Plan de mise en œuvre des cantons de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-22

Le plan de mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (SNPC) a été élaboré par un groupe de travail du Réseau national de sécurité (RNS). Il se veut indépendant, mais complémentaire au plan de mise en œuvre national et comprend 13 projets concrets dans 7 des 10 champs d'action de la SNPC.

Le Réseau national de sécurité (RNS)[1] avec l'appui de son groupe de travail, mandaté pour examiner la mise en œuvre de la SNPC dans les cantons[2], a mené les premières réflexions avant l'adoption, en avril 2018, de la stratégie nationale par le Conseil fédéral. Dans ce contexte, le groupe de travail a identifié les champs d'actions pertinents pour les cantons et qui méritaient un examen approfondi. Sur cette base, une première ébauche de plan de mise en œuvre a été élaborée et soumise à l'assemblée plénière d'automne 2018 de la Conférence des directeurs et directrices des départements cantonaux de justice et police (CCDJP), laquelle en a pris connaissance. Fort de cette décision, le groupe de travail du RNS a poursuivi ces travaux afin de soumettre le plan de mise en œuvre définitif à l'assemblée de printemps 2019 de la CCDJP qui l'a approuvé. Les cantons ont ainsi clairement manifesté leur volonté d'améliorer à leur niveau et dans une dynamique propre la protection de leur population contre les cyberrisques.

Afin d'assurer la cohérence entre le plan de mise en œuvre national et celui des cantons, des représentants des cantons, de la CCDJP et du RNS, dans son rôle d'interface entre la Confédération et les cantons, ont pris part aux ateliers organisés en vue de l'élaboration du plan national. De plus, l'organe de coordination SNPC et le bureau du RNS ont organisé conjointement en février 2019 un atelier à l'intention des cantons. Les participants à cette journée ont ainsi eu l'occasion de vérifier la cohérence des projets de mise en œuvres des deux plans. Ils ont également eu l'opportunité d'apporter des compléments dans une perspective cantonale. Concrètement, ce sont quatre projets supplémentaires qui ont été intégrés dans les plans de mise en œuvre.

[1] L'idée d'un réseau national de sécurité a été esquissée dans le rapport 2010 du Conseil fédéral sur la politique de sécurité de la Suisse. La Confédération et les cantons sont représentés de manière paritaire dans les organes du Réseau national de sécurité. La plateforme politique et la plateforme opérative gèrent la consultation et la coordination des décisions, moyens et mesures constituant des enjeux de politique de sécurité qui concernent à la fois la Confédération et les cantons. Dans des groupes de travail temporaires, des représentants de la Confédération et des cantons, des représentants des communes et de l'économie privée élaborent des propositions de solutions concrètes. Voir https://www.svs.admin.ch/

[2] Le groupe de travail se composait de représentants de plusieurs cantons issus de différents domaines d'activité (poursuite pénale, sécurité de l'information, conférence suisse informatique (CSI), secrétariat général de la CCDJP ainsi que du domaine de la recherche et de l'éducation).

1. Acquisition de compétences et de connaissances

(1) Développement d'un concept de formation continue et d'un module pour les administrations cantonales M2 Extension et encouragement des compétences	
Objectifs définis	Il est essentiel de développer de manière proactive les compétences en matière cyber de tous. Les administrations cantonales et les institutions qui y sont attachées constituent l'un des piliers du fonctionnement de notre société, à ce titre elles doivent impérativement être formées en la matière. Les services informatiques cantonaux ont pris la mesure de l'environnement dans lequel nous évoluons et veillent à engager les moyens techniques et organisationnels nécessaires au maintien d'espaces de travail sécurisés. Certaines initiatives ont déjà été prises afin de développer les compétences du personnel, mais ceci n'a à ce jour pas été réalisé de manière systématique, or il est indéniable que le facteur humain est un maillon essentiel de la sécurité de l'information.
Mise en œuvre (responsabilité)	Haute école de gestion Arc – Institut de lutte contre la criminalité économique (ILCE) en collaboration avec le Service informatique de l'Entité neuchâteloise, le Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI, la cellule de coordination SNPC, la Conférence suisse sur l'informatique (CSI)
Participation	Hautes écoles, Associations faîtières économiques, Associations professionnelles spécialisées (ASECE, Association suisse de la sécurité de l'information CLUSIS, etc.)
Instances et processus existants	Les mesures qui ont déjà été prises en la matière seront prises en compte et intégrées à la démarche s'il s'avère qu'il est pertinent de le faire.
Instruments	• Proposer un programme de formation destiné au personnel des administrations cantonales, définissant clairement et de manière pragmatique les buts à atteindre et les compétences visées ; • Assurer la pérennité du système de formation du personnel des administrations en matière cyber ; • Favoriser la propagation de cette formation à l'ensemble des administrations concernées en Suisse • La validation des contenus du programme de formation devrait idéalement être validée par la réalisation d'un pilote de formation présentiel qui pourrait être réalisé à Neuchâtel et ce, dès que le concept de formation est finalisé.
Objectifs mesurables (prestations)	• Rapport initial ; état des lieux • Concept de formation avec définition des objectifs en fonction des publics cibles • Programme complet de formation adapté à l'attention du personnel des autorités cantonales, visant les buts suivants : o Développer les compétences de base en matière cyber de l'ensemble du personnel ; o Donner à chacune et chacun les outils aptes à gérer de manières adéquate les flux d'information, en particulier ceux allant ou venant de l'extérieur des organisations ; o Permettre à toutes et à tous de mieux appréhender l'importance

	de l'information et par conséquent l'utilité des mesures visant à assurer les règles de base en matière de stockage, traitement et transfert d'informations ; o Octroyer à chaque employée, chaque employé les connaissances susceptibles d'en faire un prescripteur de bonnes pratiques en matière cyber dans son entourage privé et associatif. • Conception d'un outil didactique, par exemple dans un format e-Learning

2. Situation de la menace

(2) #MISP[3] – Malware Information Sharing Platform de MELANI pour et avec les cantons M4 Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace	
Objectifs définis	Pour améliorer leurs capacités de description et d'analyse des cyberrisques, les cantons établissent un radar des menaces exploitant les informations fournies par MELANI et y intègrent, si nécessaire, des indicateurs de menaces cantonales. Les cantons, en collaboration avec la Confédération, adoptent un vocabulaire (taxonomie) unique pour structurer et mieux représenter les cybermenaces en Suisse. De manière complémentaire, ils développent un cadre de collaboration opérationnelle pour mieux combattre les intrusions et les codes malveillants (virus) et incluant des services d'intelligence et de veille continue proactive des cybermenaces au niveau cantonal.
Mise en œuvre (responsabilité)	MELANI et les cantons
Participation	Hautes écoles, associations faîtières économiques, associations professionnelles spécialisées, acteurs privés spécialistes de cybersécurité.
Instances et processus existants	• Radar des cyber-menaces de MELANI ; • Plate-forme MISP (Malware Information Sharing Platform) de MELANI.
Instruments	En collaboration avec MELANI : 1. Adoption d'une taxonomie permettant de structurer et représenter les cyber-menaces de manières cohérente et homogène au sein de la Suisse (niveaux Confédération, cantons et communes) ; 2. Développement d'un modèle de radar cantonal des cyber-menaces ; 3. Mise en place d'un réseau suisse d'échange d'information sur les codes malveillants basé sur une solution MISP (Malware Information Sharing Platform); 4. Établissement d'un standard minimum pour détecter des vulnérabilités sur la périphérie des réseaux cantonaux exposée sur le web grâce à des scans périodiques de vulnérabilités[4] ;

[3] MISP = Malware Information Sharing Platform est un logiciel permettant le partage d'informations sur les menaces cyber.
[4] Vulnerability Scans sont possibles à travers des programmes informatiques conçu pour évaluer les vulnérabilités connues des ordinateurs, des réseaux ou des applications.

	5. Déploiement d'un processus de veille et d'analyse (OSINT - Open-source intelligence) simple, efficace et échangeable entre la Confédération et les cantons. Condition cadre : • Implication d'experts cantonaux en cybersécurité pour la mise en œuvre des mesures opérationnelles au sein des cantons.
Objectifs mesurables (prestations)	1. Une taxonomie unique décrivant les cyber-menaces est adoptée par la Confédération et les cantons ; 2. Les cantons disposent d'un radar actif de leurs cyber-menaces ; 3. Les cantons échangent activement des informations opérationnelles relatives aux codes malveillants ; 4. Les cantons évaluent périodiquement la sécurité de leurs points d'accès réseau périphériques exposés sur internet ; 5. Les cantons diffusent périodiquement des rapports de veille sur les cyber-menaces.

3. Gestion de la résilience

(3) Outil d'évaluation pour améliorer la résilience informatique dans les cantons M5 Amélioration de la résilience informatique des infrastructures critiques	
Objectifs définis	Pour améliorer leur résilience (capacité de résistance et de régénération), les cantons analysent les exigences minimales à satisfaire en matière de processus, de compétences et de tâches. Pour ce faire, ils utilisent notamment un outil d'évaluation conçu par l'Office fédéral pour l'approvisionnement économique du pays[5] et adapté à leurs besoins. Cet outil, qui propose des mesures pour améliorer la résilience informatique dans certains secteurs critiques, débouche sur une analyse permettant aux cantons d'élaborer des mesures complémentaires.
Mise en œuvre (responsabilité)	Chef suppléant de la sécurité de l'information (Deputy CISO) du canton de Bâle-Ville en collaboration avec le RNS
Participation	Chaque organisation et exploitant d'IC est responsable de sa propre sécurité de l'information. La direction, qui assume cette responsabilité, s'appuie sur divers interlocuteurs dans ce domaine : responsables de processus d'affaires, gestionnaires de risques, préposés à la sécurité de l'information, chefs de l'informatique, voire responsables de la gestion de crise.
Instances et processus existants	L'organisation met au point un plan de continuité d'activité (PCA) ou *business continuity management* (BCM) qui fait l'objet d'un contrôle externe. Les principales ressources considérées dans le PCA sont les suivantes : • personnel • sites, bâtiments et locaux • technologies de l'information et de la télécommunication (TIC) • fournisseurs et informations externes

[5] Office fédéral pour l'approvisionnement économique du pays, Norme minimale pour les TIC, Berne, 2018, https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

Instruments	**Emploi de l'outil d'évaluation** À travers l'évaluation de sa propre résilience informatique, l'entreprise renforce son organisation de sécurité. Elle dispose ainsi d'une base claire pour répartir les responsabilités, les compétences et les tâches. Un indicateur permet de savoir rapidement si les mesures de sécurité préconisées sont réalisées, et dans quelle proportion. Si une faille est constatée, des mesures pour atténuer les risques peuvent être définies. **Tableau anonyme des organisations participantes** Les résultats de l'évaluation sont divisés en cinq fonctions définies (identifier, protéger, détecter, réagir et récupérer). Les organisations les communiquent au Réseau national de sécurité (RNS) pour qu'il les traite et les anonymise avant de les présenter sous forme anonymisée aux instances concernées. **PCA** Pour établir un PCA, il est nécessaire de documenter tous les processus d'affaires : gestion des risques, gestion de crise ou des situations d'urgence, gestion des situations d'urgence informatiques. La durée maximale d'une panne et les éventuels scénarios alternatifs font partie des informations importantes. Ces directives sont définies par les responsables des processus d'affaires et par la direction.
Objectifs mesurables (prestations)	Grâce à l'outil d'évaluation mis à leur disposition, les exploitants d'IC en Suisse ont identifié leurs failles et pris des mesures pour améliorer leur résilience informatique. Sont connus : • le degré de réalisation en % • le niveau de risque (faible, moyen ou important) • le risque maximal prévisible (indépendamment de toute donnée temporelle). L'évaluation a conduit les exploitants d'IC à appliquer des mesures ciblées pour améliorer leur résilience informatique. L'efficacité des mesures mises en œuvre fait l'objet de vérifications. Sont connues : • les mesures susceptibles d'être prises • les mesures en cours • les mesures appliquées. Les résultats ont été présentés dans certaines instances prédéfinies (Conférence suisse des chanceliers d'État, Conférence suisse sur l'informatique [CSI], etc.) sous forme anonymisée. Sont disponibles : • la liste des organisations concernées • la liste des présentations.

(4) Développement des échanges d'expériences à travers la Conférence suisse sur l'informatique (CSI) pour la création de bases communes M7 Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons	
Objectifs définis	En institutionnalisant les échanges d'expériences et le dialogue, les cantons favorisent leur collaboration en vue d'améliorer la résilience informatique. Pour ce faire, ils utilisent les réseaux existants et les optimisent si nécessaire. Ils participent activement au groupe de travail Sécurité informatique de la CSI. Ils renforcent leur confiance réciproque, se soutiennent mutuellement, coordonnent leurs procédures, en

	particulier en cas d'événement. Ils se dotent de bases de travail utiles (stratégies, listes de contrôle, etc.).
Mise en œuvre (responsabilité)	Groupe de travail Sécurité informatique de la CSI en collaboration avec les services gouvernementaux responsables dans les cantons et leurs préposés à la sécurité de l'information
Participation	RNS
Instances et processus existants	• Préposés cantonaux à la sécurité de l'information • Groupe de travail Sécurité informatique de la CSI
Instruments	• Stratégie informatique cantonale • Système cantonal de gestion des risques • Gestion cantonale des risques informatiques • Concept cantonal de formation • Système cantonal de gestion de la sécurité des informations
Objectifs mesurables (prestations)	• Les cantons s'assurent que leurs préposés à la sécurité de l'information participent au Groupe de travail Sécurité informatique de la CSI. ⇨ Les préposés cantonaux à la sécurité de l'information travaillent ensemble en toute confiance et veillent à la mise en œuvre, dans leur canton respectif, des recommandations du groupe de travail. • Les cantons s'assurent que, dans toutes les questions de sécurité de l'information et de cyberrisques, leurs collaborateurs et partenaires externes suivent des formations et des instructions régulières et adaptées aux besoins. ⇨ La liste de toutes les campagnes et formations effectuées est disponible. • **Les cantons ont mis en œuvre une gestion des risques informatiques** (en tant que partie intégrante de la gestion cantonale des risques) qui couvre les risques liés aux infrastructures critiques. ⇨ La gestion des risques informatiques est disponible et comprend une liste des mesures prises pour diminuer les risques. • Les cantons ont introduit un **système de gestion de la sécurité des informations** (SGSI) adapté à leur organisation. ⇨ Le SGSI est approuvé par la direction et dûment utilisé.

(5) Sensibilisation des jeunes et des aînés aux cyberrisques	
Objectifs définis	Cette mesure vise à renforcer la sensibilisation des jeunes et des aînés afin d'améliorer la résilience de la Suisse en matière de cyberrisques. Une conscience accrue des menaces dans le cyberespace conduit ces tranches d'âge à modifier leur comportement. Elles apprennent à profiter pleinement des possibilités du numérique tout en écartant les risques évitables. Grâce à un programme adapté à leur groupe-cible, les jeunes et les seniors enrichissent leurs connaissances dans le domaine numérique, en profitant des opportunités que celui-ci offre et en réduisant les risques qu'il comporte.

Mise en œuvre (responsabilité)	Conférence suisse des directeurs cantonaux de l'instruction publique en collaboration avec la Conférence des directrices et directeurs cantonaux des affaires sociales et la Prévention suisse de la criminalité (PSC)
Participation	pro senectute, pro juventute, privatim, RNS
Instances et processus existants	
Instruments	La sensibilisation aux cyberrisques dans le cyberespace peut passer par les enseignants pour les jeunes et par le personnel soignant pour les plus âgés.
Objectifs mesurables (prestations)	• Mise en place et consolidation d'un partenariat pour la sensibilisation des jeunes et des personnes d'un certain âge • Conception de contenus didactiques sur mesure

4. Normalisation et régulation

(6) Mise en œuvre de la politique de sécurité du réseau de la CSI M8 Définition et introduction de normes minimales	
Objectifs définis	Les cantons gèrent leurs réseaux et systèmes en toute sécurité. Ils placent des barrières de sécurité aussi solides que possible aux frontières extérieures des réseaux et assurent également une surveillance continue des activités au sein de leur propre réseau. Les cantons accroissent la sécurité au sein de leurs réseaux et applications partenaires sur cette base commune. • Encouragement de la collaboration dans le respect des normes prédéfinies • Consolidation de la confiance réciproque grâce aux normes définies • Mise à disposition de documentation utile (stratégies, listes de contrôle, etc.) • Classement sûr et adapté des documents
Mise en œuvre (responsabilité)	Conférence des gouvernements cantonaux
Participation	Conférence suisse sur l'informatique (CSI)
Instances et processus existants	• Groupe de travail Sécurité informatique de la CSI • Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération (MELANI)
Instruments	• Politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) • Autres normes de même type • Processus appropriés (gestion des changements, des problèmes, des incidents, des risques et des crises) • Autres normes ou recommandations (ISO 2700x, BSI, SANS CSC, CIS 20, etc.)

Objectifs mesurables (prestations)	• Mise en œuvre par les cantons de leur propre politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017)6 • Normes définies et appliquées • Formation du personnel • Définition des processus (gestion des changements, des problèmes, des incidents, des risques et des crises et rapports sur ces sujets)

5. Gestion des crises

(7) Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé M17 Exercices communs de gestion de crise	
Objectifs définis	En cas de crise, la coordination opérationnelle entre la Confédération, les cantons et des exploitants d'IC fonctionne et les services concernés disposent d'une image de la situation actualisée. La stratégie de conduite a pu être testée dans le cas d'une crise comportant des aspects cyber.
Mise en œuvre (responsabilité)	RNS
Participation	Chancellerie fédérale, Conférence suisse des directrices et des directeurs cantonaux de la santé
Instances et processus existants	Gestion générale de la crise (procédures et processus de conduite) des cantons et de la Confédération indépendamment du scénario de l'ERNS19
Instruments	Concept M15 SNPC I élargi aux cantons et aux IC
Objectifs mesurables (prestations)	• Nombre d'exercices effectués en collaboration avec toutes les organisations concernées (un table top exercise d'ici 2020, un exercice-cadre d'état-major d'ici 2021) • Image précise et actuelle de la situation disponible à tout moment pendant tout l'exercice, considérée comme adéquate par tous les protagonistes (lors de l'évaluation) • Soutien des états-majors aux protagonistes sous forme de connaissances spécifiques (évaluation des expériences des protagonistes lors de l'exercice ; enquête) • Responsabilités et interlocuteurs connus des participants • Processus connus des participants • Évaluation des exercices et optimisation des déroulements et des processus de conduite en fonction des leçons tirées ; mise en place d'un plan de suivi (monitoring) ; compte rendu des résultats

[6] La politique de sécurité des réseaux établie par la Conférence suisse sur l'informatique (CSI) est disponible sur Intranet pour tous les membres de la CSI.

(8) Création d'organisations cantonales pour la cybersécurité	
Objectifs définis	Cette mesure a pour but de créer dans chaque canton une organisation chargée de la cybersécurité sur le modèle de la nouvelle structure d'organisation mise en place dans le domaine cyber à l'échelle de la Confédération. Ce service cantonal, qui détient la souveraineté budgétaire et a la compétence d'édicter des directives, suit la situation au plus près, représente le canton pour toutes les questions du domaine cyber, siège à l'état-major de conduite cantonal et assure la coordination au sein du canton, entre les cantons et avec la Confédération.
Mise en œuvre (responsabilité)	Département cantonal compétent
Participation	Préposés cantonaux à la sécurité de l'information, états-majors de conduite cantonaux, polices cantonales, ministères publics, exploitants d'IC, RNS, délégué de la Confédération à la cybersécurité
Instances et processus existants	Avec son groupe de travail (GT) chargé de concrétiser la SNPC II, le RNS élabore un projet avec les cantons destiné à leur servir de ligne directrice et de base pour créer leur propre organisation cantonale pour la cybersécurité.
Instruments	
Objectifs mesurables (prestations)	• Ligne directrice et base de travail mise au point avec le GT du RNS • Comparaison effectuée dans chaque canton entre la situation réelle et la situation visée • Élaboration de stratégies cantonales dans le domaine cyber définissant tâches, compétences et responsabilités • Décision des exécutifs cantonaux quant à la création d'une organisation cantonale pour la cybersécurité

6. Poursuite pénale

Le Cyberboard est chargé de la coordination des mesures dans le champ d'action de la poursuite pénale et en porte la responsabilité.[7]

M18 Tableau de la situation en matière de cybercriminalité	
Objectifs définis	La Confédération (fedpol) et les cantons (CCPCS) ont étudié et défini les conditions techniques nécessaires pour élaborer une image de la situation de la cybercriminalité en temps réel qui relève de la police à l'échelle nationale.
Mise en œuvre (responsabilité)	CCPCS, fedpol
Participation	CCDJP, HiP, cantons, MELANI

[7] Le Cyberboard est un organe de coordination entre polices et ministères publics des cantons et de la Confédération en ce qui concerne la cybercriminalité (analyse des situations, traitement des annonces).

Instances et processus existants	• Ces travaux s'effectuent en collaboration avec le programme d'harmonisation de l'informatique policière suisse (HiP). • L'image de la situation de la cybercriminalité sert au réseau de soutien aux enquêtes relatives à la cybercriminalité.
Instruments	• Phénoménologie de la cybercriminalité • Codes HiP
Objectifs mesurables (prestations)	Les autorités de poursuite pénale de la Confédération et des cantons ont un aperçu des activités de cybercriminalité et connaissent la situation en Suisse (nombre de situations ou de cas saisis au plan national, nombre de plaintes saisies, attribution à une catégorie en fonction des technologies utilisées).

M19 Réseau de soutien aux enquêtes relatives à la cybercriminalité	
Objectifs définis	La Confédération (fedpol) et les cantons (CCDJP) ont élaboré une convention administrative sur la collaboration et la coordination avec le centre de cybercompétences national (National Cyber Competence Center ou NC3) au sein du réseau de soutien aux enquêtes relatives à la cybercriminalité.
Mise en œuvre (responsabilité)	CCPCS, fedpol
Participation	CCDJP, cantons
Instances et processus existants	
Instruments	Les tâches de l'ancien Service de coordination de la lutte contre la criminalité sur Internet (SCoCI) sont reprises dans la convention administrative du réseau de soutien aux enquêtes relatives à la cybercriminalité.
Objectifs mesurables (prestations)	• La convention administrative est signée. • Le réseau est opérationnel.

M20 Formation à la lutte contre la cybercriminalité	
Objectifs définis	En collaboration avec la Conférence des commandants des polices cantonales (CCPCS) et avec la Conférence des procureurs de Suisse (CPS), des concepts de formation spécifiques ont été définis en vue de consolider sur la durée les connaissances nécessaires dans le domaine de la poursuite pénale.
Mise en œuvre (responsabilité)	CCPCS, CPS
Participation	Institut suisse de police (ISP), Fedpol, cantons
Instances et processus existants	Groupe de travail Robert Steiner sur mandat de la CCPCS Institut suisse de police
Instruments	• Modèle à cinq niveaux de formation • Formation en ligne

Objectifs mesurables (prestations)	• Le premier niveau de formation est réalisé et accessible en ligne. • Les programmes de formation pour le deuxième niveau sont proposés par l'Institut suisse de police (ISP). • Les formations pour les niveaux 3 à 5 sont proposées par des universités et des hautes écoles en Suisse.

M21 Office central de lutte contre la cybercriminalité	
Objectifs définis	fedpol a préparé la modification de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) en vue de créer un office central de lutte contre la cybercriminalité.
Mise en œuvre (responsabilité)	fedpol
Participation	Office fédéral de la justice, réseau de soutien aux enquêtes relatives à la cybercriminalité
Instances et processus existants	
Instruments	Catalogue des prestations du réseau de soutien aux enquêtes relatives à la cybercriminalité
Objectifs mesurables (prestations)	La LOC entre en vigueur (au plus tôt en 2023).

7. Visibilité et sensibilisation

(9) Communication active sur les activités des cantons dans le cadre de la SNPC II M28 Élaboration et mise en œuvre d'un concept de communication pour la SNPC	
Objectifs définis	La population intéressée en général et les partenaires du RNS en particulier peuvent s'informer à travers différents canaux sur les travaux des cantons en faveur de la SNPC II. La communication avec la population et les médias est conçue de manière active et dynamique par groupe cible. Les acteurs concernés attachent particulièrement d'importance à la collaboration entre cantons au niveau gouvernemental mais en appellent aussi à la responsabilité individuelle. Un concept de communication a été élaboré et appliqué.
Mise en œuvre (responsabilité)	RNS
Participation	CSI, CCDJP
Instances et processus existants	

Instruments	• Cyberlandsgemeinde • Site Internet du RNS • Rapports annuels sur la mise en œuvre de projets du plan • Communiqués de presse
Objectifs mesurables (prestations)	• Un concept de communication (directives, compétences, processus) existe et est appliqué. • Divers produits de communication ont été mis, en temps voulu, à disposition de la population intéressée et des partenaires du RNS à travers différents canaux (nombre de produits de communication publiés, écho, portée) • Enquête sur la notoriété