybersécurité.

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

[2] Pour de plus amples informations sur les infrastructures critiques en Suisse, veuillez consulter la définition de l'Office fédéral de la protection de la population (OFPP) : https://www.babs.admin.ch/fr/les-infrastructures-critiques

2.2 Environnement de recherche national et international

Si la Suisse fait preuve d'une grande capacité d'innovation, elle ne dispose toutefois pas des ressources nécessaires pour industrialiser ses idées. Des communautés spécialisées voient le jour et la collaboration entre le secteur privé, le monde universitaire et les pouvoirs publics s'intensifie, mais la Suisse a encore besoin d'une législation plus stricte, de ressources supplémentaires et d'un meilleur partage des données. Bien plus, tôt dans d'autres pays, la cybersécurité est devenue une priorité nationale en matière de financement de la recherche et d'expertise gouvernementale. En Allemagne, par exemple, le BSI a été créé dès 1991, alors que les premières démarches en vue de la création de l'OFCS suisse n'ont été entreprises qu'en 2020. Pourtant, grâce à son contexte politique et à ses équipes de recherche de premier plan, la Suisse peut jouer un rôle international clé en matière de cyberrésilience.

La résilience numérique constitue également un enjeu international majeur. Par exemple, le Centre for Cyber Economics (CCE) a été créé en Arabie saoudite en 2025 par le Global Cybersecurity Forum (GCF) et le World Economic Forum (WEF) afin de servir de plateforme et de permettre aux parties prenantes de contribuer à une prise de décision éclairée en matière de cyberrésilience. Les pays adoptent des stratégies différentes : les États-Unis et la Chine se sont orientés vers des politiques de sécurité visant d'autres pays par le biais de réglementations et de restrictions, tandis que d'autres se concentrent sur l'économie.

3 Objectifs du programme national de recherche

Le PNR 86 a pour principal objectif de renforcer à long terme la résilience des infrastructures critiques suisses face aux cyberattaques, en investissant dans le développement d'une défense collective agile et à la pointe de la technologie. Plus précisément, l'objectif est d'améliorer la capacité des infrastructures critiques à résister aux perturbations numériques, telles que les cyberattaques ou les défaillances de système, à s'y adapter et à s'en remettre, afin de garantir la poursuite efficace des opérations. Il s'agit non seulement d'améliorer le nombre et la proportion d'attaques que les infrastructures critiques sont capables de déjouer ou auxquelles elles peuvent résister sans subir de dommages, mais aussi d'améliorer la réponse aux attaques qui aboutissent et leur endiguement (figure 1).

Le PNR 86 permettra de renforcer la résilience des infrastructures critiques de la Suisse dans des secteurs sensibles, tels que la santé, les transports, l'agriculture, l'eau potable et l'assainissement, en évaluant et en validant les dispositifs de protection existants, et en développant de nouvelles approches préventives allant au-delà de simples mesures techniques. Afin de renforcer l'infrastructure numérique nationale de manière globale et durable, il est important de favoriser l'échange d'informations pertinentes entre les parties prenantes, notamment les pouvoirs publics, les entreprises et le monde universitaire. La recherche future en matière de cybersécurité nécessite un soutien continu grâce à des données de sécurité réalistes et actualisées. Il est donc essentiel d'identifier et de renforcer les mécanismes de coordination et de gouvernance adaptés à un paysage numérique fragmenté. Les processus actuels doivent être mieux compris, évalués et adaptés si nécessaire. Il s'agit non seulement de la mise en place de mécanismes de défense et de protection, mais aussi de tests de sécurité continus des infrastructures critiques et de réponses structurées aux incidents. Il est nécessaire d'établir une théorie cohérente des pratiques efficaces en matière de résilience, applicable à l'ensemble des domaines et des types d'infrastructures critiques. Une réflexion stratégique et des processus bien établis sont nécessaires pour faire face à la hausse du nombre de cyberattaques.

La compréhension reste limitée en matière de dynamiques sociales et économiques plus larges qui influencent la cybersécurité et les mesures incitatives à l'investissement dans ce domaine

Pour renforcer la résilience numérique de manière durable et abordable, il est nécessaire d'identifier les investissements efficaces et de comprendre comment les décisions sont prises dans un contexte d'incertitude au sein des organisations et des systèmes interdépendants, tout en tenant compte des contraintes réglementaires et comportementales. À mesure que les attaques gagnent en sophistication, il devient de plus en plus difficile de compter sur les assurances pour en absorber les conséquences. Les investissements en matière de sécurité peuvent également soutenir les modèles économiques et générer des rendements qui compensent leurs coûts. Une approche collective de la défense s'impose et elle doit tenir compte de l'ensemble des parties prenantes, des acteur·trices concerné·es et de la vulnérabilité face aux attaques visant la chaîne d'approvisionnement et aux risques liés aux monocultures logicielles. Elle doit être suffisamment agile pour s'adapter rapidement à un environnement en constante évolution, dans un contexte mondial où les nations ne cessent de chercher à atteindre une certaine forme d'autodétermination numérique. De plus, tous les pays occidentaux sont désormais confrontés à la guerre hybride, ce qui nécessite d'étudier la réaction des individus aux attaques et aux incidents, afin de se préparer à des attaques qui exploitent les comportements humains pour cibler les infrastructures nationales.

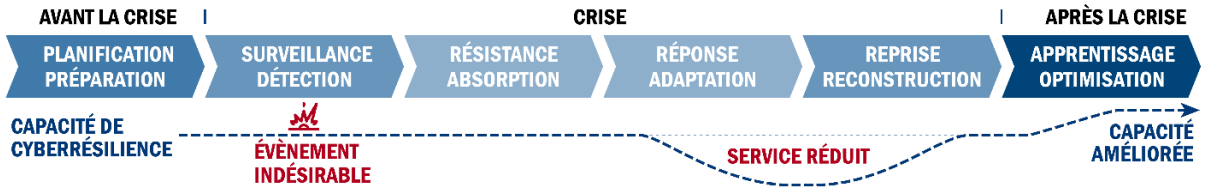

Figure 1 : Réaction face à une attaque réussie et mise en œuvre de mesures visant à renforcer la résilience numérique.[3] Le PNR 86 vise à prévenir les cyberattaques réussies grâce à une cyberdéfense collective et agile à la pointe de la technologie et, en cas d'attaque, à en limiter les conséquences et à adapter rapidement la stratégie afin d'empêcher de futures attaques réussies.

[3] Adapté de l'ouvrage 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

4 Principaux domaines de recherche

Le PNR 86 vise à améliorer la cyberrésilience des infrastructures critiques en Suisse, en mettant particulièrement l'accent sur les activités de recherche interdisciplinaires et transdisciplinaires au sein de l'écosystème plus large de la cybersécurité. Le programme s'articule autour des quatre domaines de recherche ci-dessous, qui couvrent les aspects techniques, les sciences sociales et humaines, ainsi que le cadre juridique et réglementaire. Lors de leur élaboration, les projets devront prendre en compte à la fois les aspects techniques et non techniques, afin de répondre à l'ambition interdisciplinaire du programme. Le PNR 86 sollicite des contributions dans les domaines de recherche suivants :

4.1 Données

Pour évaluer l'état actuel de la cybersécurité, identifier les faiblesses et les vulnérabilités, mener des recherches sur les solutions techniques et coordonner les efforts, il est indispensable de disposer de données. En général, les chercheuses et chercheurs n'ont pas accès aux données des opérateurs d'infrastructures critiques et ne peuvent donc pas mener certaines expériences et recherches, ou finissent par adapter excessivement leurs solutions à des points de données isolés. Les institutions publiques disposent de données, mais elles ne peuvent pas simplement les partager avec n'importe quelle partie intéressée, ni même entre elles. De même, les entreprises hésitent à partager leurs données, par crainte de dévoiler leurs stratégies commerciales ou en matière de sécurité, ou d'admettre leurs vulnérabilités. Il est nécessaire de mettre en place des approches plus méthodologiques et plus facilement applicables, voire des mesures législatives, afin de faciliter et d'intensifier le partage de données pertinentes et exploitables entre le monde universitaire, le secteur privé et les organismes publics. La mise en place de cadres de gouvernance qui concilient transparence et exigences de sécurité, c'est-à-dire qui tiennent compte des contraintes juridiques telles que les obligations en matière de protection des données prévues par la nouvelle loi sur la protection des données (nLPD), les règles de confidentialité, et qui identifient les mécanismes nécessaires, notamment les bases juridiques appropriées, les normes d'anonymisation et les dispositions en matière de responsabilité, constitue donc une priorité pour ce programme.

Ce domaine de recherche porte sur les conditions – juridiques, réglementaires, contractuelles et techniques – permettant de consulter, partager et exploiter *les données pertinentes* à des fins de recherche, d'exploitation et de prise de décision publique en Suisse.

Voici quelques exemples de questions auxquelles pourraient tenter de répondre les projets menés dans ce domaine de recherche :

- *À l'heure actuelle, quels sont les cadres juridiques et réglementaires qui favorisent ou entravent le partage de données entre les pouvoirs publics, les exploitants d'infrastructures critiques et les chercheuses et chercheurs universitaires, et comment pourraient-ils être réformés ou complétés, notamment concernant les dispositions en matière de responsabilité ?*
- *Quels modèles de gouvernance et quels dispositifs institutionnels peuvent permettre un partage des données contrôlé, sécurisé et conforme à la législation entre les parties prenantes, y compris au-delà des frontières entre les secteurs public et privé ?*
- *Quelles sont les conditions nécessaires pour permettre le partage des données relatives aux incidents et aux vulnérabilités tout en respectant les exigences en matière de protection des données ? L'anonymisation ou la pseudonymisation est-elle requise, et si oui, quelles normes seraient suffisantes – y compris dans le cadre d'une réponse aux incidents en temps réel – et comment peut-on vérifier leur respect dans la pratique ?*

- *Quels mécanismes, notamment les environnements de recherche isolés et les intermédiaires tiers de confiance, pourraient permettre aux chercheuses et chercheurs d'accéder de manière réaliste à des données opérationnelles sans compromettre les obligations en matière de sécurité ou de confidentialité ?*
- *Comment et dans quelles conditions le partage de données entre les autorités fédérales et cantonales suisses peut-il être mis en œuvre, et quels changements législatifs ou réglementaires seraient nécessaires pour le rendre possible ?*
- *Dans quelle mesure les flux internationaux de données et les données relatives aux incidents transfrontaliers pourraient-ils influencer les conditions juridiques du partage des données en Suisse, et comment harmoniser les cadres juridiques suisses avec les instruments de l'UE, tels que le règlement européen sur les données (règlement 2023/2854) ou la directive NIS2 (directive 2022/2555), sans compromettre la souveraineté ?*

4.2 Bonnes pratiques

Les institutions publiques comme les entreprises hésitent souvent à adopter les solutions, en raison d'obstacles perçus à leur mise en place ou d'avantages mal définis. Les processus doivent être testés et adaptés et bien que des normes telles que ISO/IEC 27001 prescrivent des méthodes pour y parvenir, la majorité des bonnes pratiques actuelles en matière de cybersécurité ne font pas l'objet de tests rigoureux. Pour faire face à la complexité de la chaîne d'approvisionnement, aux risques liés à la monoculture logicielle et à la multiplication des cyberattaques, il est nécessaire d'adopter une réflexion stratégique et de mettre en place des processus bien établis, notamment des tests de sécurité continus et une réponse structurée aux incidents. Il reste à déterminer dans quelle mesure les pratiques issues d'un domaine ou d'un type d'infrastructure critique donné peuvent s'appliquer à d'autres, et il n'existe pas encore de théorie cohérente des pratiques efficaces en matière de résilience.

Ce domaine de recherche vise à déterminer *quelles sont les bonnes pratiques à la pointe de la technologie* et comment les mettre en œuvre, afin de constituer une base de connaissances qui favorise le transfert intersectoriel des pratiques en matière de résilience et guide leur mise en œuvre future en Suisse.

Voici quelques exemples de questions auxquelles pourraient tenter de répondre les projets menés dans ce domaine de recherche :

- *Quels critères et indicateurs convient-il d'utiliser pour évaluer l'efficacité et le retour sur investissement des pratiques et solutions actuelles ?*
- *Quelles sont les pratiques organisationnelles et techniques qui contribuent actuellement le plus à la prévention, à la détection, à la réaction, à la continuité et à la reprise des activités au sein des infrastructures critiques suisses ?*
- *Comment les bonnes pratiques en matière de cybersécurité mises en œuvre dans un secteur d'infrastructure critique (par exemple, l'énergie) peuvent-elles être systématiquement transposées à d'autres secteurs (par exemple, la santé ou les transports) ?*
- *Comment adapter les bonnes pratiques en matière d'approvisionnement, de configuration, d'application des correctifs, de surveillance, de tests et de gestion de crise à des organisations de tailles et de structures différentes ?*
- *Quels sont les cadres de gestion des risques liés à la chaîne d'approvisionnement les plus efficaces pour réduire l'exposition aux risques liés au matériel et aux logiciels ?*
- *Quel rôle jouent la culture d'entreprise, le leadership et la communication dans l'adoption et le maintien efficaces des bonnes pratiques en matière de cybersécurité ?*

4.3 Mesures incitatives

De nombreuses solutions efficaces en matière de défense et de protection sont adoptées à contre-cœur en raison des coûts qu'elles semblent entraîner. Les entreprises considèrent la cybersécurité comme une dépense sans retour tangible, estimant parfois que les conséquences d'une attaque sont moins coûteuses en raison d'une sous-estimation des probabilités. Toutefois, la sophistication croissante des attaques remet en cause ces hypothèses. La sécurité peut étayer des modèles économiques et générer des revenus qui compensent les investissements. Nous ne disposons pas de méthodes permettant d'analyser le système socio-économique lié à la cybersécurité et les mesures incitatives à l'investissement. Pour parvenir à une résilience abordable et durable, il est nécessaire de mieux comprendre le rapport coûts-bénéfices, mais aussi la prise de décisions d'investissement malgré l'incertitude qui règne au sein des organisations et entre les systèmes interdépendants.

Ce domaine de recherche porte sur *les mesures qui incitent à investir dans la sécurité et les moyens de les renforcer*, en mettant l'accent sur les conditions économiques, réglementaires, comportementales et institutionnelles qui influencent les décisions d'investissement en matière de cybersécurité.

Voici quelques exemples de questions auxquelles pourraient tenter de répondre les projets menés dans ce domaine de recherche :

- *Quels sont les facteurs économiques, comportementaux, réglementaires et organisationnels qui, ensemble, expliquent le sous-investissement persistant en matière de sécurité des infrastructures critiques ? Comment quantifier la valeur de la sécurité et de la résilience (y compris les avantages financiers, opérationnels et systémiques, tels que la prévention des défaillances en cascade) et la traduire en indicateurs qui s'inscrivent dans le cadre de la prise de décision au plus haut niveau ?*
- *Comment un cadre axé sur la « valeur de la résilience des infrastructures critiques » peut-il être mis en œuvre à l'aide d'interfaces décisionnelles (par exemple, tableaux de bord, simulations, récits) et d'outils destinés à faciliter les décisions d'investissement dans un contexte d'incertitude ?*
- *À quoi ressemblerait un outil pratique et adaptatif d'aide à la décision en matière d'investissements dans la sécurité, qui tiendrait compte de la dynamique des menaces, de l'exposition au risque de l'organisation et des interdépendances sectorielles ?*
- *Quelles combinaisons de mécanismes réglementaires et incitatifs permettent d'aligner les investissements des organisations en matière de sécurité sur les objectifs de résilience à l'échelle du système, tout en tenant compte des interdépendances intersectorielles et en évitant un minimalisme dicté par la conformité ?*

4.4 Défense collective

Les infrastructures nationales critiques (INC) ne constituent pas des systèmes monolithiques, mais regroupent au contraire une multitude de composants matériels et logiciels, de services et de personnes chargées de leur maintenance. Les attaques visant n'importe quel élément constitutif peuvent avoir des répercussions sur des pans entiers des infrastructures critiques, mais les opérateurs en ignorent souvent les conséquences. Une résilience efficace nécessite donc une forme de défense collective qui tienne compte de toutes les parties prenantes, en particulier de la chaîne d'approvisionnement. Étant donné que des incidents passés ont montré que la population pouvait être utilisée comme vecteur d'attaque, cette réflexion doit s'étendre aux utilisatrices et utilisateurs finaux et aux bénéficiaires des services essentiels. En partant d'une prise de conscience des interdépendances, nous avons besoin de recherches pour améliorer les échanges et l'évaluation collaborative des risques entre les différentes parties prenantes.

Ce domaine de recherche porte sur *la mise en place d'une défense collective impliquant toutes les parties prenantes*, en s'intéressant notamment à son organisation dans le contexte suisse, à la compréhension et à la gestion des interdépendances, et à la manière dont des approches interdisciplinaires peuvent faire le lien entre les dimensions techniques, organisationnelles, juridiques et sociales chez des acteur·trices hétérogènes, dans un environnement de menaces en constante évolution.

Voici quelques exemples de questions auxquelles pourraient tenter de répondre les projets menés dans ce domaine de recherche :

- *Comment identifier, cartographier et hiérarchiser les interdépendances au sein des infrastructures critiques et entre celles-ci, en vue d'une gestion collective des risques ?*
- *Quelles sont les formes de coordination, d'échange d'informations et de prise de décision conjointe les plus efficaces entre les opérateurs, les fournisseurs, les autorités de régulation et les services d'intervention ? Quelles formes de collaboration stratégique et opportuniste constituent le meilleur point de départ pour la défense collective des INC ? Par exemple, le modèle de « l'équipe des équipes » peut-il s'appliquer aux INC ?*
- *Comment l'apprentissage en double boucle peut-il être appliqué aux INC ? Comment tirer les enseignements des incidents, des exercices et des quasi-accidents, et les analyser afin de développer des approches de défense collective, de mettre en place des réponses plus agiles aux renseignements et aux signaux d'alerte précoce, et d'améliorer la gouvernance (par exemple, la répartition des responsabilités, le développement des capacités et le renforcement des moyens)* ?
- *Quel rôle les pouvoirs publics, les autorités de régulation sectorielles et les organismes internationaux devraient-ils jouer dans la coordination de la cyberdéfense nationale, et comment ces rôles peuvent-ils être renforcés dans le contexte suisse ?*
- *Quelles mesures peuvent être mises en place pour permettre à la population de jouer un rôle supplémentaire de défense (« capteurs ») et la soutenir dans cette fonction, par exemple, en la sensibilisant à l'ingénierie sociale et à la désinformation en tant que vecteurs d'attaque contre les infrastructures critiques, en l'incitant à fournir des renseignements ou des signaux d'alerte précoce, et en encourageant l'accès et le partage des données pertinentes, mais aussi la vérification de leur validité (grâce à l'IA, à la vérification mutuelle, à des activités communautaires, etc.) ?*

5 Mise en œuvre et résultats attendus

5.1 Mise en œuvre

Les voies de mise en œuvre suivantes sont envisagées pour atteindre les résultats escomptés :

- Renforcer l'interaction entre les parties prenantes grâce à des recherches menées dans le cadre de projets, à des actions de sensibilisation au niveau du programme, à des partenariats avec des initiatives existantes et à des initiatives intersectorielles.
- Mettre en place des canaux de partage des données ainsi que les cadres juridiques et de gouvernance correspondants (couvrant les dispositions relatives à la protection des données, les normes d'anonymisation, les utilisations autorisées, les obligations de confidentialité et les règles en matière de responsabilité), en les considérant comme des résultats attendus du programme plutôt que comme des conditions préalables supposées.
- Soutenir la mise en œuvre de processus, de directives, de protocoles et de méthodes en matière de cyberrésilience pour les tests continus, la réponse aux incidents, la reprise après sinistre et

l'adaptation, complétés par des politiques et des réglementations officielles lorsque cela s'avère nécessaire.
- Produire toute une série de résultats, notamment des publications axées sur la pratique, des supports pédagogiques et de formation, des publications scientifiques évaluées par des pairs, des ensembles de données conformes aux principes FAIR, des outils validés et des communications destinées au grand public sur divers supports ; créer, le cas échéant, des produits ou des solutions ayant fait l'objet d'essais pilotes.
- Impliquer activement les équipes de projet universitaires dans des contextes professionnels et extra-universitaires afin de favoriser le dialogue sur le partage des données et des interactions constructives avec les milieux professionnels concernés.
- Encourager la participation directe des parties prenantes aux projets de recherche au moyen de partenariats pratiques et d'accords de cofinancement tenant compte des mesures incitatives, des risques liés à la chaîne d'approvisionnement et à la monoculture, ainsi que des facteurs humains.
- Concevoir des activités de sensibilisation et de création de partenariats, parallèlement à des cadres juridiques garantissant une protection adéquate aux parties prenantes participantes grâce à des mesures de confidentialité et à des règles de gouvernance claires concernant l'utilisation des informations partagées par les équipes de recherche et les pouvoirs publics.

5.2 Résultats attendus

Le PNR 86 vise à renforcer la résilience numérique en Suisse en développant des connaissances axées sur la pratique, des outils validés, des modèles de gouvernance et des mécanismes de coordination destinés aux infrastructures critiques.
Les résultats possibles sont notamment les suivants :

- Mise en œuvre d'un système de cyberdéfense collective agile à la pointe de la technologie et élaboration d'une théorie des pratiques efficaces intégrant l'apprentissage tiré des incidents pour renforcer la résilience.
- Communication et collaboration renforcées entre le monde universitaire, les professionnels et les autres parties prenantes, les solutions issues de la recherche étant activement adoptées par des acteur·trices non-académiques, en particulier les propriétaires et exploitants d'infrastructures critiques.
- Renforcement du partage et de l'échange de données pertinentes relatives aux opérations, aux incidents et aux vulnérabilités entre les différentes parties prenantes, par exemple les chercheuses et chercheurs universitaires, les opérateurs d'infrastructures critiques et les organismes publics.
- Progrès réalisés dans la mise en œuvre et l'adoption de directives, de réglementations, de protocoles et de politiques visant à tester les dispositifs de défense, à hiérarchiser les investissements et à coordonner les réponses afin de renforcer la cyberrésilience.
- Changements d'attitude et de comportement chez les propriétaires, les exploitants et les utilisatrices et utilisateurs finaux d'infrastructures critiques, en vue de se préparer à faire face à l'ingénierie sociale, à la désinformation et aux menaces hybrides.
- Formation d'une nouvelle génération de dirigeant·es spécialisés dans la transformation numérique, dotés d'une expertise étendue en matière de cyberrésilience, allant au-delà des simples connaissances techniques.

6 Caractéristiques du PNR et exigences en matière de recherche

6.1 Approche axée sur les solutions

Tous les projets doivent s'inscrire dans l'un des domaines de recherche 1, 2, 3 ou 4, et, dans l'idéal, dans plusieurs d'entre eux. De plus, les projets doivent être axés sur les solutions et en lien avec la pratique. Les requêtes de projet doivent comporter une discussion autour de la pertinence pratique du projet, mais aussi des propositions concrètes pour la mise en œuvre des résultats. Le PNR 86 ne financera pas la recherche fondamentale qui ne débouche pas sur des résultats exploitables dans la pratique. Les requérant·es doivent proposer des actions de sensibilisation visant à favoriser les interactions avec les parties prenantes.

6.2 Approche de recherche interdisciplinaire

Comme indiqué plus haut, la cybersécurité est un problème aux multiples facettes qui concerne de nombreuses parties prenantes. La réussite du programme proposé dépend essentiellement d'une étroite collaboration entre des spécialistes de différentes disciplines, notamment, mais sans s'y limiter, des représentant·es des domaines suivants :

- Cybersécurité (sécurité des données et de l'information, sécurité des systèmes, sécurité des logiciels, cryptographie appliquée)
- Sciences du comportement (fiabilité, sécurité centrée sur les utilisatrices et utilisateurs, éducation et formation à la sécurité)
- Droit, réglementation et politiques publiques (protection des données et vie privée, régime de responsabilité, droit des contrats, conception réglementaire et droit public régissant les infrastructures critiques)
- Aspects socio-économiques (incitations, chaîne d'approvisionnement)

Par conséquent, **tous les projets doivent aborder de manière approfondie les dimension techniques et non techniques de la résilience numérique**, y compris, le cas échéant, les aspects humains, juridiques et organisationnels. Les requérant·es devront décrire explicitement cette intégration dans une section spécifique de la requête.

6.3 Éléments de la recherche transdisciplinaire

Étant donné que le programme vise à générer des connaissances et des solutions pertinentes, applicables et ancrées dans les réalités des infrastructures critiques suisses, **tous les projets doivent impérativement inclure au moins un·e partenaire non-académique**. Ce·tte partenaire doit exercer ses activités au sein d'un secteur ou d'une fonction liés aux infrastructures critiques, fournir des services dans ce domaine, le réglementer, le soutenir ou y être directement impliqué·e d'une autre manière. Il peut s'agir d'opérateurs·trices, de prestataires de services, d'autorités publiques, d'organismes de régulation ou d'autres parties prenantes dont les activités ont une incidence sur la résilience, la continuité ou la sécurité des services d'infrastructures critiques.

Le succès du PNR 86 dépendra d'un échange de connaissances en temps opportun, d'une implication concrète des parties prenantes et de la transposition des résultats de la recherche en pratiques exploitables. Les requérant·es doivent préciser à quel moment et de quelle manière le ou les partenaires non-académiques interviendront tout au long du projet, afin que cette participation soit concrète, opportune et pertinente, et pas simplement formelle. Les principaux groupes de parties prenantes pris en compte dans le PNR 86 sont résumés dans le tableau suivant :

Groupe de parties prenantes	Rôle dans le PNR 86
Propriétaires d'infrastructures critiques	Décideurs responsables de la stratégie de résilience, des ressources et de la gouvernance
Opératrices, opérateurs et personnel technique	Assurer le fonctionnement des services, assurer la maintenance des systèmes, gérer les incidents et fournir des connaissances et des données opérationnelles
Professionnel·les de la sécurité et expert·es	Évaluer les menaces, concevoir et tester des mesures de défense, transposer les résultats de la recherche en pratiques opérationnelles en matière de sécurité
Personnel des services essentiels, usagères et usagers	Utiliser les systèmes critiques pour fournir des services et contribuer à l'évaluation de la facilité d'utilisation, des flux de travail et du taux d'adoption
Client·es, consommateur·rices et citoyen·nes	Dépendent de services essentiels et peuvent être affectés par des pannes, la désinformation, l'ingénierie sociale, etc.
Assureurs	Déterminer le prix et le transfert des cyberrisques, influencer les pratiques en matière de divulgation et contribuer à définir les mesures incitatives à l'investissement
Juristes, législateurs et régulateurs	Définir les bases juridiques, les règles de confidentialité, les modèles de responsabilité, les instruments réglementaires et les conditions politiques
Décideurs politiques et pouvoirs publics	Utiliser ces conclusions pour les décisions d'intérêt public, les missions de coordination, la préparation aux crises et les programmes de résilience
Chercheuses et chercheurs en sécurité et partenaires universitaires	Produire des approches validées empiriquement, des méthodes, des cadres de référence, des outils, des ensembles de données FAIR et des formations interdisciplinaires

Les plans de recherche doivent comporter une stratégie de mise en œuvre convaincante : les requérant·es sont invités à définir des résultats de projet clairement formulés et réalisables, pouvant être concrètement mis en œuvre dans la pratique, les politiques, la gouvernance, les processus organisationnels ou la mise en œuvre technique.

6.4 Accès aux données, gestion des données et données de recherche ouvertes

Les résultats des travaux de recherche financés par des fonds publics devraient, dans la mesure du possible, être accessibles gratuitement au grand public. Le FNS s'engage en faveur de cet objectif par le biais de la science ouverte (Open Science) (snf.ch). Pour la plupart des instruments d'encouragement, les chercheuses et les chercheurs doivent joindre un plan de gestion des données (DMP) à leur requête. Par ailleurs, le FNS attend que les données générées par les projets qu'il finance soient accessibles au public dans des bases de données numériques respectant les principes FAIR (c'est-à-dire qui garantissent que les données sont faciles à trouver, accessibles, interopérables et réutilisables), à condition qu'il n'y ait pas d'obstacles d'ordre juridique, éthique, lié au droit d'auteur ou autre.

7 Procédure de soumission et d'évaluation des requêtes

7.1 Conditions générales

Base légale : les requêtes doivent respecter les règles énoncées dans la présente mise au concours. Par ailleurs, et en l'absence de disposition spécifique dans la présente mise au concours, le Règlement des subsides du FNS et le Règlement d'exécution général relatif au règlement des subsides s'appliquent. Une seule mise au concours est prévue ; toutefois, en cas de lacunes thématiques importantes, un deuxième appel pourrait être lancé.

Activités coordonnées de recherche et de programme : les PNR ont pour objectif de contribuer à la résolution de défis urgents d'importance nationale. À cette fin, le comité de direction coordonne et gère la sélection des projets, les travaux de recherche menés ainsi que d'autres activités spécifiques au PNR, telles que les réunions régulières du programme et les échanges avec les parties prenantes. L'objectif est de garantir la qualité de la recherche, de favoriser les synergies et de diffuser les résultats des projets auprès des publics cibles concernés. Le comité de direction restera en contact permanent avec les principales parties prenantes tout au long du programme, et veillera à leur participation aux activités menées dans le cadre de celui-ci. En soumettant une requête de projet au PNR 86, les requérant·es s'engagent à participer aux activités du programme, à coopérer avec le comité de direction et la coordination du programme, et à contribuer aux résultats collectifs du programme.

Début du projet : les projets de recherche retenus doivent débuter au plus tard le 1er novembre 2027.

Durée du projet : les projets de recherche menés dans le cadre du PNR 86 doivent durer au minimum **18** mois et au maximum **36** mois.

Budget du projet : le subside demandé pour un projet doit s'élever à au moins **300 000 CHF** et ne peut dépasser **800 000 CHF**, quels que soient le nombre de chercheuses et chercheurs impliqué·es ou la durée du projet. Un financement complémentaire provenant d'autres sources, p. ex. de partenaires tiers non-académiques est le bienvenu (article 18 du Règlement des subsides du FNS et chapitre I, paragraphe 1.20 du Règlement d'exécution général relatif au règlement des subsides).

Salaires : les salaires des requérant·es ne seront pas pris en charge par le PNR 86. Les requérant·es qui prévoient d'employer des doctorant·es au moyen de fonds de projet du PNR 86 doivent garantir un financement adéquat pour toute la durée de leur doctorat, y compris pour toute période s'étendant au-delà de la fin du projet financé par le PNR 86. Les requérant·es doivent également démontrer comment le travail de doctorat contribuera au projet et comment les résultats pertinents de la thèse seront intégrés dans le rapport final du programme.

Langue des requêtes : les expressions d'intérêt et les requêtes doivent être soumises en anglais.

7.2 Critères d'éligibilité applicables aux requérant·es et aux partenaires de projet

Requérant·es : les requérant·es doivent satisfaire aux exigences de l'article 10 du Règlement des subsides du FNS. Les requérant·es titulaires d'un doctorat doivent l'avoir obtenu au moins quatre ans avant la date de dépôt de la requête. Les requérant·es non titulaires d'un doctorat doivent justifier d'au moins trois ans d'activité de recherche à temps plein.

Les requérant·es doivent être capables d'assumer l'entière responsabilité de la conduite d'un projet de recherche et de la gestion du personnel concerné. Les conflits d'intérêts et les incompatibilités sont évalués conformément au règlement du FNS relatif à la récusation et aux conflits d'intérêts. Les membres d'une même famille, les requérant·es entretenant une relation personnelle étroite ou pouvant être perçus comme insuffisamment indépendants ne peuvent pas collaborer scientifiquement sur un même projet, en particulier afin d'éviter tout problème hiérarchique.

Nombre de projets : chaque requérant·e ne peut soumettre qu'une seule requête de projet dans le cadre du PNR 86 et ne peut participer en tant que partenaire de projet à aucune autre requête soumise pour ce PNR. Les partenaires de projet non-académiques peuvent participer à plusieurs requêtes. Une requête peut être déposée, quel que soit le nombre d'autres subsides du FNS déjà

soumis ou en cours, à condition que les règlements des instruments d'encouragement concernés soient respectés. Au cours de la procédure d'évaluation, les requérant·es ne doivent pas avoir de requêtes identiques ou substantiellement similaires en cours d'évaluation au titre d'un autre instrument d'encouragement du FNS, et dont les périodes d'encouragement se chevauchent (voir art. 17 du Règlement des subsides).

Éligibilité des partenaires de projet : les partenaires de projet sont des chercheuses et chercheurs et/ou des acteur·trices non-académiques qui apportent une contribution partielle au projet de recherche sans en assumer la responsabilité. Ils sont éligibles conformément au Règlement des subsides du FNS et au Règlement d'exécution général relatif au règlement des subsides. Les requérant·es qui souhaitent mener le projet de recherche prévu en collaboration avec une institution à vocation commerciale doivent être en mesure de prouver au FNS que les principes de liberté de recherche, d'indépendance de la recherche et de liberté de publication seront respectés. Tout comme pour les requérant·es, les salaires des partenaires de projet ne seront pas financés par le PNR 86, et la part du budget total allouée aux partenaires de projet ne devrait en principe pas dépasser 20 %. Les partenaires de projet ne doivent pas présenter le soutien reçu du FNS comme un subside qu'ils auraient eux-mêmes obtenu.

Projets de recherche transfrontaliers : la collaboration avec des groupes de recherche d'autres pays est autorisée, à condition qu'elle apporte une valeur ajoutée significative qui ne pourrait être obtenue sans coopération transfrontalière, qu'elle enrichisse considérablement la recherche proposée sur le plan du contenu ou de la méthodologie, ou que les compétences des chercheuses et chercheurs étrangers soient indispensables à la réussite du projet. En règle générale, la part de financement demandée pour les chercheuses et chercheurs étrangers agissant en tant que co-requérant·es peut atteindre au maximum 30 % du budget de recherche sollicité. Pour les co-requérant·es étrangers, les barèmes salariaux et les normes en vigueur dans le pays concerné s'appliqueront mutatis mutandis, les barèmes maximaux du FNS constituant la limite supérieure. Avant de soumettre une requête comportant un volet transfrontalier, veuillez contacter le manager de programme du PNR 86.

7.3 Procédure de soumission

Pour ce PNR, la procédure d'évaluation et de sélection des requêtes se déroule en deux étapes : dans un premier temps, il est nécessaire de soumettre une expression d'intérêt (qui ne fait pas l'objet d'une évaluation), puis une requête de projet, qui sera soumise à une évaluation par des pairs. Invitez suffisamment tôt tous les requérant·es et partenaires de projet à participer à la préparation de la requête, afin qu'ils aient le temps de créer, si nécessaire, un compte utilisateur et de saisir leurs données, y compris le CV, sur le Portail FNS. Veuillez noter que tous les requérant·es et partenaires de projet doivent saisir eux-mêmes leurs données personnelles dans la requête. Ce n'est qu'après cela que vous pourrez soumettre votre requête. **Une fois le délai de soumission des expressions d'intérêt passé, il ne sera plus possible de postuler à ce PNR.**

7.3.1 Soumission en ligne via le Portail FNS

Pour soumettre une requête via le Portail FNS, les requérant·es et les partenaires de projet doivent se connecter à l'aide d'un SWITCH edu-ID. Des instructions détaillées sont fournies pour la première connexion (Créer un compte utilisateur sur le Portail FNS).

CV : les requérant·es doivent rédiger leur CV à l'aide du modèle disponible sur le Portail FNS.
Vous trouverez de plus amples informations sur le site web dédié au CV et sur le Portail FNS.

7.3.2 Expression d'intérêt

Le modèle pour le dépôt d'une requête de projet est disponible sur le Portail FNS dès la phase d'expression d'intérêt. Les requérant·es doivent soumettre une expression d'intérêt, comprenant leurs données personnelles, la composition de leur équipe et un résumé du projet proposé (4 000 caractères maximum), via le Portail FNS avant le **24 novembre 2026** à 17 h, heure locale suisse.

Les partenaires de projet confirment leur participation au projet en saisissant leurs données administratives sur le Portail FNS. L'expression d'intérêt et les informations fournies permettent au FNS d'organiser la prochaine procédure d'évaluation. Il n'y aura ni évaluation ni présélection à ce stade.

Les expressions d'intérêt seront acceptées le 25 novembre ; les requérant·es pourront ensuite finaliser la requête de projet sur le Portail FNS.

7.3.3 Requêtes de projet

La date limite de soumission des requêtes complètes est fixée au 19 janvier 2027 à 17 h, heure locale suisse.

Les requêtes de projet doivent être soumises en ligne via le Portail FNS. Outre les données administratives à saisir directement sur le Portail FNS, les documents suivants doivent être téléchargés :

- **Plan du projet et bibliographie** (au format PDF) : les requérant·es doivent utiliser le modèle fourni sur le Portail FNS. Le plan du projet ne doit pas dépasser 15 pages (bibliographie non comprise).

  Veuillez noter que des lettres d'engagement de la part des partenaires de projet non-académiques seront exigées à un stade ultérieur.

7.4 Procédure de sélection des projets

Le Secrétariat du FNS vérifie que les conditions requises sur le plan personnel et formel sont remplies avant de transmettre la requête pour examen scientifique. Le FNS ne prend pas en considération les requêtes qui ne répondent pas aux exigences personnelles et formelles. Une non-considération fait l'objet d'une décision de non-entrée en matière susceptible de recours. Le comité de direction peut procéder à une évaluation préliminaire des requêtes et écarter de l'examen ultérieur celles qui ne répondent pas aux objectifs et au champ d'application du PNR 86. Le FNS en informera les requérant·es sous la forme d'une décision susceptible de recours.

Les requêtes de projet retenues pour la suite de la procédure font l'objet d'une évaluation par des expert·es nationaux·ales et internationaux·ales. Sur la base de ces avis externes et des critères d'évaluation présentés ci-dessous, le comité de direction évalue les requêtes de projet et établi une recommandation de financement. Pendant la période d'évaluation uniquement, il peut également s'adjoindre des expert·es ad hoc chargés d'apporter une expertise spécifique et de compléter le comité d'évaluation aux côtés de ses membres. Lors de l'élaboration de sa recommandation, le comité de direction tient compte de la cohérence globale des projets sélectionnés avec les objectifs du programme ainsi que de l'application transparente et cohérente des critères d'évaluation.

Les décisions de financement finales sont prises en toute indépendance par le Conseil national de la recherche.

7.5 Critères d'évaluation

Les requêtes de projet éligibles sont évaluées selon les critères suivants :

- **Adéquation avec les objectifs du PNR 86 et pertinence par rapport à ses questions de recherche :** les requêtes de projet doivent correspondre aux objectifs du programme précisés dans la présente mise au concours et s'inscrire dans le cadre général du programme ;

- **Qualité scientifique du projet de recherche :** importance scientifique, actualité et originalité, méthodes appropriées et faisabilité ;

- **Intégration interdisciplinaire :** cohérence et valeur ajoutée découlant de la combinaison des connaissances disciplinaires techniques et non techniques, y compris, le cas échéant, les aspects humains, juridiques et organisationnels, afin de faire face aux interdépendances complexes et aux risques systémiques ;

- **Pertinence pratique :** crédibilité d'une stratégie de mise en œuvre structurée associant les parties prenantes concernées et des acteur·trices non-académiques, avec des responsabilités et un calendrier clairement définis, ainsi que des mesures concrètes visant à obtenir des résultats exploitables en matière de gouvernance ou de pratique ;

- **Compétences scientifiques du ou des requérant·es et disponibilité d'une infrastructure adaptée :** expérience scientifique dans le domaine visé par la requête et capacité à mener à bien le projet de recherche. Il est indispensable de disposer de ressources humaines suffisantes et d'une infrastructure adaptée.

8 Budget du programme et calendrier

8.1 Budget du programme

Le PNR 86 devrait financer entre cinq et dix projets, répartis entre les quatre domaines de recherche.

Projets	Domaine de recherche n° 1 : Données	CHF 4 250 000
	Domaine de recherche n° 2 : Bonnes pratiques	
	Domaine de recherche n° 3 : Mesures incitatives	
	Domaine de recherche n° 4 : Défense collective	
Échange et synthèse des connaissances		CHF 300 000
Coordination entre les projets et au niveau du programme		CHF 150 000
Évaluation scientifique, accompagnement et coordination		CHF 300 000
Budget total		**CHF 5 millions**

8.2 Déroulement

Les projets individuels du PNR 86 peuvent avoir une durée minimale de 18 mois et maximale de 36 mois.

Publication de la mise au concours	22 septembre 2026
Date limite de dépôt des manifestations d'intérêt	24 novembre 2026
Date limite de dépôt des requêtes de projet	19 janvier 2027
Décision finale concernant les requêtes de projet	Au plus tard en août 2027
Début des recherches	Au plus tard le 1er novembre 2027
Fin des recherches	Novembre 2031
Publication de la synthèse du programme	Mi-2032

9 Organisation et acteur·trices

Comité de direction du PNR 86

- Pascal Felber, Professeur d'informatique,
  Institut d'informatique, Université de Neuchâtel (président)
- Eva Cellina, titulaire du brevet d'avocat et chargée de cours,
  Digital Law Center, Faculté de droit, Université de Genève
- Fabian Muhly, Directeur Adjoint en Économie de la défense / Cyberdéfense,
  Académie militaire à l'École Polytechnique Fédérale de Zurich
- Martina Angela Sasse, Professor of Human-Centred Security,
  Horst-Görtz-Institut für IT-Sicherheit, Ruhr-Universität Bochum (Allemagne)

Représentant de l'administration fédérale suisse

- Bernhard Tellenbach, Head of Cyberdefence,
  armasuisse Science + Technologie

Délégué du Conseil national de la recherche pour la recherche thématique et orientée solutions (TSOR)

- Patrick Eugster, Professeur d'informatique,
  Computer Systems Institute, Università della Svizzera italiana

Manager du programme

- Martin Christen, Fonds national suisse de la recherche scientifique, Berne

Assistant de programme

- Julien Jauquier, Fonds national suisse de la recherche scientifique, Berne

10 Contacts

Pour toute question concernant la soumission des expressions d'intérêt et des requêtes complètes, veuillez contacter Martin Christen, coordinateur de programme : nrp86@snf.ch ou appeler le +41 31 308 22 22.

Pour toute question concernant les salaires et les coûts éligibles, veuillez contacter Roman Sollberger, Head of Finance : roman.sollberger@snf.ch ou appeler le +41 31 308 22 22.

Pour obtenir une aide technique concernant le Portail FNS et les soumissions électroniques, veuillez vous rendre sur le Portail d'assistance du FNS : https://snsf-ch.atlassian.net/servicedesk

Hotline : +41 31 308 22 00 (allemand/français/anglais)