Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Etat en février 2023 *)

Stratégies nationales protection des infrastructures critiques PIC / Cyber SNPC

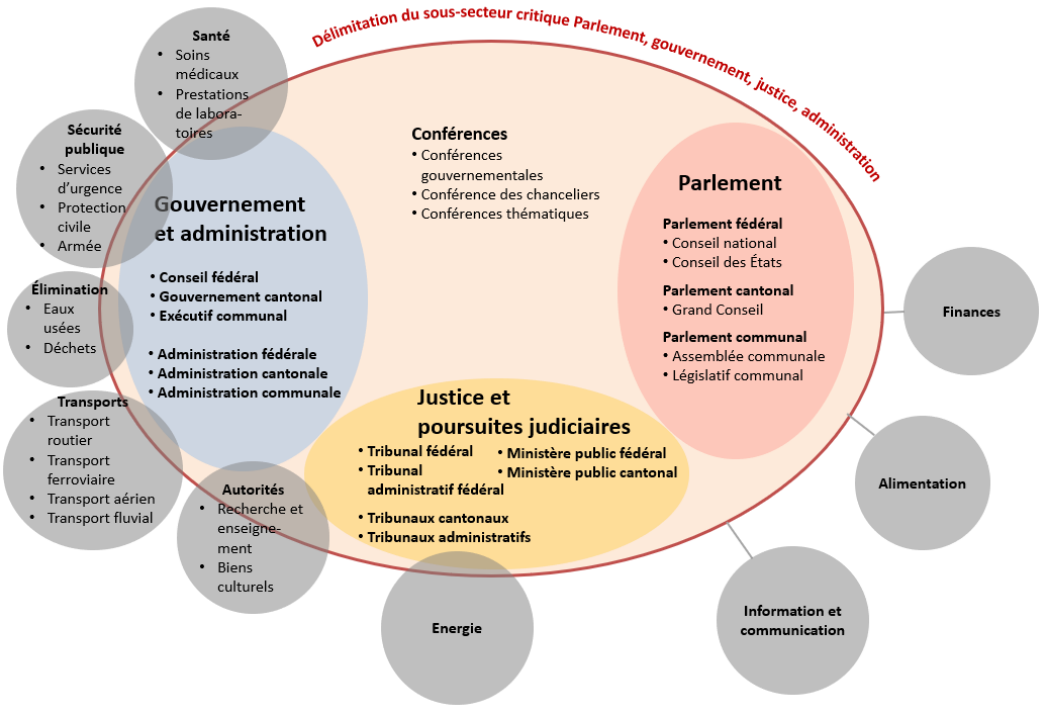
Fiche info sur le sous-secteur critique Parlement, gouvernement, justice, administration

Description générale et prestations

Le sous-secteur Parlement, gouvernement, justice, administration fournit un grand nombre de services importants à la population et à l'économie. Ces services comprennent la législation, la jurisprudence et leur application, ainsi que les prestations administratives de l'État, comme l'octroi d'autorisations et leur contrôle. Pour la plupart de ces services, des perturbations ou des pannes de courte durée, de quelques heures à quelques jours, n'entraîneraient pas de graves dommages pour la population et l'économie.

Les processus pour lesquels le facteur temps est critique sont surtout ceux qui concernent le dédouanement des échanges commerciaux, la gestion de répertoires et de registres fréquemment utilisés (bases de données de la police, registres fonciers, registres électoraux, etc.) et la protection de la population en cas de danger (information, alerte, alarme).

Les autorités fournissent également des services importants aux autres secteurs critiques. Les tâches qui touchent directement d'autres sous-secteurs, par exemple les activités de surveillance des barrages dans le sous-secteur de l'électricité, sont analysées dans les fiches les concernant.



Analyse du marché / structure du système

Le sous-secteur Parlement, gouvernement, justice, administration a une structure décentralisée avec les sous-domaines Exécutif, Législatif et Judiciaire ainsi que les trois niveaux Confédération, cantons et communes. Au sein de ces domaines, le sous-secteur se compose d'acteurs individuels d'importance systémique qui assument des tâches spécifiques dans leur champ de compétences. Ces acteurs ne peuvent se soutenir mutuellement que de manière restreinte. Les conséquences des défaillances sont toutefois limitées dans l'espace et, comme de nombreuses tâches peuvent être déplacées dans le temps, elles ne sont généralement pas critiques de ce point de vue.

*) Le contenu de cette fiche se base sur l'analyse des risques et des vulnérabilités de l'OFPP de 2018.

Processus étudiés

Dans le cadre de l'analyse des risques et des vulnérabilités, 13 processus ont été examinés de plus près, soit parce qu'ils sont importants pour le bon fonctionnement des autorités, soit parce qu'ils ont déjà une importance majeure à court terme pour la population et l'économie :

Parlement (pouvoir législatif)	**Gouvernement et administration (pouvoir exécutif)**	**Justice (pouvoir législatif)**
Processus clés	***Processus clés***	***Processus clés***
– Adoption de lois – Prise de décision parlementaire	– Services administratifs généraux – Missions de maintien de la sécurité intérieure – Gestion de répertoires et de registres – Protection de la population, de l'économie et de l'environnement – Garantie des droits politiques – Dédouanement	– Jurisprudence – Poursuites judiciaires
Processus de soutien	***Processus de soutien***	***Processus de soutien***
– Prestations des Services du Parlement	– Entretien des infrastructures, y compris les systèmes informatiques	– Prestations des services judiciaires

Dangers pertinents pour le sous-secteur critique


Cyberattaque


Panne d'électricité


Panne informatique


Attentat conventionnel

Remarque : Les risques examinés concernent l'ensemble du sous-secteur. D'autres risques peuvent être pertinents pour certains ouvrages d'infrastructures critiques.

Risques et vulnérabilités

Les plus grandes vulnérabilités des processus étudiés se situent au niveau des systèmes informatiques utilisés en commun par la Confédération, les cantons et les communes, qui dépendent beaucoup du fonctionnement des réseaux de télécommunication publics et de leur propre approvisionnement en électricité. Dans le cadre de l'analyse des risques, différents scénarios ont été examinés, tels que les cyberattaques contre les systèmes informatiques des autorités (p. ex. bases de données et registres), une panne d'électricité suprarégionale, la défaillance d'un fournisseur central de services informatiques et un attentat contre une installation importante.

L'analyse montre que de tels événements peuvent causer des dommages économiques et sociaux directs, par exemple en empêchant l'accomplissement d'un grand nombre de tâches faute d'extraits de registre. Les dommages indirects consécutifs à de tels événements peuvent également être graves. Des défaillances prolongées de systèmes ou d'installations des autorités peuvent entraîner une perte de confiance de la population et nuire à la réputation de la Suisse (avec des conséquences pour la place économique et le tourisme).

Le sous-secteur Parlement, gouvernement, justice, administration peut être considéré dans son ensemble comme relativement résilient. Divers projets et programmes dans le domaine de la résilience de l'alimentation électrique et des services informatiques sont actuellement en cours de planification ou de mise en œuvre et contribueront à renforcer encore cette résilience. Le réseau de centres de calcul ou le réseau de données sécurisé (RDS) en sont des exemples. Il faut toutefois s'attendre à ce que la résilience actuelle du sous-secteur diminue en raison de la poursuite de l'interconnexion des systèmes informatiques si on ne prend pas de mesures d'accompagnement.

Mesures de résilience

Amélioration de l'échange d'informations

- Intensifier la coopération entre tous les niveaux (fédéral, cantonal, communal) dans le domaine des cyberrisques et de la dépendance aux services informatiques.

Communication en cas d'événement

- Examiner les redondances dans le domaine de la communication avec les représentations suisses à l'étranger.
- Vérifier l'information et la communication pendant les événements.
- Examiner l'utilisation ou une connexion au réseau de données sécurisé (RDS).

Interdépendances du sous-secteur Parlement, gouvernement, justice, administration

Pour de plus amples informations sur la PIC et la SNPC, consultez les sites :

www.infraprotection.ch

www.ncsc.admin.ch