Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

Rapport annuel sur l'état d'avancement des projets du plan de mise en œuvre des cantons de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022

Mars 2021

Ce rapport fournit à la Conférence des directrices et directeurs des départements cantonaux de justice et police un aperçu périodique de l'avancement des projets prévus par le plan de mise en œuvre des cantons de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022. Il couvre les douze derniers mois (avril 2020 – mars 2021) et a été élaboré par le Réseau national de sécurité, en collaboration avec les chef(fe)s de projets.

Table des matières

Aperçu de la mise en œuvre des projets

Champ d'action	Nom du projet	Responsabilité de la mise en œuvre	Objectifs (selon plan de mise en œuvre)	Étapes accomplies	Activités en cours/à venir
Acquisition de compétences et de connaissances	(1) Développement d'un concept de formation continue et d'un module pour les administrations cantonales	Groupe de travail sous la direction de Sébastien Jaquier, doyen de l'Institut de lutte contre la criminalité économique (ILCE) de la Haute école de gestion Arc, Neuchâtel	• 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 • Conception d'un outil didactique, par exemple dans un format e-Learning	• Constitution du groupe de travail et de sous-groupes de travail • Élaboration d'un état des lieux • Élaboration du concept de formation • Présentation du concept de formation au comité de la CCDJP • Adoption du concept de formation par le comité de la CCDJP et octroi du financement • Démarrage officiel du projet avec financement • Transmission d'un *Request for information* à quatre entreprises pressenties	• *Request for offer* (conforme aux exigences de l'OMC) • Sélection du ou des fournisseurs • Conception de l'e-Learning
Situation de la menace	(2) #MISP – Malware Information Sharing Platform du NCSC pour et avec les cantons[1]	Marc Barbezat, directeur de la sécurité numérique du canton de Vaud, en collaboration avec le NCSC	• Une taxonomie unique décrivant les cybermenaces est adoptée par la Confédération et les cantons • Les cantons disposent d'un radar actif de leurs cybermenaces • Les cantons échangent activement des informations opérationnelles relatives aux codes malveillants • Les cantons évaluent périodiquement la sécurité de leurs points d'accès réseau périphériques exposés sur internet • Les cantons diffusent périodiquement des rapports de veille sur les cybermenaces	• Élaboration d'une taxonomie unique décrivant les cybermenaces • Utilisation par 12 cantons de la plateforme MISP • Formation par GovCERT de 4 cantons à l'utilisation de la plateforme MISP • Accompagnement des cantons pour une utilisation active des informations du MISP • Préparation d'une approche pour accompagner la mise en place / l'évolution d'un processus de veille OSINT	• Intégration des autres cantons à la plateforme MISP • Accompagnement des cantons pour une utilisation active des informations de la plateforme MISP • Accompagnement des cantons pour la mise en place d'un processus de veille OSINT
Gestion de la résilience	(3) Outil d'évaluation pour améliorer la résilience informatique dans les cantons	Max Haefeli, chef suppléant de la sécurité de l'information (Deputy CISO) du canton de Bâle-Ville, en collaboration avec le RNS, l'OFAE et la Conférence suisse sur l'informatique (CSI)	• Les cantons ont identifié leurs failles grâce à l'outil d'évaluation et ont pris les mesures appropriées pour améliorer leur résilience informatique • L'évaluation a conduit les cantons à appliquer des mesures ciblées pour améliorer leur résilience informatique. • 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	• Préparation et traduction de l'outil d'évaluation • Envoi de l'outil d'évaluation aux organisations participantes • Les organisations participantes procèdent à l'évaluation • Réception et analyse des données • Envoi de l'évaluation aux organisations participantes • Présentation sous forme anonymisée des résultats au groupe spécialisé cyber du RNS • Échange avec le délégué fédéral à la cybersécurité et le secrétaire général de la CSI	• Présentation sous forme anonymisée des résultats à certaines instances • Nouvelle réalisation de l'enquête

[1] Le projet était initialement intitulé " #MISP – Malware Information Sharing Platform de MELANI pour et avec les cantons, selon le Plan de mise en œuvre des cantons de la SNPC, p. 3

	(4) Développement des échanges d'expériences à travers la Conférence suisse sur l'informatique (CSI) pour la création de bases communes	Groupe de travail Sécurité informatique de la CSI	• Les cantons s'assurent que leurs préposés à la sécurité de l'information participent au Groupe de travail Sécurité informatique de la CSI. • 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. • 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. • Les cantons ont introduit un système de gestion de la sécurité des informations (SGSI) adapté à leur organisation.	• 17 cantons sont représentés au sein du groupe de travail Sécurité informatique de la CSI • Le groupe de travail a pris connaissance du plan de mise en œuvre des cantons de la SNPC et du projet. • Plusieurs recommandations et directives ont été émises par la CSI et mises à disposition des cantons	
	(5) Sensibilisation de la population aux cyberrisques	Chantal Billaud, directrice de Prévention Suisse de la Criminalité (PCS)	• Mise en place et consolidation d'un partenariat pour la sensibilisation de la population aux cyberrisques • Conception de contenus didactiques sur mesure	• Les structures ont été créées et les différents groupes (groupe restreint, groupe d'échange et groupes de travail) ont commencé leurs activités • Plusieurs produits destinés à sensibiliser la population ont été élaborés	• Conception d'autres produits destinés à sensibiliser la population • Campagne sur les réseaux sociaux « Sécurité digitale » (mai 2021)
Normalisation et régulation	(6) Mise en œuvre de la politique de sécurité du réseau de la CSI	Groupe de travail Sécurité informatique de la CSI, sous la direction d'Adrian Gutknecht, en collaboration avec le centre de compétence PTI (Kompetenzzentrum Polizeitechnik).	• 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) • 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)	Développement des lignes directrices pour la mise en œuvre du niveau de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) • Élaboration par le groupe de travail d'une liste de contrôle sur l'état de la mise en œuvre de la politique de sécurité des réseaux de la CSI fournie aux cantons afin de vérifier le niveau de référence requis. • Mise en œuvre dans huit cantons, mais aussi au Liechtenstein, de leur politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017)	• Mise en œuvre dans neuf cantons de leur propre politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) prévue en 2021 • Mise en œuvre dans 2 autres cantons prévue en 2022/2023
Gestion de crise	(7) Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé	Groupe de travail, sous la direction d'André Duvillard, délégué du RNS	• 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	• Identification de l'hôpital universitaire de Zurich (USZ) comme partenaire pour la mise en œuvre du projet • Conduite d'un workshop à l'USZ pour développer le contenu adéquat du scénario de référence de l'exercice	• Développement du scénario de référence pour l'exercice, en coopération avec le NCSC • Les progrès dépendent de la disponibilité de l'USZ dans le contexte de la pandémie de Covid-19

	(8) Création d'organisations cantonales pour la cybersécurité	Groupe de travail, sous la direction d'André Duvillard, délégué du RNS	• Ligne directrice et base de travail mise au point avec le groupe de travail 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	• Élaboration du nouveau concept d'organisation cantonale pour la cybersécurité et consultation des différents partenaires (OFPP, MPC, OFAE, CCDJP) • Adoption du concept d'organisation cantonale pour la cybersécurité par l'assemblée plénière de la CCDJP en novembre 2020	• Présentation du concept d'organisation cantonale à différentes conférences spécialisées
Visibilité et sensibilisation	(9) Communication active sur les activités des cantons dans le cadre de la SNPC 2018-2022	André Duvillard, délégué du RNS	• 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	• Publication et mise à jour des actualités des cantons dans le domaine cyber sur le site internet du RNS • Organisation de la 8e Cyber-landsgemeinde (août 2020) • Publication du rapport annuel sur l'état d'avancement des projets du plan de mise en œuvre des cantons de la SNPC	• Organisation de la 9e Cyber-landsgemeinde avec pour objectif la communication de l'avancement des projets du plan de mise en œuvre des cantons de la SNPC

1. Introduction

Le plan de mise en œuvre cantons 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) et adopté le 11 avril 2019 par la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP). Le groupe spécialisé Cyber du RNS en est l'organe de pilotage stratégique.

Ce document fait partie intégrante du plan de mise en œuvre de la Confédération de la SNPC, dont il figure en annexe. La cohérence dans la mise en œuvre des deux plans (Confédération et cantons) est assurée par la représentation du Réseau national de sécurité et de la CCDJP au sein du groupe spécialisé Cyber du RNS mais également au sein du comité de pilotage de la SNPC. Cet organe, chargé de la gestion commune des projets, veille à la mise en œuvre coordonnée et ciblée des mesures de la SNPC. Il s'est réuni deux fois entre avril 2020 et mars 2021.

Treize projets sont prévus par le plan de mise en œuvre des cantons de la SNPC 2018-2022 dans sept des dix champs d'action définis par cette dernière. Quatre mesures du champ d'action de la poursuite pénale seront coordonnées dans le cadre de la plateforme stratégique Cyberboard, qui réunit les acteurs de la poursuite pénale des cantons et de la Confédération. Pour la majorité des neufs autres projets, un ou une chef(fe) de projet issu(e) des cantons est responsable de leur mise en œuvre et sont soutenu(e)s par le RNS. La mise en œuvre de ces projets repose sur le calendrier que le groupe de travail du RNS a jugé approprié, mais qui permet toutefois une certaine marge de manœuvre, lors de sa réunion du 7 mai 2019.

2. Groupe spécialisé Cyber du Réseau national de sécurité

Le groupe spécialisé Cyber du RNS, présidé par le délégué du RNS, est composé de représentants des cantons, du Secrétariat général de la CCDJP, du Secrétariat général de la Conférence des gouvernements cantonaux (CdC), de la Prévention suisse de la criminalité (PCS), de la Conférence des chanceliers d'Etat, de la Conférence informatique suisse (CIS), de l'Union des villes suisses, de l'Association des communes suisses, du délégué fédéral à la cybersécurité et du délégué cyberdéfense du DDPS. Le mandat et la composition de ce groupe spécialisé Cyber du RNS, créé dans le cadre de la première SNPC, ont été adaptés par le délégué du RNS à la suite de l'adoption de la SNPC 2018-2022 et de son plan de mise en œuvre des cantons. Le 19 août 2019, la plateforme politique RNS a approuvé ce nouveau mandat. Cet organe s'est réuni à quatre reprises dans le cadre de la deuxième SNPC et une de ses tâches consiste à coordonner la mise en œuvre des différents projets du plan de mise en œuvre des cantons. Le groupe spécialisé Cyber du RNS joue également un rôle important comme interface avec le comité de pilotage de la SNPC dans la mesure où tant le délégué RNS que le secrétaire général de la CCDJP en sont formellement membres.

3. Etat de la mise en œuvre des projets

Champ d'action 1: Acquisition de compétences et de connaissances

Le projet « **Développement d'un concept de formation continue et d'un module pour les administrations cantonales** » (mesure 2 de la SNPC « Extension et encouragement des compétences en matière de recherche et de formation ») prévoit la conception d'un programme complet de formation du personnel des administrations. Quelques avancées significatives ont été franchies dans sa mise en œuvre. En effet, après un état des lieux partiel des formations existantes dans les cantons et l'élaboration par un groupe de travail expressément constitué d'un concept de formation, le comité de la CCDJP a approuvé ce dernier et également octroyé le budget nécessaire à sa conception. Le groupe de travail et les sous-groupes de travail, composés de responsables cantonaux et fédéraux en matière de sécurité de l'information, ont travaillé sur l'élaboration de la matrice didactique, la détermination de mesures d'accompagnement ainsi que les exigences liées aux environnements informatiques

cantonaux. Par ailleurs, un *Request for Information* a été transmis à quatre entreprises pressenties. Un appel d'offre conforme aux exigences de l'Organisation mondiale du commerce est en cours de préparation. La formation sera proposée à l'ensemble du personnel des administrations cantonales et communales. La possibilité que le personnel de différents départements de l'administration fédérale soit aussi bénéficiaire de la formation est discutée. La mise en œuvre de ces directives et recommandations au sein des cantons varie néanmoins et dépend principalement des ressources à disposition dans le domaine de la sécurité de l'informatique de chaque canton.

Champ d'action 2: Situation de la menace

Dans le cadre du projet intitulé « **#MISP – Malware Information Sharing Platform** », contribuant à la mise en œuvre de la mesure 4 de la SNPC « Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace », une taxonomie de référence pour les cybermenaces a été développée par le Centre national pour la cybersécurité (NCSC) sur la base des « fiches phénomènes » définies par fedpol. Cette taxonomie a été créée pour les administrations, avec pour objectif de fournir à ces dernières un langage commun minimum. Elle a été présentée lors de la Cyber-landsgemeinde organisée par le RNS le 27 août 2020 et a fait l'objet d'un atelier spécifique à cette occasion. En ce qui concerne la solution MISP, 12 cantons font usage de cette source d'information (AG, BS, GE, GR, JU, LU, SZ, SO, VD, VS, ZH, ZG) et exploitent les informations fournies, améliorant ainsi leurs capacités de définition et d'analyse des cyberrisques. Durant l'année 2020, trois formations à l'utilisation de la plateforme MISP ont été organisée par GovCERT, auxquelles environ 130 participantes et participants, dont 6 participantes et participants de 4 cantons, ont pris part. La situation liée à la pandémie de Covid-19 a eu des conséquences non négligeables sur la mise en œuvre de ce projet, dont la difficulté à organiser des ateliers en ligne pour de larges audiences tout en assurant leur confidentialité.

Champ d'action 3: Gestion de la résilience

Le projet intitulé « **Outil d'évaluation pour améliorer la résilience informatique dans les cantons** » (mesure 5 de la SNPC « Amélioration de la résilience informatique des infrastructures critiques »), prévoit une analyse par les cantons des exigences minimales à satisfaire en matière de processus, de compétences et de tâches. Cette analyse est effectuée au moyen d'un outil d'évaluation élaboré par Max Haefeli, chef suppléant de la sécurité de l'information (Deputy CISO) du canton de Bâle-Ville, et fondé sur l'outil d'analyse introduit par la Norme minimale pour améliorer la résilience informatique de l'Office fédéral pour l'approvisionnement économique du pays (OFAE). Les organisations participantes, dont une majorité de cantons, ont procédé à cette analyse en 2020 et les données ont été analysées par la direction du projet. Les résultats sous forme anonymisée et comparés aux résultats des autres organisations ont été transmis aux organisations participantes qui ont pu identifier et analyser leurs failles en matière de résilience informatique. Ils pourront décider, sur la base de cette évaluation, de mesures de sécurité ciblées dans le but de diminuer les risques et renforcer leur propre sécurité. Les résultats ont également été présentés au groupe spécialisé Cyber du RNS et discuté avec le délégué fédéral à la cybersécurité. Il est prévu qu'à terme, les résultats soient présentés à des comités sélectionnés et que l'évaluation soit réalisée une nouvelle fois.

Les cantons, dans le cadre du projet « **Développement des échanges d'expériences à travers la Conférence suisse sur l'informatique (CSI) pour la création de bases communes** » (mise en œuvre de la mesure 7 de la SNPC « Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons ») favorisent leur collaboration en institutionnalisant les échanges d'expériences et le dialogue et améliorent ainsi leur résilience informatique. Pour ce faire, les cantons utilisent les réseaux

existants tels que la CSI et son groupe de travail Sécurité de l'information et cybersécurité, qui responsable de la mise en œuvre du projet et au sein duquel 17 cantons ainsi que d'autres organisations (Office fédéral de l'informatique et de la communication OFIT, Département fédéral des finances DFF avec le NCSC, etc) sont représentés. Ce groupe de travail a pour objectif de produire des recommandations ou lignes directrices sur des sujets d'actualité en matière de sécurité de l'information et de les mettre à disposition des membres de la CSI. Cette dernière a récemment publié un rapport qui définit les conditions à remplir pour que des solutions de vidéoconférences sûres et conviviales entre administrations publiques puissent être facilement utilisées. Celui-ci est publié sur l'intranet de la CSI. La thématique des solutions de vidéoconférences sécurisées sera reprise par le groupe de travail de la CSI nouvellement constitué « Cloud Governance ». Ce groupe de travail traite des questions juridiques et techniques liées à l'utilisation de *clouds* dans l'administration publique et entretient un contact étroit avec le groupe de travail Sécurité de l'information et cybersécurité pour les questions relatives à la sécurité. En outre, une recommandation sur le thème du suivi des anomalies de sécurité a été élaborée, adoptée par le groupe de travail de la CSI lors de sa première réunion en 2021 et mise à disposition de tous les cantons. Finalement, l'adoption par les cantons de la directive relative à la mise en œuvre des directives de sécurité minimales (protection informatique de base) est prévue pour 2021.

Les activités prévues par le projet «**Sensibilisation de la population aux cyberrisques** » [2] ont pour objectif de renforcer la prévention de la population de manière générale et ainsi améliorer la résilience de la Suisse en matière de cyberrisques. La collaboration avec le réseau national de soutien aux enquêtes de la lutte contre la criminalité informatique (*Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung* NEDIK) et les groupes de travail constitués pour la mise en œuvre de ce projet s'est prolongée en 2020, malgré la situation liée au Covid-19. Prévention Suisse de la Criminalité (PCS) a, durant la période couverte, publié de nombreux produits sur différents thèmes destinés à la prévention de la population dont quelques exemples sont listés ci-dessous :

- « My little little Safebook » et « Ta vie en ligne ? », dépliants contenant des informations sur le comportement à adopter sur internet et en cas de cyberharcèlement, destinés aux jeunes et aux responsables éducatifs.
- Trois clips de prévention sur les thèmes « Sextorsion », les faux services d'assistance et « Cybergrooming ».
- Coédition de la 2e bande dessinée de l'OFCOM « Tranches de vie connectée », qui abordent des sujets tels que les fake news, les sextos, le mobbing, la protection des données, la dépendance au smartphone, etc
- Le dépliant « Les 5 règles pour votre sécurité numérique », publié en collaboration avec « eBanking – en toute sécurité ! » (EBAS), sur les précautions à prendre pour se protéger soi-même et son infrastructure TI contre les cybercriminels.
- Diffusion à l'échelle nationale de la campagne « Card Security contre les fraudes à la carte bancaire » de la Police municipale de Zurich (voir www.card-security.ch).

Tous les produits imprimés et en ligne réalisés par la PCS ou par un corps de police et traduits et diffusés par la PCS ont largement été relayés via les canaux de communication de tous les corps de police. Ils ont été également largement repris par la population et diffusés sur les réseaux sociaux et dans les médias. D'autres produits de sensibilisation sont prévus pour 2021. En ce qui concerne la collaboration avec les acteurs concernés, PCS entretient un échange régulier au sujet des nouveaux phénomènes avec la police cantonale zurichoise, qui a mis sur pied en novembre 2019 le site www.cybercrimepolice.ch ayant pour objectif la sensibilisation de la population à la cybercriminalité. La collaboration avec le

[2] Le projet était initialement intitulé "Sensibilisation des jeunes et des aînés aux cyberrisques", selon le Plan de mise en œuvre des cantons de la SNPC, p. 6

NCSC, ibarry et EBAS s'est intensifiée en 2020, en vue de l'organisation de la semaine d'action (campagne sur les réseaux sociaux) « sécurité digitale » prévue en mai 2021.

Champ d'action 4: Normalisation et régulation

Les cantons prévoient, dans le cadre de la mesure 8 de la SNPC "Définition et introduction de normes minimales", de mettre en œuvre la **politique de sécurité des réseaux établie par la CSI en 2017** (et disponible sur Intranet pour tous les membres). En 2018, les lignes directrices pour une mise en œuvre de la politique de sécurité des réseaux propre aux cantons ont été élaborées et approuvées par la CSI. Une liste de contrôle sur l'état de la mise en œuvre de la politique de sécurité des réseaux de la CSI a ensuite été établie par le groupe de travail et fournie aux cantons afin que ces derniers puissent vérifier le niveau de référence requis. À l'heure actuelle, 8 cantons ainsi que le Liechtenstein ont mis en œuvre leur propre politique de sécurité des réseaux, sur la base de celle établie par la CSI en 2017, et 11 autres la prévoient d'ici 2023. Sur cette base commune, les cantons gèrent leurs réseaux et systèmes et assurent également une surveillance continue des activités au sein de leur propre réseau et en accroissent ainsi leur sécurité. La mise en œuvre de cette politique reste néanmoins dépendante de processus de long terme tels que des adaptations techniques et structurelles des infrastructures, la planification budgétaire par exemple.

Champ d'action 5: Gestion de crise

Le projet « **Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé** » (mesure 17 de la SNPC « Exercices communs de gestion de crise ») mis en œuvre par le RNS, qui prévoit la réalisation d'un exercice *table top* comportant des aspects cyber au sein d'une infrastructure critique dans le secteur de la santé, puis d'un exercice-cadre d'état-major, a connu quelques modifications de son calendrier liées au Covid-19. L'hôpital universitaire de Zurich (USZ), associé à la mise en œuvre du projet en tant que partenaire du RNS, a fortement été impliqué dans la gestion de la pandémie. La situation n'a pas empêché un échange régulier entre le RNS et l'USZ qui a débouché sur l'organisation d'un workshop, soutenu par le NCSC et Markus Meile en qualité de responsable de l'organe de gestion de crise de la ville de Zurich, réunissant le RNS et le groupe spécialisé pour les situations extraordinaires de l'USZ. Ce workshop, qui a eu lieu en automne 2020, a eu pour objectif de mieux comprendre l'environnement de travail des employés de l'USZ et de recueillir des éléments de base pour l'élaboration du scénario de référence. Le RNS travaille actuellement, en collaboration avec NCSC, sur le scénario de référence de l'exercice *table top* et espère pouvoir le réaliser dans le courant de l'année 2021. Les progrès de mise en œuvre du projet dépendent néanmoins de la disponibilité de l'USZ dans le contexte de la pandémie de Covid-19.

Dans le cadre de la mise en œuvre du projet « **Création d'organisations cantonales pour la cybersécurité** », le RNS a effectué des étapes décisives. Le groupe de travail RNS, dirigé par son délégué et composé de représentants des cantons de Bâle-Ville, Fribourg, Genève, Tessin, Zürich, mais aussi du Lichtenstein et du NCSC, a élaboré et finalisé, après consultation des différents partenaires (OFPP, MPC, OFAE, CCDJP), le concept «Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité». Celui-ci a été adopté par l'assemblée plénière de la CCDJP en novembre 2020 et sera présenté à diverses conférences spécialisées dans le courant de l'année 2021. Ces recommandations sont dorénavant à disposition des cantons et faciliteront la réflexion des autorités compétentes lors de l'élaboration d'une cyberorganisation au niveau cantonal.

Champ d'action 6: Visibilité et sensibilisation

Le RNS contribue à respecter l'intérêt des cantons de rendre visibles les travaux de ces derniers en faveur de la SNPC. Dans le cadre du projet intitulé « **Communication active sur**

les activités des cantons dans le cadre de la SNPC » (mesure 28 « Élaboration et mise en œuvre d'un concept de communication pour la SNPC »), les activités des cantons dans le domaine cybersécurité sont régulièrement publiées sur le site internet du RNS (svs.admin.ch). En outre, la huitième Cyber-landsgemeinde, qui a pour objectif, en plus d'échanger entre acteurs concernés, de communiquer sur l'avancement des projets du plan de mise en œuvre des cantons de la SNPC a été organisée par le RNS en août 2020. Cet évènement annuel a rassemblé plus d'une centaine de participants principalement issus des cantons et de la Confédération.

4. Développement des structures cyber de la Confédération et implication des cantons

La mise en œuvre et le développement des structures cybersécurité de la Confédération adoptées par le Conseil fédéral en janvier 2019, s'est poursuivie en 2020.

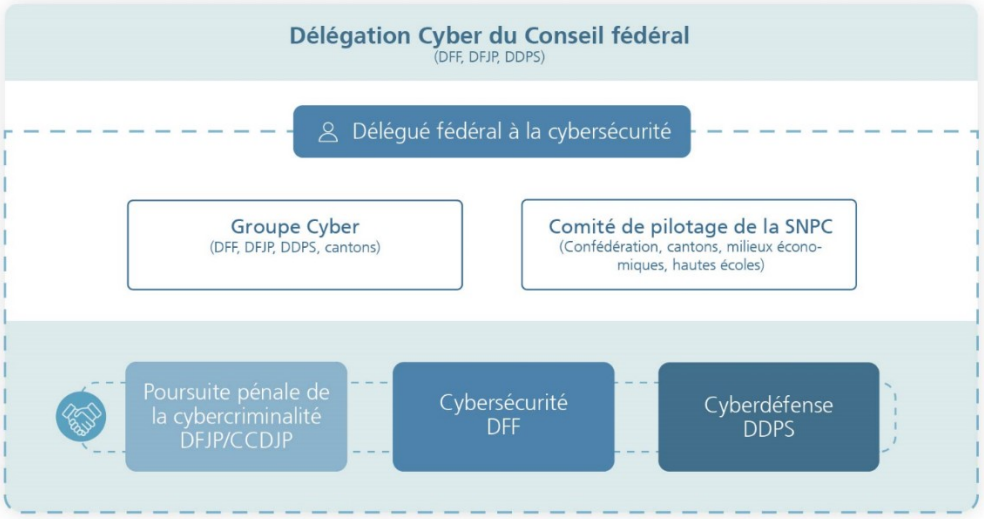

Illustration I : Organisation de la Confédération pour la cybersécurité (Source : NCSC)

Les cantons sont représentés au sein des trois organes de coordination. Le président de la CCDJP participe aux séances de la délégation Cyber du Conseil fédéral, le président de la CCPCS aux séances du Groupe cyber et les cantons sont représentés au sein du comité de pilotage de la SNPC par le secrétaire général de la CCDJP et le délégué du RNS.

Le délégué fédéral à la cybersécurité, en poste depuis août 2019, a entre autres pour rôle de veiller à une coordination optimale des travaux des cantons et de la Confédération afin d'assurer la protection de la Suisse contre les cyberrisques. Ainsi, les cantons ont été associés à ses activités dans le cadre de la mise en œuvre de la SNPC. Un véritable partenariat entre le délégué fédéral à la cybersécurité et le RNS s'est développé, résultat d'une intensification de leurs échanges au cours des douze derniers mois.

Lors de sa séance du 27 mai 2020, le Conseil fédéral a adopté l'ordonnance sur les cyberrisques qui crée la base juridique nécessaire la mise sur pied du Centre national pour la cybersécurité (NCSC). Le Conseil fédéral a, à la même occasion, décidé de créer 20 nouveaux postes en vue de la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2020 à 2022. Le NCSC, qui est placé sous la direction du délégué fédéral à la cybersécurité, intègre dorénavant le service spécialisé de sécurité informatique de la Confédération, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et l'équipe d'intervention en cas d'urgence informatique (GovCERT) en tant que service spécialisé. Le NCSC a mis à disposition dès le 21 décembre 2020 un nouveau formulaire interactif d'annonce volontaire de cyberincidents, dans l'optique d'en améliorer la

convivialité et la plus-value pour les émetteurs d'annonces. Le site du NCSC est également remanié depuis cette date.

Le NCSC a pour objectif d'associer à son réseau les cantons, hautes écoles et milieux économiques ayant développé des compétences spécifiques. Dans ce contexte, le RNS travaille en collaboration avec le NCSC dans le cadre de la mise en œuvre du mandat « Réseau de compétences en matière de cybersécurité » confié par la plateforme politique du RNS en mars 2020. Le RNS a été chargé de faire l'état des lieux des compétences et prestations dans le domaine de la cybersécurité dans les cantons et développer les bases d'une collaboration structurée entre le NCSC et les cantons. Les résultats montrent qu'il existe encore peu de compétences et de prestations dans les cantons qui pourraient être proposées au niveau régional ou même national. L'enquête effectuée dans un deuxième temps auprès des hautes écoles a néanmoins démontré qu'il existe plusieurs projets et offres pour les PME proposées par les Hautes Écoles Spécialisées. Finalement, l'enquête a permis de faire état d'une large variété d'offres de formation continue (CAS, MAS, DAS, etc.) dans le domaine de la cybersécurité, dont la liste sera mise à disposition du public.

5. Autres activités du bureau du délégué du RNS

Dans la lutte contre la cybercriminalité, les cantons œuvrent conjointement avec les autorités de poursuite pénale de la Confédération. Ils sont représentés par le délégué du RNS au sein de la plateforme stratégique Cyberboard, élaborée en 2018, permettant d'opérer le renforcement nécessaire de la coordination dans le cadre du traitement conjoint des affaires intercantonales et internationales. Le délégué du RNS est également membre de l'Expert Group du DDPS, il dispose donc de la vue d'ensemble des enjeux de la cybersécurité, la cyberdéfense et la cybercriminalité.

En outre, le RNS, en collaboration avec la Police cantonale bernoise, a contribué à l'édition de mai 2020 du magazine « Communes suisse » de l'Association des Communes Suisses avec la rédaction d'un article sur la gestion des cyberrisques par les communes.

6. Bilan et perspectives

La période couverte a été marquée par la situation liée à la pandémie de Covid-19, qui a eu des conséquences indéniables sur l'avancée des travaux. La mise en œuvre des projets prévus par le plan de mise en œuvre de la SNPC au niveau cantonal a principalement été perturbée par cette situation exceptionnelle, sans oublier les défis déjà existants, liés aux structures cantonales existantes variables, aux ressources et au personnel dans les cantons.

Malgré ces obstacles, fort est de constater que des étapes importantes ont été franchies dans la mise en œuvre de certains projets et ce, grâce à l'engagement des responsables de projets provenant pour la plupart des structures cantonales qui ont tenté, malgré ces perturbations, de mener à bien leurs travaux. Les cantons améliorent par conséquent la protection de leur administration et de leur population contre les cyberrisques. Les efforts des cantons en matière de cybersécurité se sont traduits, par exemple, par l'adoption de la première stratégie cantonale de protection contre les cyberrisques par l'exécutif du canton de St-Gall.

Pour l'année 2021, les divers projets devraient être poursuivis dans la mesure du possible selon le calendrier établi et leur mise en œuvre dépendra aussi de l'évolution de la situation liée à la pandémie de Covid-19. Il conviendra également de veiller à ce que les intérêts et besoins des cantons soient pris en compte dans les premières réflexions visant à l'élaboration de la troisième SNPC qui débuteront prochainement, à mesure que ces derniers constituent des acteurs incontournables en matière de cybersécurité.