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 2022

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 2021 – mars 2022) et a été élaboré par le Réseau national de sécurité, en collaboration avec les responsables 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 mesurables (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'intention 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 des formations continues disponibles dans les cantons • 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 • Appel d'offre (conforme aux exigences de l'OMC), sélection du fournisseur et conclusion du contrat • Planification et début de la réalisation • Ajout d'un icône « les autorités » sur le site ncsc.ch (mesure d'accompagnement)	• Coneption 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	• Adoption par la Confédération et les cantons d'une taxonomie unique décrivant les cybermenaces • Radar actif des cybermenaces à la disposition des cantons • Échanges actifs d'informations opérationnelles relatives aux logiciels malveillants entre les cantons • Évaluation périodique par les cantons de la sécurité de leurs points d'accès réseau périphériques exposés sur internet • Diffusion périodique par les cantons de rapports de veille sur les cybermenaces	• Élaboration d'une taxonomie unique décrivant les cybermenaces • Utilisation par 14 cantons de la plateforme MISP • Formations par le NCSC 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	• Organisation par le NCSC de formations à l'utilisation de la plateforme MISP • Auto-évaluation des cantons de leur niveau de préparation face aux cybermenaces liées aux rançongiciels
Gestion de la résilience	(3) Outil d'évaluation pour améliorer la résilience informatique dans les cantons	Réseau national de sécurité, en collaboration avec Max Haefeli (Haefeli Consulting)	• Identification par les cantons de leurs failles grâce à l'outil d'évaluation et mesures appropriées pour améliorer leur résilience informatique • À l'issue de l'évaluation, application par les cantons de mesures ciblées pour améliorer leur résilience informatique. • Présentation des résultats 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 du premier outil d'évaluation aux organisations participantes • Première évaluation par les organisations participantes • Réception et analyse des données • Envoi de la première évaluation aux organisations participantes • Présentation sous forme anonymisée des résultats au groupe spécialisé cyber du RNS	• Analyse des résultats de la deuxième 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

				• Échange d'expériences avec le délégué fédéral à la cybersécurité et le secrétaire général de la CSI • Présentation sous forme anonymisée des résultats à certaines instances • Préparation de la deuxième enquête	
	(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	• Garantie par les cantons de la participation de leurs préposés à la sécurité de l'information au Groupe de travail Sécurité informatique de la CSI • Garantie par les cantons de la formation et de l'instruction régulière et adaptée aux besoins de son personnel et de ses partenaires externes dans toutes les questions de sécurité de l'information et de cyberrisques • Mise en œuvre par les cantons d'une gestion des risques informatiques (en tant que partie intégrante de la gestion cantonale des risques) qui couvre les risques liés aux infrastructures critiques • Introduction par les cantons d'un système de gestion de la sécurité des informations (SGSI) adapté à leur organisation	• 17 cantons désormais représentés au sein du groupe de travail Sécurité informatique de la CSI • Prise de connaissance, par le groupe de travail, du plan de mise en œuvre par les cantons de la SNPC et du projet • Plusieurs recommandations et directives émises par la CSI et mises à disposition des cantons • Échange d'expériences avec les membres et workshop dans le cadre de la 9e Cyber-Landsgemeinde sur le sujet des répercussions des «Solarwind Hacks» • Activités de la CSI transférées à l'Administration numérique suisse (ADS) au 1er janvier 2022.	
	(5) Sensibilisation de la population aux cyberrisques[2]	Fabian Ilg, directeur 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	• Création de structures et début des activités de différents groupes (groupe restreint, groupe de dialogue et groupes de travail) • Élaboration de plusieurs produits destinés à sensibiliser la population • Campagne de sensibilisation en ligne, organisée en collaboration avec le NCSC, iBarry et « eBanking – en toute sécurité ! » (EBAS).	• Conception d'autres produits destinés à sensibiliser la population • Poursuite de la collaboration avec les acteurs concernés et renforcement des partenariats établis
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) • Définition et application des normes • 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) • Information aux cantons et échange d'expériences sur la nouvelle loi sur la sécurité de l'information	• Mise en œuvre dans 11 cantons de leur propre politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) jusqu'en 2023 • Poursuite de la mise en œuvre prévue au-delà de la période de la SNPC 2018-2022

[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 II, p. 6

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	• Un certain 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) • Connaissance des responsabilités et des interlocuteurs par les participants • Connaissance des processus par les 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 • Préparation de l'exercice, développement de la méthode, des objectifs et du scénario de référence • Organisation par le RNS d'un exercice « table top » en décembre 2021	• Organisation d'un exercice-cadre d'état-major
	(8) Création d'organisations cantonales pour la cybersécurité	Groupe de travail, sous la direction d'André Duvillard, délégué du RNS	• Mise au point d'une ligne directrice et base de travail avec le groupe de travail du RNS • Comparaison entre la situation réelle et la situation visée dans chaque canton • 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 • Mise en œuvre en cours ou prévue des recommandations du concept dans plusieurs cantons (LU, ZH, BS, VD, SG, AG,…)	• Mise à jour du concept d'organisation cantonale pour la cybersécurité
Visibilité et sensibilisation	(9) Communication active sur les activités des cantons dans le cadre de la SNPC 2018-2022	André Duvillard, délégué du RNS	• Existence et application d'un concept de communication (directives, compétences, processus) • Mise à disposition en temps voulu de divers produits de communication à l'intention 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 9e Cyber-Landsgemeinde (septembre 2021) • 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 10e 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 des 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 RNS 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.

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 celle-ci. Quatre mesures du champ d'action de la poursuite pénale sont 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, des responsables de projet issus des cantons et soutenus par le RNS sont chargés de leur mise en œuvre, laquelle repose sur le calendrier que le groupe de travail du RNS a jugé approprié lors de sa réunion du 7 mai 2019, mais qui permet toutefois une certaine marge de manœuvre.

2. Groupe spécialisé Cyber du Réseau national de sécurité

Le groupe spécialisé Cyber du RNS, présidé par le délégué du RNS, est constitué de membres issus 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 et de l'Association des communes suisses, ainsi que du délégué fédéral à la cybersécurité et du délégué cyberdéfense du DDPS.

Le mandat de ce groupe spécialisé Cyber du RNS, créé dans le cadre de la première SNPC, a été adapté 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. La composition de ce groupe spécialisé a également été revue ; il accueille désormais Peppino Giarritta, chargé de mission Confédération et cantons de l'Administration numérique Suisse (ANS), dont les structures sont comparables à celles du RNS. Cette nouvelle organisation a été créée par le Conseil fédéral et les gouvernements cantonaux le 1er janvier 2022 afin de renforcer la collaboration entre la Confédération, les cantons, les communes et les villes en vue de la mise sur pied et du pilotage de la transformation numérique de l'administration. L'intégration du nouveau chargé de mission de l'ANS au sein du groupe spécialisé Cyber constitue un premier pas vers une collaboration plus intensive entre le RNS et l'ANS et d'un rapprochement des domaines de la cybersécurité et de la transformation digitale.

Les tâches du Groupe spécialisé Cyber du RNS consistent principalement à coordonner la réalisation des différents projets du plan de mise en œuvre par les cantons de la SNPC. 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 qu'un représentant du secrétariat général de la CCDJP en sont formellement membres.

3. État 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 fédérale, cantonales et communales. Un état des lieux partiel des formations existantes dans les cantons et un concept de formation ont été élaborés par le groupe de travail expressément constitué. Le comité de la CCDJP a approuvé ce concept et également octroyé le budget nécessaire à sa conception. Après un *Request for Information* transmis à quatre entreprises pressenties, un appel d'offre conforme aux exigences de l'Organisation mondiale du commerce a été lancé par le groupe de travail, qui, à son terme, a choisi le fournisseur. La planification des travaux de conception du module de formation sous forme d'e-Learning, a été fixée et la réalisation a débuté.

Une mesure d'accompagnement définie par le groupe de travail a été également mise en œuvre ; il s'agissait d'ajouter un icône « Les autorités » sur le site du ncsc.ch, qui fournit aux autorités les informations nécessaires relatives aux menaces actuelles, ainsi qu'une marche à suivre en cas de cyberattaques.

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 celles-ci un langage commun minimum. Concernant l'objectif principal de ce chantier, 14 cantons (AG, BS, GE, GR, JU, LU, SZ, SO, VD, VS, ZH, ZG ainsi que BE et SG via leur fournisseur de services) utilisent la solution MISP de MELANI et exploitent les informations fournies, améliorant ainsi leurs capacités de définition et d'analyse des cyberrisques. De plus, dix formations ont été organisées par le NCSC en 2021, auxquelles une vingtaine de personnes ont participé en moyenne. L'alternative virtuelle à l'organisation de ces formations s'est généralisée pour ce projet. Ces formations vont se poursuivre en 2022 et seront complétées par une campagne d'autoévaluation par les cantons de leur niveau de préparation face aux cyberattaques.

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. Deux évaluations sont prévues pendant la période de la stratégie 2018-2022. C'est pourquoi, l'année dernière, les activités menées dans le cadre de ces mesures se sont concentrées essentiellement sur la préparation de la deuxième évaluation. L'analyse est rendue possible grâce à un outil d'évaluation Excel élaboré par Max Haefeli, depuis lors propriétaire de Haefeli Consulting. Cet outil a été conçu selon la norme minimale pour les TIC[3] et adapté aux besoins des cantons. Tous les documents et outils de travail pour la deuxième évaluation ont été envoyés en décembre 2021. Le délai de remise des formulaires remplis est fixé à fin mars 2022. En participant une nouvelle fois à l'évaluation nationale, les cantons ont un instantané anonymisé et comparatif de la résilience informatique de leur organisation et de celle des autres, ainsi qu'une visualisation des progrès réalisés par chacun d'eux.

[3] Norme minimale pour améliorer la résilience TIC de l'Office fédéral pour l'approvisionnement économique du pays (OFAC)

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 »), les cantons favorisent leur collaboration en institutionnalisant les échanges d'expériences et le dialogue, améliorant ainsi leur résilience informatique.

Le groupe de travail Sécurité de l'information et cybersécurité de la CSI, placé sous la direction d'A. Gutknecht, a continué de siéger régulièrement pendant la période sous revue. Au premier semestre, il a approuvé deux recommandations, l'une concernant la publication des informations sur le personnel informatique et l'autre traitant de la mise en place d'un monitorage de la sécurité (avec ou sans *security operations centers* [SOC]). Pendant la période sous revue, le groupe de travail Télécommunication de la CSI a aussi rédigé des lignes directrices faisant office de recommandation pour le travail avec l'IoT (Internet des objets).

La création du groupe de travail Cloud Governance remonte déjà au mois de septembre 2020. Celui-ci élabore des bases, des outils de travail et des principes de bonnes pratiques pour l'intégration et l'utilisation des services en nuage dans l'administration publique. Il compte plus de vingt collaborateurs issus de la Confédération, des cantons, et des villes. Il a procédé à une analyse particulièrement intensive du domaine de la protection des données lors d'échanges avec différents partenaires et formulé des clauses standard pour la rédaction des contrats avec les prestataires informatiques afin de garantir la sécurité juridique. La préparation de contrats type ainsi que la négociation des conditions contractuelles est une offre centrale de la CSI, car le regroupement des exigences et des volumes apporte des avantages lors de négociations avec des fournisseurs de prestations informatiques.

Pour améliorer la cybersécurité dans les communes, la CSI a lancé une étude de faisabilité concernant le produit SCION (Internet pour un transfert sûr des données) en collaboration avec le centre de recherche de l'EPFZ.

Une mention particulière revient en conclusion aux répercussions du piratage informatique Solarwind sur les administrations publiques, qui a occupé des mois durant les responsables de la sécurité. La CSI a discuté de la situation de la menace en décembre 2020 avec ses membres et organisé en août 2021, dans le cadre de la Cyber-Landsgemeinde, un atelier consacré à des échanges approfondis d'expertises et d'expériences avec les personnes intéressées des cantons et de la Confédération.

Les activités de la CSI ont été transférées au 1er janvier 2022 à l'Administration numérique Suisse (ANS).

Les activités prévues par le projet « **Sensibilisation de la population aux cyberrisques** » 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. Dans ce cadre, la Prévention Suisse de la Criminalité (PSC) a établi un partenariat fort avec le réseau national de soutien aux enquêtes de la lutte contre la criminalité informatique (*Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung* NEDIK) et cybercrimepolice.ch. En outre, elle échange régulièrement des informations sur le thème de la sensibilisation et sur les phénomènes de cybercriminalité avec le NCSC. Plusieurs produits visant à sensibiliser le public aux cyberrisques ont été élaborés, mis à la disposition de la population et relayés via les différents canaux de communication de la PSC. Celle-ci a d'ailleurs renforcé sa présence sur différents réseaux sociaux ; elle les a développés afin d'assurer sa visibilité en ligne. Parmi les projets que la PSC a mis en œuvre durant la période couverte, on peut notamment citer :

- une campagne de sensibilisation en ligne "S-U-P-E-R" sur les 5 étapes de la sécurité numérique, en collaboration avec le NCSC, l'EBAS et iBarry,
- une brochure « Rendements de rêve? Gare au réveil! » ainsi que la sensibilisation de plusieurs instituts financiers par l'intermédiaire de l'Association Suisse des Banquiers, l'Association Suisse d'Assurances et l'Association Suisse des Institutions de Prévoyance,
- trois nouvelles vidéos de prévention sur les thèmes « sexting », « arnaque aux faux logements » et « fraude à l'investissement »,
- la coordination et le relais de la campagne #gaffetoi de la police de la ville de Zürich, lancée dans le cadre de Card Security, qui a pour but d'alerter le public sur les risques liés aux achats en ligne avec les cartes de débit et de crédit.

Cette mesure a pour public-cible la population dans son ensemble. Dans le cadre du travail de sensibilisation aux « rendements de rêve », on a toutefois fait l'effort de cibler une population âgée de plus de 50 ans, notamment par la prise de contact avec des institutions offrant des formations continues de préparation à la retraite, telles que Publica par exemple.

Champ d'action 4 : normalisation et régulation

Les cantons prévoient, dans le cadre de la mesure 8 de la SNPC 2018-2022 **« Définition et introduction de normes minimales »**, de mettre en œuvre la politique de sécurité des réseaux établie par la CSI en 2017 (disponible sur l'intranet de la CSI pour tous les membres). L'état de la mise en œuvre correspond en grande partie à l'état relevé dans le rapport de la période précédente. À l'heure actuelle, 8 cantons ainsi que la principauté du 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 prévoient de le faire d'ici à 2023. On peut s'attendre à ce que la mise en œuvre de la politique de sécurité des réseaux 2017 dans les cantons restants ne s'achèvera qu'après la période de la stratégie. Néanmoins, la norme minimale exigée a été un sujet important dans les cantons l'année dernière. Ainsi, le groupe de travail Sécurité de l'information et cybersécurité de la CSI, en collaboration avec le groupe de travail Cloud Governance de la CSI, a prévu d'adresser en annexe les exigences de sécurité accompagnant l'utilisation des services en nuage sous une forme élargie de la politique de sécurité des réseaux 2017. Les cantons sont en outre concernés par la nouvelle loi sur la sécurité de l'information (LSI). Celle-ci vise à esquisser le cadre d'un traitement sûr des informations, dont la Confédération est responsable, et de l'engagement sûr des moyens informatiques. Cela signifie que les cantons aussi sont tenus de garantir une sécurité de l'information au moins équivalente dans le traitement des données ou l'accès aux moyens informatiques de la Confédération. En collaboration avec le DDPS et avec d'autres partenaires des cantons (CG MPS et PTI), A. Gutknecht, président du groupe de travail Sécurité de l'information et cybersécurité de la CSI, s'occupe de dispenser une information appropriée et d'engager le dialogue sur la nouvelle loi dont l'entrée en vigueur est prévue le 1er avril 2023. Il s'agit en particulier de clarifier l'implication des cantons dans le cadre de la LSI et d'en déduire les exigences de sécurité nécessaires.

Champ d'action 5 : gestion de crise

Dans le cadre du projet **« Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé »** (mesure 17 de la SNPC « Exercices communs de gestion de crise »), le RNS, en collaboration avec le NCSC (Max Klaus, chef suppléant de la cybersécurité opérationnelle CSO et Pascal Lamia, responsable opératif), avec Markus Meile, chef d'état-major de l'organe de gestion de crise de la ville de Zurich et avec Balz Dürst, collaborateur scientifique, Chancellerie fédérale, Section aide à la conduite stratégique (SACS), a organisé en décembre 2021 un exercice *table top*. L'année dernière, les activités dans le cadre de cette mesure consistaient pour l'essentiel à préparer l'exercice, à savoir définir la méthode et les objectifs et adapter le scénario en conséquence. En raison de la pandémie, la direction de l'exercice a mis un point d'honneur à ne pas solliciter trop fortement les ressources de l'USZ.

Les principaux enseignements de l'exercice se réfèrent à la portée et à la grande confusion que produirait une cyberattaque sur l'USZ. Tous les groupes, les directions et les services de l'USZ seraient pour une bonne part associé à la gestion de la crise. De surcroît, les personnes exercées ont reconnu qu'il était nécessaire de sensibiliser en continu aussi bien la direction et le conseil de l'hôpital que l'ensemble du personnel afin d'être prêt le cas échéant. Il est prévu d'organiser, vers la fin de la période de la stratégie, un exercice cadre d'état-major basé sur cette situation et confrontant une nouvelle fois les participants à une cyberattaque. Contrairement aux exercices *table top* précédents, de nouveaux éléments fictifs viendront rehausser l'impression d'urgence.

Le concept « Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité » [4], élaboré dans le cadre de la mesure 8 « **Création d'organisations cantonales pour la cybersécurité** » par un groupe de travail du RNS, en est la pièce maîtresse. Après son adoption par la CCDJP en novembre 2020, il a été présenté à plusieurs commissions par le délégué du RNS, notamment au Cyberboard et dans le cadre d'un atelier à la Cyber-Landsgemeinde en 2021, dirigé par le délégué du RNS en collaboration avec Florian Schütz, délégué fédéral à la cybersécurité. Durant la période précédente, plusieurs cantons ont réfléchi à leur organisation dans le domaine de la cybersécurité. Quelques-uns d'entre eux ont déjà pris des mesures concrètes. Par exemple, le canton de Lucerne a mis au concours pour la première fois un poste de délégué à la cybersécurité à l'automne 2021. De son côté, le canton de Zurich a fait savoir que son office de l'informatique travaillait à une proposition de cyberorganisation cantonale selon ce concept en collaboration avec la police cantonale zurichoise, le ministère public et la protection de la population. Dans le courant de l'année 2022, le concept existant sera mis à jour pour la première fois et complété par des exemples des cantons. Afin d'obtenir une vue complète de la cyberorganisation cantonale, une étude s'impose.

Champ d'action 6 : visibilité et sensibilisation

Le RNS respecte l'intérêt des cantons à rendre visibles leurs propres travaux 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 de la cybersécurité sont régulièrement publiées sur le site internet du RNS (svs.admin.ch). La neuvième édition de la Cyber-Landsgemeinde, qui a pour objectifs de favoriser le dialogue entre acteurs concernés et d'échanger des informations sur l'avancement des projets du plan de mise en œuvre des cantons de la SNPC, s'est tenue le jeudi 16 septembre 2021. Les discussions ont plus particulièrement porté sur le cas d'une cyberattaque concrète et de sa gestion, ainsi que sur les questions d'identité numérique. Cet évènement annuel a rassemblé plus d'une centaine de personnes principalement issues des cantons et de la Confédération.

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

Les structures de cybersécurité de la Confédération adoptées par le Conseil fédéral en janvier 2019 se présentent comme telles :

[4] Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité, Réseau national de sécurité (2021)

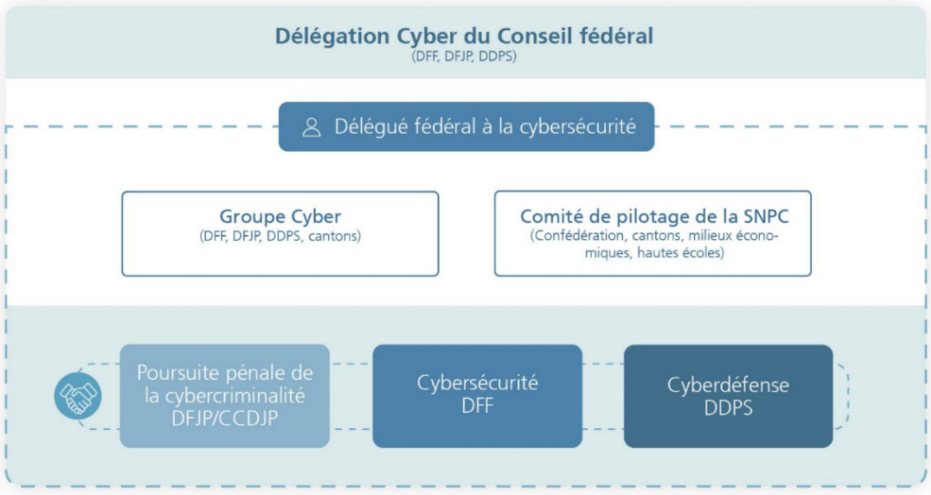

Illustration I : Organisation de la Confédération pour la cybersécurité (Source : NCSC)

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 dialogue entre le RNS et le délégué fédéral à la cybersécurité, en poste depuis août 2019 et dont le rôle est 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, s'est maintenu au cours des douze derniers mois. L'étroite collaboration qui a lieu entre le RNS et le Centre national pour la cybersécurité (NCSC) s'est illustrée dans le cadre de plusieurs travaux.

Dans le cadre du mandat « Réseau de compétence cyber », attribué au RNS par sa plateforme politique en mars 2020, l'enquête réalisée par le RNS avait mis en lumière une large offre de formation et de perfectionnement dans le domaine de la cybersécurité. Le RNS s'est alors chargé d'élaborer un **aperçu de ces formations, proposées par des universités et hautes écoles suisses**, en collaboration avec le Cyber Defence Campus d'armasuisse et l'Académie Militaire (ACAMIL). Le NCSC a publié en novembre 2021 cet aperçu sur son site internet[5] et l'a actualisé en février 2022.

Le RNS a été intégré aux travaux de mise en œuvre de la mesure 9 de la SNPC 2018-2022 (examen d'une **obligation de notifier** les cyberincidents et décision quant à son introduction) par le NCSC. Selon la stratégie nationale de protection des infrastructures critiques, les autorités font partie d'un secteur partiel critique, raison pour laquelle les autorités cantonales et communales seront soumises à l'obligation de notifier. De plus, beaucoup d'entreprises soumises à l'obligation de notifier ont des organes responsables au niveau cantonal ou communal. Dans ce sens, le délégué du RNS a participé à plusieurs séances du comité de coordination sur la création d'une obligation de notifier, qui étaient dirigées par le bureau du NCSC. La consultation concernant l'avant-projet de modification sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques, auquel le RNS est appelé à contribuer, est ouverte jusqu'à mi-avril 2022. Cet avant-projet crée les bases légales nécessaires à l'introduction de l'obligation de signalement et définit les tâches du NCSC, qu'il institue comme centrale de signalement des cyberattaques. Le Conseil fédéral entend renforcer le système d'annonce en obligeant les exploitants d'infrastructures critiques à signaler au NCSC les cyberattaques dont ils sont victimes.

[5] Aperçu des offres de formation en Suisse dans le domaine de la cybersécurité

L'obligation vise à permettre au NCSC de dresser un tableau précis de la situation, d'évaluer le niveau de menace et d'identifier les modes opératoires à un stade précoce en se basant sur des informations complètes et, ainsi, d'alerter à temps les autres exploitants d'infrastructures critiques.

Le plan de mise en œuvre de la SNPC 2018-2022 prévoyait, dans le cadre du *controlling* stratégique, un **examen de l'efficacité** d'ici à la fin de l'année 2022. Le NCSC a mandaté à cet effet les deux entreprises de recherche et de conseil econcept et EBP. En tant que membre du comité de pilotage et service responsable des mesures, le RNS a été associé à ce processus. Concrètement, le délégué et le bureau ont été interrogés, entre autres, sur l'utilité et l'adéquation de la SNPC 2018-2022 eu égard aux défis dans le domaine Cyber. Le rapport sera rendu d'ici à la fin du premier trimestre 2022.

5. Autres activités du bureau du délégué du RNS

Durant la période couverte, le RNS a été engagée dans plusieurs activités pouvant être considérées comme des effets subséquents de la mise en œuvre de la SNPC 2018-2022, et en particulier dans des projets prévus par le plan de mise en œuvre des cantons de la même SNPC.

La période couverte a vu la collaboration entre le RNS et le Swiss Support Center for Cybersecurity (SSCC) s'intensifier. Le SSCC avait déjà présenté en détail ses tâches et son rôle lors d'une séance du groupe spécialisé Cyber du RNS en décembre 2020. Il a proposé de tenir le rôle d'intermédiaire pour les demandes des pouvoirs publics dans le domaine de la cybersécurité et, dans ce cadre, de mettre son réseau particulier dans le domaine académique à la disposition des participants. Lors d'un séminaire en ligne organisé par le SSCC en mai 2021, le délégué a présenté un exposé sur la sécurité des chaînes d'approvisionnement en logiciels (*Software Supply Chain Security*). Le 23 novembre 2021, le SSCC et le RNS ont organisé un autre séminaire en ligne sur le thème des attaques avec rançongiciels, qui a été suivi par plus d'une centaine de personnes issues des disciplines les plus diverses du monde académique, des autorités et de l'économie privée. Une fois de plus, le SSCC, par son savoir technique, a soutenu les mesures définies dans le plan de mise en œuvre des cantons. Il a aussi présenté ses propres idées de projets venant compléter ces mesures.

Les cyberattaques, notamment par des rançongiciels, est en outre une thématique qui préoccupe fortement les communes. Un dialogue a été initié entre le RNS et l'Association des Communes Suisses au sujet de la protection de celles-ci contre les cyberattaques. Ces discussions ont à terme pour objectif de définir une ou plusieurs solutions de protection pour les communes contre ces attaques. Un état des lieux de l'organisation des communes de Suisse contre ces menaces pourrait être prochainement élaboré.

D'autre part, le RNS a initié un dialogue entre l'Armée et d'autres offices concernés afin d'examiner de quelle manière les cantons pourraient être soutenus dans l'organisation d'exercices cyber.

Finalement, le délégué RNS a été sollicité pour faire partie du Conseil consultatif du projet « Trust Valley » né à l'initiative des cantons de Vaud et Genève, et qui vise à promouvoir toute l'expertise de la région lémanique dans le domaine de la confiance numérique et la cybersécurité. Dans ce contexte, les collectivités publiques, institutions académiques et acteurs économiques s'unissent pour faire rayonner ce pôle de compétences unique et favoriser l'éclosion de projets novateurs.

6. Bilan et perspectives

Les travaux relatifs à la mise en œuvre des projets se sont poursuivis sur la période couverte, grâce à l'engagement des responsables de projets. En effet, malgré les différentes restrictions liées à la pandémie de Covid-19, qui avaient eu des conséquences sur l'avancée des travaux, la mise en œuvre est globalement satisfaisante. Les cantons améliorent ainsi la protection de leur administration et de leur population contre les cyberrisques.

L'année écoulée a également vu le renforcement de la collaboration entre le NCSC et les cantons, en particulier dans le cadre des réflexions sur les nouveaux objectifs stratégiques de la troisième SNPC, le but étant que les cantons y soient encore mieux intégrés. Ceux-ci seront en outre contactés par le RNS qui, avec leurs représentants, coordonne la mise en œuvre de la troisième stratégie au niveau cantonal. Le Groupe spécialisé Cyber du RNS se réunira d'ailleurs trois fois, au lieu des deux séances ordinaires annuelles, dans le courant 2022.

La mise en œuvre des divers projets devrait être poursuivie jusqu'à la fin de l'année 2022, dans la mesure du possible selon le calendrier établi. Dans le futur, il s'agira également d'approfondir la collaboration avec le chargé de mission Confédération et cantons de l'ANS, d'autant plus que les activités de la CSI ont été reprises par cette récente structure.