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 (SNPC II)

Mars 2020

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 onze derniers mois, depuis son adoption en avril 2019, 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, responsable adjoint 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 • Élaboration d'un état des lieux • Élaboration du concept de formation • Présentation du concept de formation au comité de la CCDJP	• Décision en session plénière de la CCDJP le 2 avril 2020 • Constitution/remaniement du groupe de pilotage et du groupe de travail • Planification détaillée • Kick-off
Situation de la menace	(2) #MISP – Malware Information Sharing Platform de MELANI pour et avec les cantons	Marc Barbezat, chef de la sécurité numérique du canton de Vaud, en collaboration avec MELANI	• Une taxonomie unique décrivant les cyber-menaces est adoptée par la Confédération et les cantons • Les cantons disposent d'un radar actif de leurs cyber-menaces • 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 cyber-menaces	• Analyse des taxonomies existantes et préparation d'une taxonomie unique décrivant les cyber-menaces • Préparation d'une approche pour accompagner la mise en place / l'évolution d'un processus de veille OSINT • Les cantons ont un accès au radar de situation MELANI • Accompagnement des cantons pour une utilisation active des informations du Radar MELANI	• Accompagnement des cantons pour une utilisation active des informations du Radar MELANI • 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 et pris des mesures 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 cantons	• Les cantons procèdent à l'évaluation • La direction de projet analyse les résultats • Les résultats seront présentés sous forme anonymisée à certaines instances (CSI, CCDJP)
	(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.	• Le groupe de travail a pris connaissance du plan de mise en œuvre des cantons de la SNPC II et du projet.	

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
	(5) Sensibilisation de la population aux cyberrisques	Chantal Billaud, directrice de Prévention Suisse de la Criminalité (PSC)	• 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 commencés leurs activités • Les différents groupes de travail ont élaboré et publié les premiers produits destinés à sensibiliser la population	• Conception d'autres modules de formation sur mesure au sein des groupes de travail respectifs
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 des lignes directrices établies par la CSI en 2017 • Établir une checkliste pour les cantons afin d'évaluer l'état actuel de leur niveau de sécurité des réseaux (réel/objectif). • Mise en œuvre dans six cantons de leur propre 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)
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 d'un hôpital universitaire et des partenaires pour la mise en œuvre du projet	• Constitution du groupe de travail
	(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 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	• Élaboration d'un premier modèle d'organisation cantonale pour la cybersécurité • Discussion du modèle d'organisation cantonale pour la cybersécurité au sein du groupe de travail	• Finalisation du modèle d'organisation cantonale pour la cybersécurité • Présentation du modèle d'organisation cantonale pour la cybersécurité à la CCDJP
Visibilité et sensibilisation	(9) Communication active sur les activités des cantons dans le cadre de la SNPC II	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	• Mise à disposition sur le site internet du RNS des actualités des cantons dans le domaine cyber • Publication du rapport annuel sur l'état d'avancement des projets du plan de mise en œuvre des cantons de la SNPC II	• Organisation de la 8ème Cyberlandsgemeinde avec pour objectif la communication de l'avancement des projets du plan de mise en œuvre des cantons de la SNPC II

1. Introduction

Le plan de mise en œuvre des cantons de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (SNPC II) 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 Cybersécurité 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 II, 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 Cybersécurité du RNS mais également au sein du comité de pilotage de la SNPC II. 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 au cours de la période couverte par ce rapport.

Treize projets sont prévus par le plan de mise en œuvre des cantons de la SNPC II 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 Cybersécurité du Réseau national de sécurité

Le groupe spécialisé Cybersécurité 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 (PSC), 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 de la Confédération à la cybersécurité, du bureau de coordination de la SNPC et du délégué cyberdéfense du DDPS. Le mandat et la composition de ce groupe spécialisé Cybersécurité 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 II 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 deux 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 Cybersécurité du RNS joue également un rôle important comme interface avec le comité de pilotage de la SNPC II 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

Les cantons ont décidé de développer les compétences en matière cybersécurité de leur personnel en particulier. Les administrations cantonales disposeront, grâce au projet intitulé **"Développement d'un concept de formation continue et d'un module pour les administrations cantonales"** (mesure 2 de la SNPC II "Extension et encouragement des compétences en matière de recherche et de formation"), d'un programme complet de formation adapté. Le concept de formation pourrait également être proposé à l'ensemble du personnel des administrations communales et au personnel des différents départements de l'administration fédérale. Sébastien Jaquier, responsable adjoint de l'Institut de lutte contre la criminalité économique (ILCE) de la Haute école de gestion Arc de Neuchâtel, dirige le groupe de travail composé de responsables cantonaux et fédéraux en matière de sécurité de l'information. Ce groupe a effectué un état des lieux partiel des formations (e-Learning inclus) existantes dans les cantons, élaborées spécifiquement pour les administrations cantonales ou

basées sur des solutions commerciales (IS-Fox, ESEC, Wombat, Kaspersky, par exemple). Sur la base de cet état des lieux, le concept de formation a pu être élaboré, il a ensuite été présenté au comité de la CCDJP, qui l'a approuvé lors de sa séance du 6 mars 2020.

Champ d'action 2: Situation de la menace

Pour améliorer leurs capacités de description et d'analyse des cybermenaces en Suisse, les cantons ont prévu de mettre en place et de déployer plusieurs instruments permettant de combattre les intrusions et codes malveillants. Ce projet, intitulé **"#MISP – Malware Information Sharing Platform de MELANI pour et avec les cantons"**, permet la mise en œuvre de la mesure 4 de la SNPC II "Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace". Marc Barbezat, directeur de la sécurité numérique du canton de Vaud, dirige, en collaboration avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), la mise en œuvre de ce projet. En plus du radar de situation MELANI, auquel tous les cantons ont un accès (au minimum à la version statique), l'outil open sources MISP, qui permet l'échange d'informations sur les indices de compromission et dont le but est de mieux détecter les cybermenaces, devrait être connu, utilisé et nourri par les cantons. Le MISP est devenu une référence car elle est largement nourrie par MELANI en particulier. Actuellement, une dizaine de cantons échangent activement des informations opérationnelles relatives aux codes malveillants sur ce réseau. M. Barbezat entreprend un travail d'accompagnement des cantons (sensibilisation, information) pour une utilisation active du MISP est en cours. L'utilisation et la valorisation de cet instrument varie beaucoup d'un canton à l'autre selon la disponibilité des experts et des ressources financières. Pour une utilisation optimisée de ces instruments, une même taxonomie permettant de structurer et de représenter les cybermenaces de manière cohérente et homogène au sein de la Suisse (niveaux Confédération, cantons et communes) est nécessaire. M. Barbezat a analysé les taxonomies existantes (NIST, ENISA, MITRE) et des discussions avec plusieurs partenaires de la Confédération ont eu lieu afin de préparer un vocabulaire unique en lien avec les cybermenaces.

Champ d'action 3: Gestion de la résilience

Afin d'améliorer la résilience informatique des cantons, ces derniers ont prévus trois projets définis par le plan de mise en œuvre.

Les cantons sont amenés à analyser les exigences minimales à satisfaire en matière de processus, de compétences et de tâches grâce à 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). M. Haefeli est, en collaboration avec le RNS, l'OFAE et la Conférence suisse sur l'informatique (CSI), responsable de ce projet intitulé **"Outil d'évaluation pour améliorer la résilience informatique dans les cantons"**, (mesure 5 de la SNPC II "Amélioration de la résilience informatique des infrastructures critiques"). L'objectif de ce projet est d'identifier et d'analyser les failles en matière de résilience informatique de chaque canton et de prendre, sur la base de cette évaluation, des mesures de sécurité ciblées dans le but de diminuer les risques et renforcer leur propre sécurité. En janvier 2020, les cantons ont reçu l'outil qui permettra aux services compétents de procéder à l'analyse avant avril 2020.

Dans le but encore d'améliorer la résilience informatique des cantons, ceux-ci prévoient de favoriser leur collaboration en institutionnalisant les échanges d'expériences et le dialogue. Le projet intitulé **"Développement des échanges d'expériences à travers la Conférence suisse sur l'informatique (CSI) pour la création de bases communes"** est prévu par le plan de mise en œuvre de la SNPC II et sa mesure 7 en particulier (Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons). La responsabilité de ce projet est, selon le plan de mise en œuvre, attribuée au 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. Le groupe de travail Sécurité informatique de la CSI a pris connaissance du plan de mise en œuvre des cantons de la SNPC II et de ce projet, le but étant de définir, au cours des prochaines séances, des prochains objectifs à atteindre.

Le projet "**Sensibilisation de la population aux cyberrisques**"[1] vise à renforcer la prévention de la population afin d'améliorer la résilience de la Suisse en matière de cyberrisques. Chantal Billaud, directrice de Prévention Suisse de la Criminalité (PSC), détient la responsabilité du projet. Une première rencontre entre la Confédération et des polices cantonales et municipales a été organisée afin de définir les structures et canaux adéquats, nécessaire à la mise en œuvre de mesures de prévention efficaces. Les différents groupes (groupe restreint, groupe d'échange et groupes de travail) ont été créés sur la base des discussions et ont commencé leurs activités. Certains groupes de travail ont d'ores et déjà élaboré et publié les premiers produits destinés à sensibiliser la population, détaillés ci-dessous. Tous les projets et mesures sont lancés en collaboration avec le réseau national de soutien aux enquêtes de la lutte contre la criminalité informatique (*Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung*, NEDIK).

- Groupe de travail "Perfectionnement de la police dans le domaine cyber", dirigé par la PSC: Le sondage qu'a mené la PSC a montré qu'il existe un certain besoin en matière de formation supplémentaire.
- Groupe de travail "Films", dirigé par la Police cantonale vaudoise et la Conférence des commandants de police de Suisse romande, Berne et Tessin (CCPC RBT): de courtes campagnes de prévention sur les thèmes des cyberarnaques (petites annonces frauduleuses, arnaques aux sentiments (*Romance scams*) et phénomène des *money mules* ou "passeurs d'argent") ont été diffusées en 2019 via les canaux médiatiques des corps de police et de la PSC. L'alliance suisse pour la sécurité sur internet (Swiss Internet Security Alliance) contribue aux campagnes de prévention des corps de polices et en diffuse les messages sur son site (ibarry.ch) et ses réseaux sociaux.
- Groupe de travail "Petites et moyennes entreprises", dirigé par la Police cantonale de Berne et MELANI. Une brochure ainsi que du matériel de prévention destiné spécifiquement aux PME ont été mis à disposition en février 2020.
- Groupe de travail "Site national de prévention et d'annonce", dirigé par le NEDIK et la Police cantonale zurichoise en collaboration avec MELANI: la police cantonale zurichoise a mis en ligne, en novembre 2019, le site cybercrimepolice.ch qui met en garde la population contre la cybercriminalité.

Champ d'action 4: Normalisation et régulation

Les cantons ont adopté la politique de sécurité des réseaux établie par la CSI en 2017 (disponible sur Intranet pour tous les membres de la CSI). Ils prévoient, dans le cadre de la mesure 8 de la SNPC II "Définition et introduction de normes minimales", de mettre en œuvre les standards de la **politique de sécurité des réseaux de la CSI** au niveau cantonal. Le directeur du groupe de travail Sécurité informatique de la CSI, Adrian Gutknecht, dirige ce projet et travaille en collaboration avec le centre de compétence PTI (Kompetenzzentrum Polizeitechnik). 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. Aujourd'hui, six cantons ont mis en œuvre leur propre politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) et neuf cantons la prévoient en 2020. Intégrer les standards de la politique de sécurité des réseaux de la CSI au niveau cantonal implique des adaptations techniques et structurelles des infrastructures et donc des conséquences sur la planification budgétaire cantonale. Le degré de mise en œuvre par les cantons dépend donc en partie de ces processus de long terme.

[1] 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 II, p. 6

Champ d'action 5: Gestion de crise

Le plan de mise en œuvre des cantons prévoit pour la mesure 17 de la SNPC II "Exercices communs de gestion de crise" un projet intitulé "**Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé**". Le but de ce projet est, dans un premier temps, la réalisation d'un *table top* exercice comportant des aspects cyber au sein d'une infrastructure critique dans le secteur de la santé, puis d'un exercice-cadre d'état-major, durant lesquels la stratégie de conduite est testée et la coordination opérationnelle entre la Confédération, les cantons et les exploitants d'infrastructures critiques et les services concernés fonctionne.
Il s'agissait, dans un premier temps, d'identifier une infrastructure critique, en l'occurrence un hôpital universitaire. André Duvillard, délégué du RNS et responsable du projet, est en contact avec l'Hôpital universitaire de Zürich, qui a manifesté son intérêt pour la mise en œuvre de ce projet. Les discussions sont en cours afin de composer un groupe de travail qui s'occupera d'élaborer le scénario de référence.

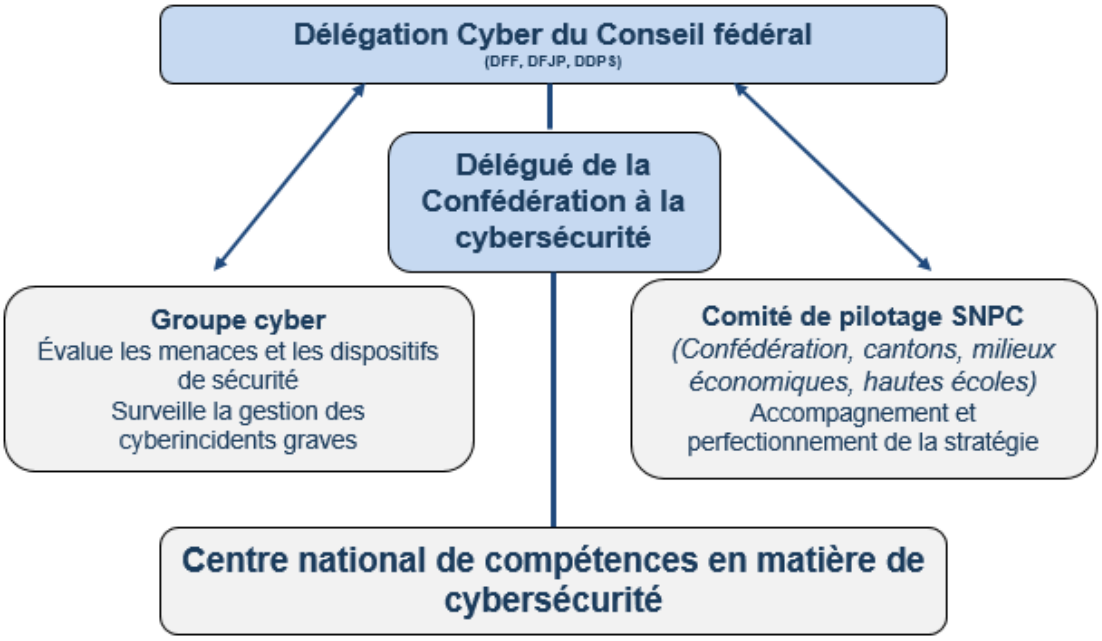
Le projet "**Création d'organisations cantonales pour la cybersécurité**" a pour but d'élaborer un modèle d'organisation qui puisse être mis en œuvre dans les cantons et soit à même de coordonner les divers aspects de matière de cybersécurité. Le groupe de travail RNS, dirigé par le délégué du RNS et composé de représentants des cantons de Bâle-Ville, Fribourg, Genève, Tessin et Zürich, s'est chargé, dans un premier temps, d'élaborer des lignes directrices et une base de travail sous forme de concept, dont la finalisation est prévue au printemps 2020. Celui-ci sera présenté à la CCDJP dans le courant de cette année. Le groupe de travail a rencontré quelques défis et besoins liés à l'élaboration de ce concept tels que la compréhension et l'étendue des compétences d'un éventuel cyberdélégué cantonal, sa position dans l'organisation et sa subordination, qui varient d'un canton à l'autre. Malgré les différents besoins et attentes des cantons dans le domaine de la cybersécurité, le concept facilitera la réflexion des autorités cantonales compétentes lors de l'élaboration de leur propre cyberorganisation.

Champ d'action 6: Visibilité et sensibilisation

Les cantons ont montré, lors de l'élaboration du plan de mise en œuvre des cantons, un certain intérêt à ce que leurs activités dans le cadre de la SNPC II soient visibles. Un projet intitulé "**Communication active sur les activités des cantons dans le cadre de la SNPC II**" (mesure 28 de la SNPC II "Élaboration et mise en œuvre d'un concept de communication pour la SNPC") est prévu par le plan de mise en œuvre des cantons de la SNPC II. Le RNS, dont le délégué est responsable du projet, rend visible, grâce à son site internet, les activités des cantons dans le cadre de la SNPC II. À ce jour, un nouvel onglet "Actualités" a été ouvert sur la page internet du RNS (svs.admin.ch), permettant la mise à disposition des actualités des cantons dans le domaine cyber, régulièrement mises à jour. Le RNS se charge également de l'organisation de la huitième Cyberlandsgemeinde, qui aura lieu en 2020 et aura comme objectif, de même que le présent rapport, de communiquer sur l'avancement des projets du plan de mise en œuvre des cantons de la SNPC II.

4. Implication des cantons dans les structures cyber de la Confédération

L'année 2019 a été caractérisée par la mise en œuvre des structures cyber de la Confédération telles qu'adoptées par le Conseil fédéral en janvier 2019, sur la base de sa décision du 4 juillet 2018.



La désignation du délégué du Conseil fédéral à la cybersécurité a permis aux différentes instances de progressivement débuter leurs activités et ce en y associant systématiquement les cantons. Ainsi le président de la CCDJP a été invité à participer à la première séance de la délégation cyber du Conseil fédéral. D'autre part, le délégué de la Confédération à la cybersécurité, dès son entrée en fonction, a été associé aux activités du RNS dans le domaine cyber.

Le centre national de compétences en matière de cybersécurité est encore en phase de développement et son champ devra être précisé au cours des prochains mois. Néanmoins, plusieurs cantons ont d'ores et déjà manifesté leur intérêt à y être associés dans le cadre de projets qu'ils développent. Deux tables rondes sous la présidence du Conseiller fédéral Ueli Maurer, chef du Département fédéral des finances (DFF), se sont tenues en août et novembre 2019.

5. Autres activités du bureau du délégué du RNS

Grâce aux projets menés dans le cadre de la SNPC I et des contacts établis au cours des dernières années, le bureau du délégué RNS a été en mesure de construire un important réseau dans le domaine cyber tant au niveau de la Confédération, des cantons, des communes que des infrastructures critiques. Ceci lui permet d'avoir une excellente vision des enjeux, mais aussi de pleinement jouer son rôle d'interface au niveau stratégique entre les cantons et Confédération.

En sa qualité de membre du groupe d'experts cyber du DDPS et de la plateforme stratégique du Cyberboard, le délégué RNS dispose ainsi d'une excellente vue d'ensemble sur les enjeux des trois domaines d'activité que sont la cybersécurité, la cyberdéfense et la cybercriminalité. Même si notre système fédéraliste impose de nombreuses structures de coordination, des progrès indéniables ont été réalisés au cours des cinq dernières années, lesquels ont conduit à une meilleure prise en compte des intérêts et besoins des différents acteurs institutionnels.

6. Bilan et perspective

En adoptant le plan de mise en œuvre des cantons de la SNPC II, les cantons ont clairement manifesté leur volonté d'améliorer, sous leur propre responsabilité et de leur propre initiative, la protection de leur population contre les cyberrisques. Certains défis, liés aux structures cantonales existantes variables, aux ressources et au personnel dans les cantons sont

toutefois venus mettre à l'épreuve la mise en œuvre des projets. Malgré ces quelques difficultés, l'avancement des travaux est globalement satisfaisant. En effet, la majorité des projets prévus par le plan de mise en œuvre des cantons sont initiés et le calendrier est généralement respecté. L'engagement des chef(fe)s de projets, provenant pour la plupart de structures cantonales, et leur collaboration fructueuse avec le RNS, contribuent fortement à la mise en œuvre avancée des projets.

Pour l'année 2020, les divers projets devraient être poursuivis selon le calendrier établi. Il conviendra en particulier de veiller à ce que les intérêts et besoins des cantons soient pris en compte de manière systématique, à mesure qu'ils constituent un acteur incontournable en matière de cybersécurité.

Finalement, et en ce qui concerne le rôle futur des cantons, un projet doit être mentionné de manière spécifique. Il s'agit de la contribution des cantons au centre national de compétences en matière de cybersécurité. En effet, à la suite des deux tables rondes mentionnées au chapitre 4, il a été convenu qu'un véritable état des lieux de tous les projets et prestations développés dans les cantons, le plus souvent en partenariat avec les mondes académique et de l'économie, aussi exhaustif que possible, soit établi. Cet état des lieux devrait servir de catalogue de référence à disposition du centre national de compétences en matière de cybersécurité et de tous les cantons. Un concept a été établi dans ce sens par les délégués à la cybersécurité et au Réseau national de sécurité. Il a été présenté au colloque présidentiel de la Conférence des gouvernements cantonaux (CdC) en janvier 2020. Celle-ci a pris connaissance du concept, qui a été formalisé dans le cadre d'un mandat au délégué du RNS. Celui-ci a été approuvé par la plateforme politique RNS par voie de circulation en mars 2020.