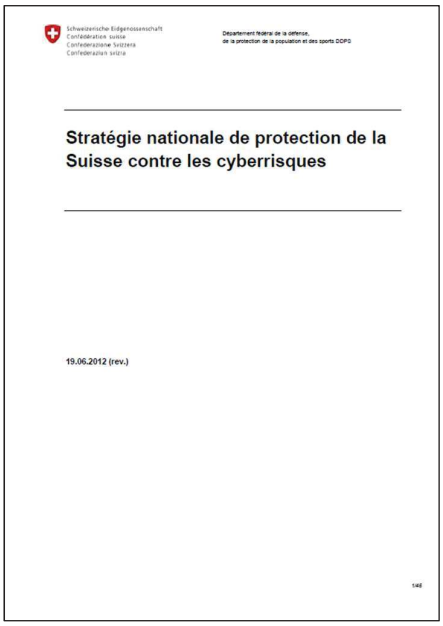
La stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

1) Résultats de la mise en œuvre de la SNCP 2012-17
2) État de l'élaboration de la SNPC 2018-22

SNPC 2012-2017


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Stratégie nationale de protection de la Suisse contre les cyberrisques

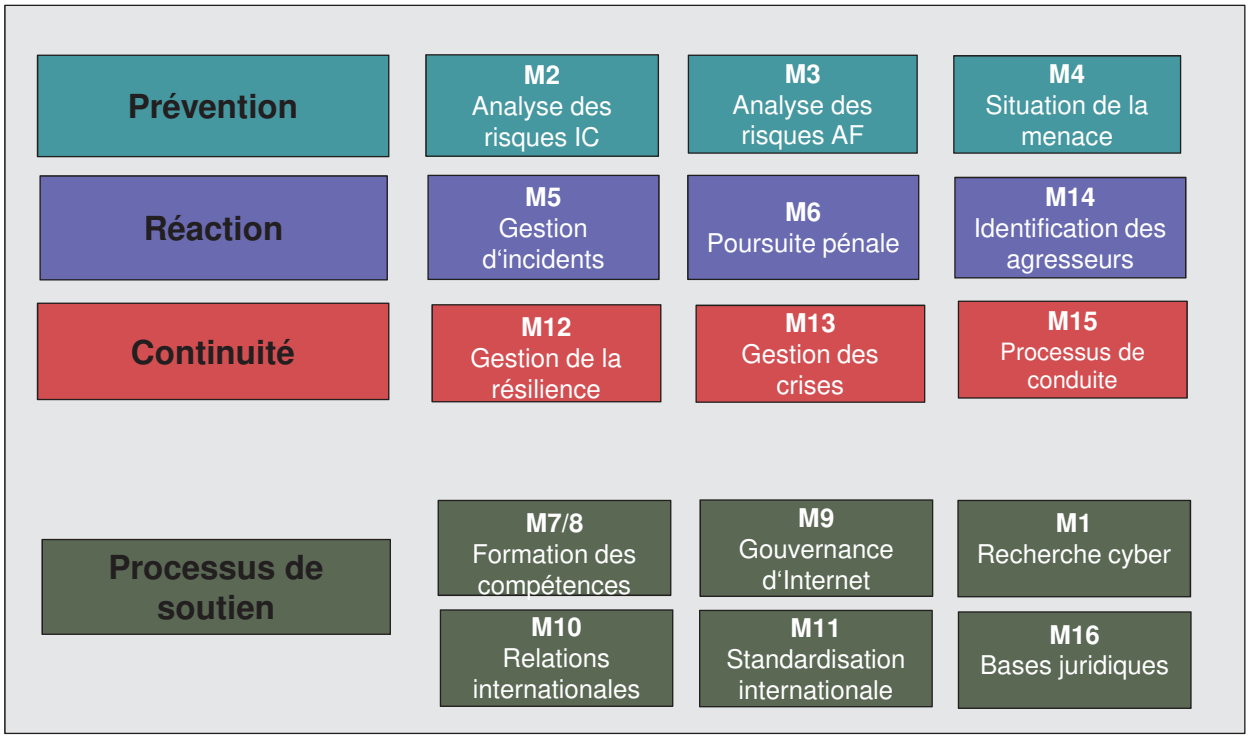
19.06.2012 (rev.)

Objectifs stratégiques

1. Détection précoce des menaces et des dangers dans le cyberespace
2. Augmentation de la capacité de résistance des infrastructures critiques
3. Réduction des cyberrisques

➔ **Mises en œuvre de 16 mesures jusqu'en 2017**

Les 16 mesures



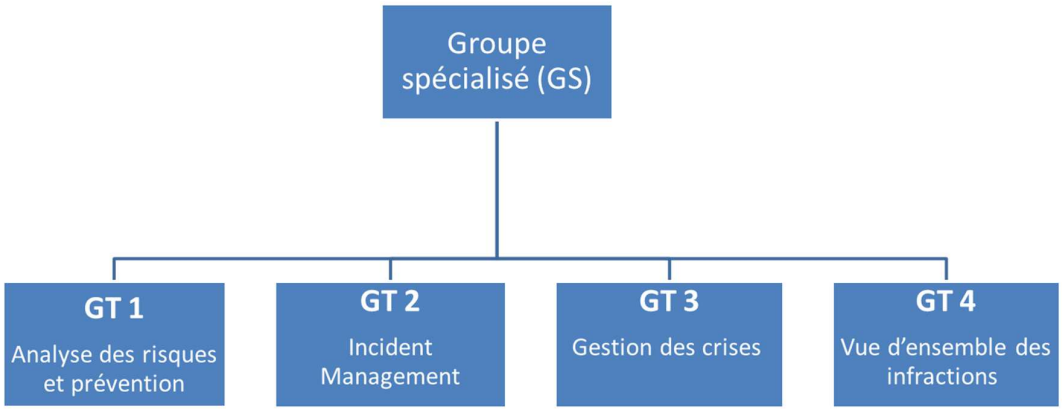
Principaux résultats de la SNPC (1/2)

- **Situation de la menace:** un radar de la situation est disponible pour les infrastructures critiques
- **Gestion des incidents:** les unités spécialisées (GovCERT, CSIRT-OFIT, milCERT) ont augmenté leurs ressources et leurs capacités. Des incidents ont pu effectivement être gérés sous la direction de MELANI.
- **Gestion des crises:** des exercices communs avec les cantons et les opérateurs des infrastructures critiques ont été organisés
- **Poursuite pénale:** un catalogue phénoménologique détaillé sur les différentes formes de cybercriminalité a été créé

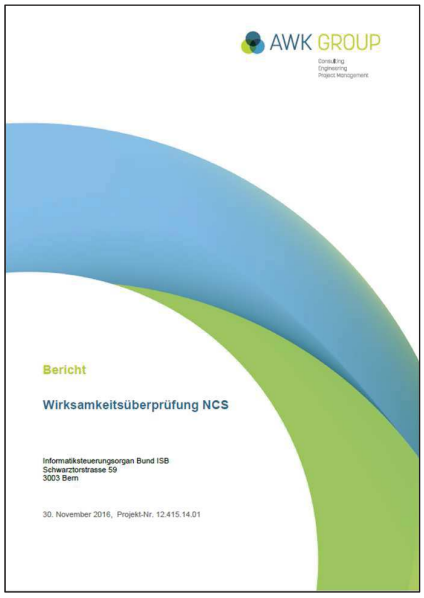
Principaux résultats de la SNPC (2/2)

- **Gestion de la résilience:** des analyses des risques et vulnérabilités ont été effectuées dans les 28 secteurs partiels critiques et des mesures d'amélioration de la résilience ont été élaborés (entre autres encouragement de l'échange d'informations, standardisation, plans d'urgence, formation)
- **Recherche et formation:** les thèmes de recherche les plus importants ont été identifiés en collaboration avec les hautes écoles; un nouveau profil professionnel «ICT Security Expert» a été créé (avec l'association ICT-Formation professionnelle)
- **Coopération internationale:** mesures de confiance de l'OSCE; collaboration avec le Cooperative Cyber Defense Centre of Excellence (OTAN), etc.

Interfaces avec les cantons: le réseau national de securité (RNS)



Évaluation de l'efficacité de la SNPC



- **Points forts:**
  - **Contenu:** les objectifs et les mesures ont été de manière générale judicieusement fixés
  - **Mise en œuvre:** les mesures ont été mises en œuvre conformément au calendrier prévu (l'impact des travaux reste toutefois encore difficile à mesurer)
  - **Structure:** La mise en œuvre décentralisée des mesures a fonctionné
- **Faiblesses:**
  - **Répartition peu claire des responsabilités:** il reste des questions ouvertes concernant les responsabilités (par ex. gestion des crises, rôle de l'armée)
  - **Manque de visibilité:** la SNPC est trop peu perçue par le domaine politique, l'économie et le public
  - **Accent mis sur la protection des infrastructures critiques:** Les cyberrisques concernent toute l'économie et la société

Prochaines étapes: arrêté du Conseil fédéral du 26 avril 2017

1. Prise de connaissance du rapport annuel SNPC 2016, du rapport relatif au contrôle de gestion stratégique de la SNPC au 31 décembre 2016 et du rapport concernant l'évaluation de l'efficacité de la SNPC
2. Attribution à l'UPIC d'un mandat d'élaboration d'une deuxième stratégie d'ici à fin 2017
3. Maintien des 30 postes destinés à la mise en œuvre de la SNPC

Développement de la stratégie

Ateliers
- 4 ateliers avec toutes les personnes de l'administration fédérale impliquées, ainsi que les représentants des cantons et des milieux économiques (de mai à septembre)

Consul-tations
- Consultations (informelles) des associations économiques et des cantons* (d'août à septembre)

Proposition au Conseil fédéral
- Présentation de la stratégie et de son plan de mise en œuvre au Conseil fédéral (décembre 2017)*

*** Mise à jour: les cantons ont demandé une procédure de consultation officielle de trois mois. L'adoption de la SNPC ne pourra avoir lieu qu'au printemps 2018 au plus tôt (ACF en avril 2018)**

Objectifs stratégiques de la SNPC 2018-22

Version préliminaire
Novembre 2017

1) La Suisse dispose des **compétences, des connaissances et des capacités** nécessaires au repérage et à l'évaluation des cyberrisques.
2) La Suisse élabore des **mesures de prévention** efficaces.
3) La Suisse peut **gérer les incidents**, y compris ceux de longue durée et touchant différents secteurs.
4) Les infrastructures critiques sont **résilientes** face aux cyberrisques.
5) La protection de la Suisse contre les cyberrisques est assumée comme une **tâche commune** de la société, des milieux économiques et de l'État.
6) La Suisse s'engage en faveur de **la coopération internationale** pour accroître la cybersécurité.
7) La Suisse **tire des leçons des cyberincidents** survenus en Suisse et à l'étranger.

10 champs d'action de la SNPC 2018-22

Version préliminaire Novembre 2017

- Développement de compétences et de connaissances
- Situation de la menace
- Gestion de la résilience
- Standardisation et réglementation
- Gestion des incidents
- Gestion des crises
- Poursuite pénale
- Cyberdéfense
- Politique internationale de cybersécurité
- Visibilité et sensibilisation

➔ 28 mesures concrètes dans ces dix champs d'action

Principales nouveautés dans le contenu

Version préliminaire Novembre 2017

- **Élargissement du groupe cible:** les PME et la population doivent être prises en compte. MELANI développe des produits pour ces groupes cibles.
- **Standardisation**: des standards minimaux pour la sécurité TIC seront évalués et introduits dans les secteurs critiques.
- **Examen d'une obligation de notification:** une obligation de notifier les cyberincidents est examinée en collaboration avec les autorités compétentes.
- **Integration de la cyberdéfense dans la SNPC:** les travaux du DDPS dans le domaine du cyberdéfense font partie intégrante de la SNPC.

Organisation et plan de mise en œuvre (en cours de traitement)

- La stratégie est completée par un plan de mise en œuvre qui contient les éléments suivants :
  - **Structure organisationelle de la SNPC**: qui assume la responsabilité stratégique, qui assume les tâches de coordination, qui est en charge du contrôle stratégique?
  - **Responsabilité pour les mesures:** quelle unité administrative met en œuvre quelle mesure?
  - **Objectifs de performance:** quelles prestations doivent être fournies jusque à quelle date?

- La politique demande une centralisation des activités concernant la protection contre les cyberrisques (Motion Eder 17.3508, adoptée au Conseil des États)

Renseignements / Contact

Organe de coordination de la SNPC
Manuel Suter
Unité de pilotage informatique de la Confédération (UPIC)
Schwarztorstrasse 59
3003 Bern

manuel.suter@isb.admin.ch
+41 58 461 43 20