Recherche rapide
Chercher
Recherche avancée

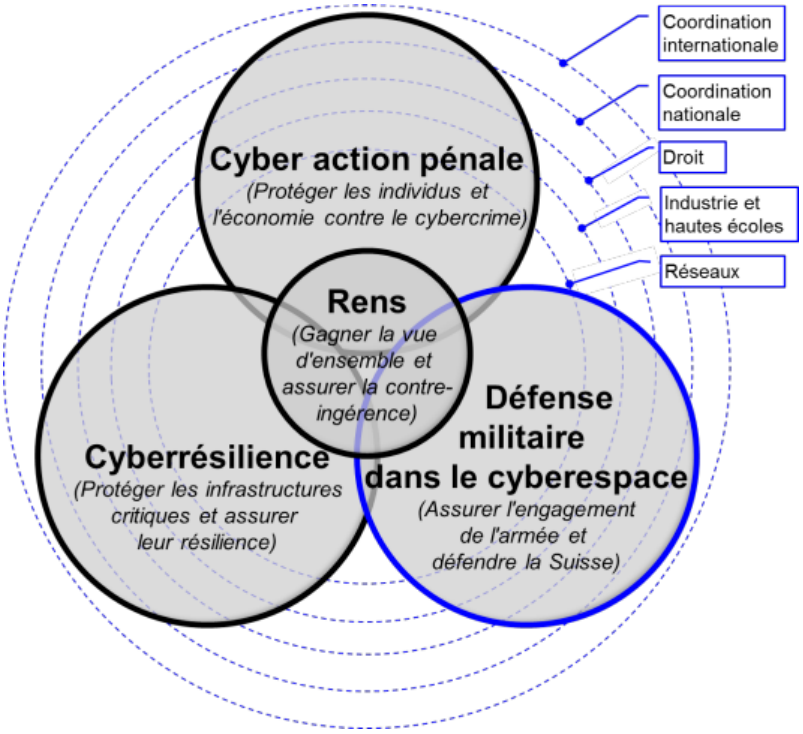
- Les tâches de l'armée
- Affaires sanitaires
- Aide militaire en cas de catastrophe
- Amiante dans des cantonnements de la troupe
- Avis de tirs
- Cyber Defence
  - Historique
  - Dispositif national
  - Cybermenaces
  - Analyse par l'armée
  - Conséquences pour l'armée
  - Rôle de l'armée
  - Dimensionnement
  - Perspectives
- Déminage et élimination de munitions non explosées
- Engagements et opérations
- Immobilier
- Lutte contre l'extrémisme au sein de l'armée
- Ouvrages minés de l'Armée suisse
- Prévention des accidents et des dommages militaires (PADM)
- Métiers militaires
- Musique militaire
- Police militaire
- Relations internationales
- PLAN GÉNÉRAL Développement des forces armées et de l'entreprise
- Promotion de la paix
- Programmes d'armement
- Engagements subsidiaires de sûreté de l'armée
- Unités spéciales de l'armée
- Economie et armée
- Office central du matériel historique de l' armee (OCMHA)

Page d'accueil > Thèmes > Cyber Defence > **Dispositif national**

Imprimer cette page

Dispositif national actuel

Un dispositif global pour la Suisse, pouvant être considéré comme fonctionnel et assez complet, bien que manquant encore de maturité, s'est développé sur la base des efforts consentis ces dernières années.



Le dispositif suisse de cyberdéfense

Sans prétendre donner une image complète de la situation, l'illustration ci-dessus présente un condensé du dispositif actuel.

La fonction « cybersécurité » est assumée par l'UPIC ; cet organe, directement subordonné au DFF, fournit la plupart de ses prestations par le truchement de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), le tout s'effectuant, entre autres, en étroite collaboration avec l'Office fédéral de l'approvisionnement économique du pays (OFAE) et l'Office fédéral de la protection de la population (OFPP), lequel est compétent pour appliquer la stratégie de protection des infrastructures critiques (PIC). A ce sujet, la SNPC constitue la base de référence.

La fonction « lutte contre la cybercriminalité » est assurée par la fedpol, au DFJP, en collaboration avec les forces cantonales de police ; quant à la conception et à la coordination, elle est assumée par la Police judiciaire fédérale (PJF), avec le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) comme élément de base.

La fonction « service de renseignement » est une tâche incombant au Service de renseignement de la Confédération (SRC), assumée en étroite collaboration avec d'autres services (dont le Renseignement militaire, RM). L'armée appuie cette fonction dans le domaine technique / analytique en tirant profit des synergies existantes.

La fonction « cyberdéfense » est assurée par le domaine Défense, au DDPS. Ses moyens sont principalement engagés dans la protection de ses propres systèmes TIC et infrastructures, de même que pour garantir la capacité de l'armée à agir, quelle que soit la situation. Le Conseil fédéral, dans sa décision du 15 mai 2013 préalablement mentionnée, attend aussi de l'armée qu'elle assume, à titre subsidiaire, un rôle important en cas de conflit/guerre. Des précisions quant à ce rôle et aux ressources dont l'armée devra disposer dans l'accomplissement de cette tâche devront encore être données, notamment dans le cadre du prochain rapport sur la politique de sécurité.

En tant qu'autres parties constitutives de ce dispositif, les éléments ci-après doivent être pris en compte :

Coordination : selon la SNPC, l'UPIC est chargée de la coordination générale. Dans le cadre de l'application de la SNPC, la collaboration entre la Confédération et les cantons est dirigée par le Réseau national de sécurité (RNS) ; quant au DFAE, il assure la coordination à l'échelon international.

Affaires juridiques : des efforts ont été consentis par les instances impliquées dans la procédure pour établir un cadre juridique solide, pour harmoniser et accroître l'efficacité des bases juridiques et, de ce fait, pour combler les lacunes existantes.

Industrie et hautes écoles : la Suisse dispose de compétences et de capacités excellentes, tant sur le plan quantitatif que sur le plan qualitatif. L'objectif est de recourir avec souplesse à ces compétences dans le traitement des cyberrisques, quel que soit le cas de figure.

Réseaux des organisations de milice : le réseau particulièrement dense établi avec les organisations de milice représente un instrument unique au monde. De nombreux domaines de la société peuvent donc mieux percevoir la cyberthématique.

Le dispositif décrit ici n'en est qu'à son élaboration et il reste encore beaucoup à faire au niveau de l'harmonisation opérationnelle et de l'interopérabilité.

Pour des questions concernant cette page: Communication Défense

---
