canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal

1014 Lausanne

Madame la Cheffe du Département
fédéral de la défense, de la protection de
la population et des sports
Viola Amherd
Palais fédéral Est
3003 Berne
Par courriel :
patrick.gansner@gs-vbs.admin.ch

Lausanne, le 7 juillet 2021

Consultation fédérale relative au Rapport sur la politique de sécurité

Madame la Conseillère fédérale,

Le Conseil d'Etat vaudois tient à vous remercier de l'avoir consulté sur le Rapport sur la politique de sécurité.

Remarques générales

Le Conseil d'Etat a pris acte du contenu du rapport, tout en formulant les remarques suivantes.

Le Conseil d'Etat considère que le rapport manque en partie sa cible en raison de la faible concrétisation et priorisation des mesures : Alors que, selon la lettre d'accompagnement, ce rapport est censé donner « *des objectifs et des priorités claires pour la politique de sécurité de la Suisse dans les années à venir, ainsi que des mesures concrètes pour leur mise en œuvre* », il indique plutôt les grandes lignes et orientations, sans priorisation ni concrétisation des objectifs.

La première partie du rapport qui décrit la situation actuelle est très étendue, contrairement aux mesures de mise en œuvre qui ne sont pas assez développées. Or ce sont justement ces dernières qui intéressent les responsables fédéraux et cantonaux. Pour éviter que les mesures ne se limitent à des déclarations d'intention, le Conseil d'Etat demande que les projets soient priorisés, qu'ils soient plus détaillés avec notamment un calendrier quant à leur concrétisation.

Il formule ainsi plusieurs observations et propositions d'améliorations

De manière générale, le Conseil d'Etat soutient la position de la CG MPS.

Remarques particulières

Chapitre 2 – Situation actuelle
Progrès technologique (2.1.3)

Les menaces que peuvent représenter les développements de l'intelligence artificielle doivent faire l'objet d'une attention particulière, tant du point de vue de la sécurité que de son impact sur la libre formation de l'opinion. La question des données numériques et de leur traitement dans ce contexte est centrale, puisque les algorithmes d'intelligence artificielle se basent sur des jeux de données dont la qualité est essentielle pour garantir une fiabilité de la technologie.

Espionnage et cybermenaces (2.3.1 - 2.3.7 – 2.3.8)

La notion de guerre économique est à prendre globalement en considération. L'espionnage des startups dans des domaines stratégiques nécessite une réelle prise de conscience et l'adoption de « gestes barrières numériques », c'est-à-dire des mesures de protection effective. Le volet des vulnérabilités et de la protection de notre système financier, y inclus celles de ses données sensibles, reste une priorité stratégique.

Par ailleurs, les cyber-attaques et les virus, en particulier de type rançongiciel, sont aujourd'hui une vraie menace pour le fonctionnement de l'Etat, Confédération, cantons et communes. Dans ce contexte, une collaboration opérationnelle renforcée est nécessaire.

Catastrophes et situations d'urgence (2.3.9)

Premièrement, nous proposons que le titre soit adapté comme suit « Catastrophes, situations d'urgence et situations sortant de l'ordinaire ». En effet, les scénarios d'événements ne doivent pas nécessairement être des catastrophes ou des situations d'urgence. En cas d'événement, les dangers naturels mentionnés peuvent menacer la population d'une région. Même s'il s'agit d'événements majeurs, ils ne doivent pas nécessairement avoir l'ampleur d'une situation d'urgence ou d'une catastrophe.

En outre, les dangers de nature technique doivent être complétés avec les accidents majeurs, puisque les explosions et les événements ABC (par exemple des émanations de chlore se produisant au sein d'entreprises ou sur des axes de transport), peuvent mettre en danger un grand nombre de personnes et constituent un risque significatif. De tels événements nécessitent l'intervention rapide de forces d'intervention, notamment des sapeurs-pompiers.
En pages 20 et 21 du rapport, il faut corriger une erreur de plume : *« Pour les dangers de nature technique, il est important de relever que ~~d'accroître~~ la dépendance de la société envers les infrastructures critiques (p. ex. l'approvisionnement en électricité, les voies de communication, la téléphonie mobile) augmente »*.

Il est également important de rappeler qu'en cas de rupture complète de l'approvisionnement ou de pénurie d'électricité, de nombreuses infrastructures vitales ne seraient plus en mesure de remplir correctement leur fonction que cela soit sur le plan sanitaire (hôpitaux, EMS, ambulances, pharmacies), de l'approvisionnement en eau et en nourriture ainsi que dans les domaines de la police, des sapeurs-pompiers et de la protection civile. Afin de limiter l'impact d'une telle catastrophe, il est nécessaire que les infrastructures vitales soient équipées de solutions de secours pour faire face à une telle éventualité.

Or, les dispositions en vigueur n'imposent aucune couverture minimale des besoins pour les infrastructures vitales et laissent une grande liberté aux exploitants de s'équiper ou non de solutions de secours. La solution de la location de génératrices est souvent évoquée. Toutefois en cas de crise, les génératrices disponibles et le carburant ne seraient pas suffisants pour couvrir la demande. Afin d'établir un cadre minimal, la Confédération doit fixer la préparation des infrastructures vitales dans ses priorités et fournir des recommandations contraignantes pour ces infrastructures en fonction des résultats de l'analyse des risques.

Migration et politique de sécurité (2.3.10)

La phrase « *La migration n'est en soi pas une menace importante pour la politique de sécurité de la Suisse, mais elle peut avoir des retombées significatives* » est mal traduite et peut porter à confusion. Dans la version allemande, il est indiqué que la migration « *n'est pas une menace en soi* » et en français « *pas une menace importante* ». Il convient donc de corriger la version française pour être fidèle à la version allemande.

Chapitre 4 - Mise en œuvre : domaines politiques et instruments de la politique de sécurité
Domaines politiques et instruments (4.1)

Dans l'énumération des instruments de la politique de sécurité, le domaine de la protection de la population appelle quelques commentaires, en plus de ceux formulés par la CG MPS :
la protection de la population, en tant que système coordonné, doit disposer de plus de ressources et faire l'objet de réels efforts de développement. L'Office fédéral de la protection de la population (OFPP) doit disposer de moyens pour accompagner et soutenir les cantons dans la préparation et la gestion de divers scenarii.

Libre formation des opinions (4.2.4)

Selon le rapport, plusieurs éléments indiquent que la Suisse et sa population sont relativement robustes face à des tentatives d'influence et de désinformation et notamment « *qu'une bonne éducation scolaire favorise grandement les compétences médiatiques et politiques* ». Avec la numérisation croissante de la société et en particulier l'utilisation des réseaux sociaux, et également avec la remise en question des médias traditionnels l'acquisition de connaissances et de compétences pour évaluer la qualité de l'information est centrale. Dans ce sens, la formation des enfants et des jeunes joue un rôle important.

Ainsi, le système de formation mériterait d'être intégré aux réflexions de la politique de sécurité. L'éducation numérique, telle que nouvellement intégrée dans les plans d'études romand et alémanique, permettra de former davantage les jeunes à l'utilisation des technologies, outils numériques et médias sociaux. C'est un élément fort du dispositif de prévention et un investissement certain sur le moyen et long terme permettant de limiter les dérives qui peuvent conduire à des brèches sécuritaires.

Par ailleurs, les deux mesures visant à évaluer les activités d'influence qui pourraient menacer la libre formation des opinions semblent manquer de consistance. La Confédération devrait identifier des moyens de prévention de la diffusion de fausses informations et ne pas prévoir seulement une réaction lorsque des activités d'influence surviennent, telles que les deux mesures citées dans le rapport. A cet égard, on peut citer le projet élaboré par la Commission européenne, le Digital Services Act, dont le but est notamment de mettre en place un cadre solide pour la transparence des plateformes en ligne et clair en ce qui concerne leur responsabilité. Il vise à encourager les plateformes à lutter contre la prolifération de fausses informations.

Accroître la protection contre les cybermenaces (4.2.5)

De manière générale, les capacités dans ce domaine devraient être augmentées, puisque les cybermenaces font aujourd'hui partie des principaux risques pour la Suisse. Il en va de même de la coopération entre les différentes entités, publiques ou privées, en charge de la cybersécurité.

Un accent devrait également être mis sur des incitations pour les infrastructures critiques à améliorer leur sécurité informatique et leur résilience face aux cyber-attaques. Comme l'ont montré des exemples récents, des mesures doivent être prises pour mieux assurer la protection et la disponibilité des données. L'obligation d'annoncer les cyber-incidents va ainsi dans la bonne direction.

Une réflexion devrait également être menée concernant les objets connectés, dont leur nombre est appelé à augmenter. Selon le rapport en réponse aux postulats Glättli 17.4295 et Reynard 19.3199, « *on constate à la fois une absence de demande commercialement intéressante d'appareils connectés sûrs et une offre insuffisante de ces derniers. (...) Il est peu probable que le marché commence d'exercer une pression suffisamment marquée en faveur d'une amélioration de la sécurité de ces appareils* ». Le risque de voir les objets connectés mal sécurisés devenir les portes d'entrée d'attaques informatiques plus vastes est ainsi en augmentation et il conviendrait de prendre des mesures coordonnées pour y faire face.

Prévenir le terrorisme, l'extrémisme violent, le crime organisé et les autres formes de criminalité transnationale (4.2.6)

Les dispositifs de collaboration entre les différentes autorités pour la prise en charge des jeunes radicalisés devraient être maintenus voire renforcés dans la prévention de la rupture (scolaire, sociale et professionnelle).

Renforcer la résilience et la sécurité d'approvisionnement en cas de crises internationales (4.2.7)

La crise du COVID a montré les risques de la dépendance de la Suisse à des biens stratégiques produits à l'étranger lorsque des goulets d'étranglement se sont créés. Cet aspect devrait être corrigé pour 'l'éthanol puisque les réserves devraient être reconstituées (ordonnance sur le stockage obligatoire d'éthanol). Toutefois, pour d'autres produits nécessaires en cas de crise, la proposition faite dans le rapport de vérifier et réduire les dépendances au niveau de l'approvisionnement en biens et en prestations critiques et de première nécessité doit être soutenue. Il est important qu'il s'agisse d'une réflexion globale, pas uniquement centrée sur la pénurie de masques ou de gel désinfectant mais également d'identifier les secteurs économiques concernés et les moyens de relocaliser une partie de la production afin de réduire cette dépendance.

Améliorer la protection contre les catastrophes, la préparation aux situations d'urgence (4.2.8)

Il convient de rappeler que les dangers naturels ne relèvent pas de la seule politique sécuritaire, puisque leur prévention repose sur des politiques publiques transverses, comme les politiques environnementales notamment. Une coordination entre les différentes entités, que ce soit au niveau fédéral ou au niveau cantonal, est ainsi nécessaire pour bien appréhender ces risques.

La dernière phrase de l'avant-dernier paragraphe de la page 40, devrait être modifiée pour mieux englober la réalité : « *Ces mesures comprennent l'aménagement du territoire et des constructions ~~techniques~~ par exemple en établissant des cartes de dangers, des évaluations du risque et des déficits de protection et en construisant des structures de protection contre les crues* ».

La première phrase du dernier paragraphe de la page 40, devrait également être modifiée comme suit : « *L'Office fédéral de l'environnement soutient les cantons dans la planification et l'application de mesures de protection contre le ruissellement et les crues* ». En effet, consécutivement à l'augmentation de l'intensité des événements météorologiques due au dérèglement climatique, le ruissellement tend à devenir un phénomène de plus en plus problématique pour les forces d'intervention en cas de catastrophe d'origine naturelle comme à Lausanne en juin 2018.

Renforcer la collaboration entre les autorités et les acteurs de la gestion de crise (4.2.9)

Dans ce paragraphe, les organes cantonaux de conduite (OCC) ne sont pas mentionnés, alors qu'ils sont le principal instrument de conduite des cantons en cas de crise.

La crise du COVID a révélé certaines failles dans la coordination des acteurs de la gestion de crise, qui ont été notamment relevés par le rapport de la Chancellerie fédérale du 11 décembre 2020 sur la gestion de la première vague par la Confédération. La coopération et la collaboration entre organes de sécurité, cantonaux et fédéraux, devraient donc être améliorées et plus développées.

Conclusion

Le Conseil d'Etat prend acte du contenu du rapport et considère que le rapport manque en partie sa cible en raison de la faible concrétisation et priorisation des mesures.

De plus, en raison de changements intervenus depuis la rédaction du rapport, notamment la rupture des négociations sur l'accord-cadre avec l'Union européenne, il suggère de compléter l'analyse afin de prendre en compte les conséquences possibles en matière sécuritaire ou d'approvisionnement en énergie, notamment.

Le Conseil d'Etat vous prie de croire, Madame la Conseillère fédérale, à l'expression de sa haute considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Nuria Gorrite	Vincent Grandjean

Copie

· OAE