Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Conseil fédéral suisse

Projet, état : 14 avril 2021

La politique de sécurité de la Suisse

Rapport du Conseil fédéral

Table des matières

1 Introduction

Le Conseil fédéral publie périodiquement des rapports sur la politique de sécurité de la Suisse. Sur la base d'une analyse détaillée du contexte, les rapports servent à vérifier si et dans quelle mesure cette politique et ses instruments doivent être adaptés afin de réagir rapidement et correctement aux nouvelles formes de menaces et dangers, de décider de la stratégie à suivre et de déterminer les priorités. Le dernier rapport date du 24 août 2016.

La situation internationale, où règne l'incertitude, évolue à un rythme soutenu. C'est également le cas pour la politique de sécurité de notre pays et pour les menaces et dangers auxquels il est confronté. Bien que ces derniers n'aient pas fondamentalement changé ces dernières années, ils se sont toutefois développés, voire renforcés. La manière de gérer la politique de sécurité internationale est devenue plus difficile et la défense des intérêts de pouvoir encore plus marquée. La dégradation de la collaboration multilatérale et des structures de sécurité internationales s'est intensifiée, tout comme le recours à des moyens de gestion des conflits dits *hybrides*. La digitalisation et l'interconnexion de plus en plus rapides ont de nombreux avantages, mais ont également accru la vulnérabilité de l'État, de l'économie et de la société. Les conflits armés et les crises à la périphérie de l'Europe non seulement persistent, mais se sont en partie aggravés. Les événements extrêmes liés aux conditions météorologiques se multiplient avec le changement climatique, et les dangers dus aux pandémies se sont radicalement confirmés avec la pandémie de COVID-19.

Le présent rapport analyse ces évolutions et explique ce qu'elles représentent pour la politique de sécurité de la Suisse. Il expose les principes de cette politique, ses intérêts et objectifs, et démontre comment ses instruments contribuent à la réalisation de ces derniers et dans quel sens ils doivent être utilisés.

La politique de sécurité est une tâche commune en Suisse. C'est pourquoi, comme pour les rapports précédents, les cantons ont été sollicités pour la préparation de ce rapport. Cela démontre à quel point cette politique est globalement et largement comprise dans notre pays. Elle englobe la totalité des mesures de la Confédération, des cantons et des communes destinées à protéger la Suisse et sa population des menaces et dangers politiques, criminels, naturels et anthropiques. Ses objectifs sont de protéger la capacité d'action, l'autodétermination et l'intégrité de la Suisse et de sa population ainsi que ses conditions d'existence contre les menaces et les dangers, et de contribuer à la stabilité et à la paix en dehors des frontières.

Le rapport détermine aussi l'orientation et les principes fondamentaux de la politique de sécurité de la Suisse pour les années à venir. Il sert de base pour d'autres documents de référence plus détaillés concernant les différents domaines ou instruments de cette politique.

Il est coordonné avec le message sur le programme de la législature 2019 à 2023 du 29 janvier 2020, où il figure comme mesure de mise en œuvre de l'objectif 15 : « La Suisse connaît les menaces qui pèsent sur sa sécurité et dispose des instruments nécessaires pour y parer efficacement ». Il est prévu qu'un tel rapport soit publié à chaque législature.

2 Situation actuelle

2.1 Tendances générales

La sécurité de la Suisse est surtout influencée par les tendances suivantes : la concurrence accrue des grandes puissances, une mondialisation avec des tendances, en partie contradictoires, à la régionalisation et à la nationalisation, le progrès technologique et la polarisation sociale. La politique internationale en matière de sécurité est marquée par des rivalités de pouvoir. La mondialisation se poursuit, bien que certains États essaient de limiter, voire de réduire, leur propre implication.

2.1.1 Concurrence accrue des grandes puissances

La politique internationale en matière de sécurité est aujourd'hui marquée par une concurrence accrue des grandes puissances et des puissances régionales émergentes. Les rivalités de pouvoir le prouvent tout particulièrement. Ainsi, la Chine, les États-Unis, la Russie ainsi qu'une série de puissances régionales ont de plus en plus recours à des moyens de pression afin d'imposer leurs exigences : influence politique, économique ou militaire, propres normes juridiques et de comportement, contrôle des infrastructures, des technologies, des ressources et des voies de transport, et parfois utilisation d'outils d'information.

La raison principale de cette évolution tient au le fait que les États-Unis n'ont, ces dernières années, assumé que très sélectivement leur leadership. La Chine et la Russie en profitent notamment pour accroître leur influence. Cependant, ni l'une ni l'autre ne dispose jusqu'à présent des capacités militaires ou économiques suffisantes, et encore moins de la puissance dite douce, pour marquer profondément et durablement le monde, comme l'ont fait les États-Unis après la Seconde Guerre mondiale. L'Union européenne en a le potentiel, mais la mesure dans laquelle elle serait capable de l'exploiter demeure incertaine.

D'autre part, la capacité d'action d'organisations internationales de sécurité telles que l'ONU et l'OSCE, qui dépendent de la volonté de leurs États membres, en particulier des grandes puissances, baisse. Cela prouve qu'il n'existe aucun consensus entre les grandes puissances sur la manière dont la collaboration mondiale devrait être structurée et ce qu'elle devrait engendrer. Ces développements favorisent les rivalités de pouvoir appuyées par des sanctions unilatérales et des moyens diplomatiques et militaires, augmentant ainsi l'instabilité, les tensions et le risque de conflits armés.

La fin de la guerre froide a mis un terme à la bipolarité dans la politique internationale de sécurité. La période de dominance des États-Unis qui a suivi semble également toucher à sa fin. La question peut se poser de savoir si, dans un futur proche, une nouvelle structure stable prendra forme, par exemple un ordre bipolaire entre les États-Unis et la Chine ou un ordre multipolaire.

2.1.2 Mondialisation et régionalisation

D'un point de vue global, si les imbrications économiques, technologiques, politiques et sociales gagnent en importance, des contre-tendances s'imposent aussi : dans bien des régions, le nationalisme et les réflexes protectionnistes ont pris de l'ampleur. Dans

certaines sociétés industrielles, le scepticisme vis-à-vis de la mondialisation grandit. Le fait qu'aucune grande puissance ne domine mondialement encourage les politiques régionales.

La tendance à la régionalisation touche aussi l'économie mondiale. Les expériences faites avec la pandémie de COVID-19 pourraient las renforcer. La pandémie a certes clarifié la définition de la coopération internationale, mais a également illustré les risques liés aux chaînes mondiales de valeur et d'approvisionnement : des dépendances qui intéressent aussi la politique de sécurité, par exemple sur le plan de l'approvisionnement économique. Les pénuries d'approvisionnement de matériel de protection médicale et de produits pharmaceutiques au début de la pandémie de COVID-19 en sont une illustration. Les bouleversements dans la production industrielle dus à la digitalisation et à l'automatisation pourraient également favoriser la régionalisation, par exemple par une délocalisation des usines provenant des pays à bas salaires. De même , le passage des énergies fossiles à celles renouvelables devrait engendrer des systèmes d'approvisionnement plus spécifiques aux régions.

Le renforcement durable des acteurs non étatiques se démarque sur le plan de la politique de sécurité. Il s'agit notamment d'entreprises commerciales et d'organisations non gouvernementales, mais également d'organisations terroristes. Les mouvements transfrontaliers ont également un impact politique ou économique. La mondialisation, la grande vitesse d'organisation et de coordination ainsi que leur résilience sont des caractéristiques communes. Certaines grandes entreprises actives dans le secteur des technologies disposent, dans divers domaines, pratiquement d'une fonction régulatrice qui rivalise avec une influence étatique ou internationale. Les intérêts économiques de ces entreprises s'opposent en partie à ceux de la politique de sécurité des États, ce qui peut, en temps de crise, limiter la capacité d'action de ces derniers à ce niveau.

Même si les acteurs non étatiques ont gagné en pouvoir, les États continuent de jouer un rôle central dans la sauvegarde des intérêts politiques, normatifs ou économiques. La lutte contre la pandémie de COVID-19 a également souligné l'importance de l'État dans beaucoup de pays. Il est possible que les chaînes de production soient plus fortement ancrées dans certaines régions afin d'atteindre une plus grande fiabilité. Les (groupes d')États pourraient aussi se détourner des fora économiques mondiaux, ce qui ébranlerait les normes internationales établies. Une véritable rupture avec la mondialisation semble néanmoins peu probable, d'autant qu'elle aurait de lourdes conséquences sur le plan financier et ne pourrait être mise en œuvre rapidement.

2.1.3 Progrès technologique

Les nouvelles technologies se développent toujours plus rapidement et sont utilisées plus largement. La digitalisation et les progrès dans le domaine des capteurs conduisent à de meilleures et plus nombreuses données. Les technologies de communication modernes permettent l'échange de quantités de données sans cesse croissantes, qui sont saisies, connectées et rendues disponibles à l'aide d'ordinateurs et d'algorithmes performants. L'utilisation et l'évaluation de ces données sont un avantage concurrentiel, mais renferment un potentiel d'abus. Au cours de la digitalisation, les logiciels prennent de plus en plus souvent le contrôle des processus manuels actuels, également de ceux ayant des effets physiques.

L'apprentissage automatique et l'informatisation, qu'on appelle l'intelligence artificielle, vont également progresser dans les années à venir. Ainsi, les systèmes fonctionnent progressivement de manière autonome et les machines peuvent prendre des décisions sans influence humaine directe, dans lesquelles il sera de plus en plus difficile de suivre totalement le processus décisionnel. Les décisions automatisées concernent aussi de plus en plus des processus critiques. Cette délégation de décisions soulève des questions politiques, juridiques et éthiques, en particulier concernant les conflits armés.

Les États peuvent devenir dépendants d'acteurs, leaders dans le développement de ces technologies. Fondamentalement, un échange des technologies de l'information et des communications aussi ouvert que possible est bénéfique, car cela renforce la liberté de choix et la sécurité. Cependant, l'échange ouvert peut être limité ou empêché pour des raisons de politique de sécurité ou de pouvoir, par exemple pour protéger ses propres infrastructures, la recherche et le développement, ou pour refuser aux concurrents l'accès aux marchés. D'où l'émergence de chaînes de technologies et de fabricants dont les produits et systèmes sont incompatibles avec toutes les autres chaînes, ce qui pourrait au final briser l'élan technologique, voire obliger les États à opter pour une chaîne plutôt que pour une autre. Dans tous les cas, il faut s'attendre à une restriction de la liberté d'action lors du choix et de l'acquisition de nouvelles technologies, comme le montre déjà les chicaneries autour de l'utilisation des produits chinois par les États occidentaux.

2.1.4 Polarisation sociale

Le changement constant des comportements individuels et collectifs influe également sur la politique de sécurité. L'une des principales caractéristiques de ce changement est le renforcement de *l'identité* en tant que noyau des mouvements politiques. Ce phénomène, également connu sous le nom de *politique d'identité*, met en exergue les caractéristiques telles que le sexe, l'ethnie, la langue, l'origine ou l'orientation politique. L'identité est perçue comme transfrontalière et comme un choix individuel. Ce développement favorise la fragmentation et la polarisation sociales : pendant que certains groupes approuvent le développement de l'ouverture sociale et de la diversité et réclament l'égalité pour eux-mêmes ou d'autres groupes, d'autres prônent l'isolationnisme et s'agitent contre des groupes de population présentant certaines caractéristiques. Ces groupes sont de plus en plus irréconciliables. Le risque de radicalisation politique et d'extrémisme violent est associé à la fragmentation et à la polarisation.

Les médias sociaux et les moteurs de recherche marquent aujourd'hui de plus en plus le paysage de l'information. Généralement, ils sont créés comme plateformes pour l'échange de contenu et ne bénéficient en grande partie d'aucun suivi rédactionnel. En outre, la sélection algorithmique personnalisée de contenu peut conduire les utilisateurs d'internet à être exposés presque uniquement aux informations qui correspondent à leur configuration existante. Cela favorise la création de ce qu'on appelle les *bulles de filtres*. Le comportement de sélection des utilisateurs peut également faciliter la formation de *chambres d'écho* dans lesquelles des personnes ayant le même avis interagissent et, avec le temps, se radicalisent. Cependant, l'effet réel des deux mécanismes est plus minime que ce que l'on suppose parfois : la grande majorité des personnes se tourne encore vers des moyens traditionnels comme source d'information et est intégrée dans les médias sociaux avec des avis diversifiés. Reste que des chambres d'échos peuvent tout à fait naître en marge de la politique.

2.1.5 Développement du modèle de conflit

La manière dont les conflits sont traités est en train de changer. Le modèle de conflit actuel reflète les développements politiques, technologiques et sociaux de ces dernières années.

La propension à la violence dans les relations internationales reste élevée à l'échelle mondiale. Les États qui défendent ou veulent changer les rapports de force existants en usant de violence agissent plus qu'autrefois dans la zone grise entre le conflit armé et la paix. Ils effacent intentionnellement les frontières entre les acteurs étatiques et non étatiques, par exemple en engageant des entreprises spécialisées dans le mercenariat plutôt que leurs forces armées ordinaires. Cette méthode vise à mener des actions sous couverture et à pouvoir en nier la qualité d'auteur, bien que souvent avec peu de crédibilité. Ainsi, les coûts politiques, économiques et sociaux liés à un conflit ouvert devraient être évités et les réactions répressives déterminées, rendues difficiles. C'est pourquoi les conflits actuels suivent de moins en moins un processus d'escalade classique. Ils se caractérisent par le fait que les moyens politiques, économiques, militaires, informationnels, criminels et de renseignement sont orchestrés en tenant compte des armes et technologies modernes, en particulier dans le domaine de l'information et du cyberespace, et sont utilisés secrètement aussi longtemps que possible en dessous du seuil d'un conflit armé.

Ce type de gestion des conflits, dits hybrides, vise initialement la stabilité politique, économique et sociale de la société et de l'État, ainsi que la capacité d'action de ce dernier. Il se caractérise par la complexité et l'imprévisibilité, et cible en premier lieu la population afin de gagner sa sympathie et d'affaiblir la cohésion sociale. Les personnes, les groupes et également les États peuvent être directement atteints par des informations ciblées ou à grande échelle, par exemple via les médias sociaux. La désinformation (informations trompeuses ou entièrement inventées) est utilisée pour influencer ou saboter des processus politiques, attaquer la crédibilité des institutions et des médias ou tout simplement pour semer le doute sur la fiabilité des informations. L'utilisation de moyens cybernétiques et d'information à des fins politiques est aujourd'hui usuelle, et de plus en plus d'acteurs étatiques et non étatiques vont vraisemblablement recourir à ces moyens dans les années à venir.

Néanmoins, cela ne retire rien à l'importance des moyens traditionnels (militaires) dans le déroulement des conflits. Les moyens cybernétiques et d'information peuvent servir à dégrader une situation en préparation à une attaque pour finalement déboucher sur un conflit armé traditionnel. Dans l'environnement actuel, il faut compter avec une large palette de moyens et de types d'attaques, allant des forces d'opérations spéciales et des armes de précision aux opérations relevant du domaine spatial. Cela inclut les menaces dans et depuis l'espace aérien, surtout que toujours plus d'acteurs étatiques et non étatiques peuvent utiliser des armes de grande portée. Le développement rapide de nouvelles technologies et de l'intelligence artificielle offre de nouvelles possibilités, également pour les systèmes d'armes autonomes. Ainsi, les drones augmentent considérablement le potentiel des attaques, du renseignement et de la transmission de données, et cela à moindre coût et sans risques. C'est pourquoi les forces armées d'Europe doivent toujours être en mesure de faire face à un adversaire égal, au moins en termes d'espace et de temps. Elles misent donc sur la mobilité, les formations à disponibilité

élevée, la défense aérienne, les capacités efficaces et interconnectées de contrôle, de communication et de conduite, la digitalisation et les nouvelles technologies.

Pour convenir à ce large éventail de possibilités d'attaques, les forces armées doivent aussi être en mesure d'opérer dans la zone grise, entre le conflit armé ouvert et la paix. Pour ce faire, leurs aptitudes défensives et offensives sont consolidées dans le cyberespace. Les autorités doivent être à même d'identifier les agissements visant à influencer et à désinformer, et d'y réagir selon la nature du conflit.

Les moyens modernes de déroulement des conflits sapent les stratégies de dissuasion. Celle-ci repose sur le principe que l'adversaire doit croire, à travers une communication crédible, qu'il risque en cas d'attaque de subir des dommages qu'il n'est pas prêt à supporter. Mais cette dissuasion est en grande partie inefficace lorsqu'une attaque se déroule en dessous du seuil d'un conflit armé, que son auteur ne peut être déterminé de manière concluante et que la population se détourne en partie de son propre État du fait des activités de désinformation. La dissuasion militaire est donc complétée par un mélange d'instruments civils pour la prévention des conflits et le renforcement de la résilience de la société et de l'État face aux attaques hybrides.

Changements fondamentaux

La politique internationale en matière de sécurité est marquée par la concurrence entre les grandes puissances. Elle se manifeste dans une lutte d'influence et est renforcée par le progrès technologique. Dans le domaine de la technologie notamment naît une concurrence systémique entre les différents modèles d'économie et de développement. De même, le progrès technologique, avec la mondialisation, donne naissance à de nouveaux acteurs majeurs sur le plan de la sécurité politique, tels que des entreprises d'importance mondiales. En outre, une polarisation renforcée des sociétés, qui peut se manifester par l'extrémisme, est perceptible. Le modèle de conflit s'est fortement développé dans la direction décrite dans le rapport sur la politique de sécurité 2016. L'importance des outils d'information et des cyberoutils continue d'augmenter afin que les conflits se déroulent le plus secrètement possible, ce qui ne retire toutefois rien aux capacités conventionnelles des forces armées qui continuent de jouer un rôle important. Une dissuasion classique à elle seule est devenue en grande partie inefficace ; l'interaction entre les moyens civils et militaires et une résilience renforcée sont nécessaires.

2.2 Contexte

Le contexte qui influe sur la politique de sécurité de la Suisse n'a cessé de changer ces dernières années : la concurrence entre les grandes puissances et les puissances régionales émergentes s'est intensifiée, la capacité d'action de l'UE et de l'OTAN est mise au défi, l'instabilité à la périphérie de l'Europe s'est amplifiée. En même temps, les organisations internationales sont souvent bloquées dans des dossiers importants touchant la politique de sécurité.

La volonté de certains États, y compris des États européens, de s'engager ensemble pour la sécurité a décliné, comme en témoignent des coalitions ad-hoc ou certains États faisant cavaliers seuls. En outre, les États européens et les États-Unis sont confrontés à des tensions internes sociales, économiques et politiques qui pourraient aussi déboucher sur des conflits violents et qui attirent donc fortement l'attention des dirigeants. Dans

l'ensemble, l'effet protecteur du contexte géographique et politique de la Suisse décline car il est devenu instable, et certains événements éloignés peuvent rapidement et directement compromettre la sécurité du pays.

L'Europe occidentale et centrale se montre relativement stable et résistante aux crises. L'intégration économique et politique entre les États qui la composent pourrait ne pas être fondamentalement remise en question, malgré le Brexit et diverses crises.

L'UE, qui est l'une des plus grandes économies mondiales et actrice au niveau planétaire, a le potentiel pour s'imposer face à de grandes puissances comme la Chine ou les États-Unis. Toutefois, beaucoup de choses dépendent de sa cohésion interne. Trouver un consensus pour se positionner en matière de politique extérieure reste difficile. Alors que l'Europe joue un rôle incontestable en tant que plus grande donatrice mondiale d'aide au développement et défenseur de l'ordre multilatéral, son rôle actuel dans la politique de défense n'est que secondaire. Les initiatives telles que la collaboration structurée permanente ou le Fonds européen de la défense témoignent de la volonté politique à renforcer la capacité de défense, mais ne peuvent cependant pas faire oublier qu'à cet égard, l'Europe continue de fonctionner de manière fortement intergouvernementale et est encore loin d'être autonome dans les questions stratégiques face aux États-Unis et à l'OTAN. Néanmoins, en matière de sécurité intérieure, la situation est différente : grâce aux accords de Schengen, l'UE a réussi à promouvoir une coopération policière efficace. De nombreux développements ont été conclus avec succès.

La pandémie de COVID-19 a montré que les États et les sociétés sont, par réflexe, enclins à faire cavaliers seuls pour le moment. Au sein de l'UE, la politique de la santé relève de ses membres, raison pour laquelle l'Union n'est intervenue qu'en aval et en lien avec les questions économiques et financières. Actuellement, il n'est pas possible de prévoir dans quelle mesure la crise aura des répercussions structurelles et quelles seront les conséquences sur sa cohésion (en matière de politique de sécurité) et sa capacité d'action.

Les lignes de fracture entre *l'Europe et la Russie* ont continué de se renforcer, ce qui a des conséquences directes pour les États voisins occidentaux de la Russie, tout en pouvant pénaliser les intérêts de la Suisse. L'annexion de la Crimée, contraire au droit international, le conflit armé persistant dans l'est de l'Ukraine ainsi que l'utilisation d'armes chimiques contre des personnes honnies du pouvoir pèsent sur les relations entre les deux blocs. Même les futures relations entre l'UE et la *Biélorussie* restent incertaines. Les tensions politiques considérables et les conflits non résolus dans le *Caucase du Sud* peuvent tourner en hostilités ouvertes à tout moment.

L'Europe du Sud-Est est toujours confrontée à des tensions. Dans les Balkans occidentaux, le processus de rapprochement européen a des répercussions stabilisatrices sur la région, bien que le risque de conflit persiste sur place, par exemple entre la Serbie et le Kosovo ainsi qu'en Bosnie et Herzégovine.

L'instabilité des États d'*Afrique du Nord* a des conséquences directes sur la sécurité en Europe. Ces États jouent un rôle important dans la canalisation de la migration de l'Afrique subsaharienne. La pandémie de COVID-19 y a augmenté l'instabilité. L'Algérie doit affronter un surcroît de difficultés au niveau économique et dans sa politique intérieure. Dans les années à venir, il ne faut s'attendre à aucune solution politique viable pour le conflit en Libye. Le fait que des acteurs étrangers s'immiscent dans le conflit sur les plans politique et militaire ne facilite pas la recherche d'une solution.

La sécurité déjà précaire dans la *région du Sahel* s'est encore amenuisée. Le terrorisme djihadiste a engendré le séparatisme, la violence interethnique, une mauvaise gouvernance, la corruption et la criminalité, et s'est répandu dans toute l'Afrique de l'Ouest. Les États touchés ne seront certainement pas en mesure de venir seuls à bout de ces menaces ; c'est pourquoi un engagement international reste important pour la stabilité de la région. Il y a peu de chance que l'augmentation de la population dans plusieurs États du Sahel soit compensée par les économies régionales, sans parler des conséquences économiques de la pandémie de COVID-19 qui freinent tout développement. Il est à supposer que la pression migratoire élevée sur les États d'Afrique du Nord, puis sur l'Europe, perdurera.

Les conflits en *Méditerranée orientale et dans les régions adjacentes* vont très probablement se poursuivre. En Syrie, une solution politique, nécessaire à la résolution du conflit qui la mine, reste encore à trouver. La Turquie s'éloigne des États occidentaux et coopère de manière accrue avec la Russie. L'objectif de la politique turque est de créer sa propre zone d'influence en Afrique du Nord ainsi qu'au Proche et au Moyen-Orient. Cependant, les réalités économiques, y compris les conséquences de la pandémie de COVID-19, pourraient restreindre la portée de sa politique extérieure et de sécurité dans les années à venir. La confrontation entre les États-Unis, Israël et les États arabes du Golfe d'un côté, et l'Iran de l'autre, continuera de marquer la dynamique de la région. Bien qu'une escalade militaire semble peu probable, elle pourrait être déclenchée par un incident militaire ou par une expansion massive des activités d'enrichissement d'uranium de l'Iran. Les États de la région, en particulier l'Irak et le Liban, sont confrontés à de lourdes crises socio-économiques et politiques persistantes, aggravées par la pandémie de COVID-19. À cela s'ajoutent des tensions entre groupes religieux et ethniques. Le conflit du Proche-Orient n'est toujours pas résolu et reste de grande importance pour la région, bien que son potentiel de mobilisation ait décliné aux yeux de l'opinion publique internationale. À l'avenir également, les groupes djihadistes utiliseront à leur avantage les tensions et conflits, les faiblesses économiques et la polarisation sociale dans les États de la région. L'interaction de ces facteurs peut conduire à des conflits armés nationaux et internationaux, comme à l'effondrement de divers États.

Le retrait partiel des États-Unis du Proche et du Moyen-Orient ainsi que leur retenue en Afrique du Nord augmentent les possibilités d'influence de la Russie, de la Chine, de la Turquie et de l'Iran dans ces régions. Les États européens devraient continuer à s'engager en Afrique du Nord et au Proche et Moyen-Orient sur le plan de la politique de sécurité, mais devront de plus en plus composer sur place avec les activités des Chinois et des Russes.

Concurrence entre les grandes puissances

Les *États-Unis* alignent stratégiquement leur politique de sécurité sur le défi posé par la Chine. La tendance à procéder unilatéralement et à se retirer des organisations ou des accords internationaux s'est amplifiée ces dernières années. Cependant, avec la nouvelle présidence, elle pourrait être inversée, au moins en partie. Les États-Unis disposent toujours d'énormes moyens économiques, diplomatiques et militaires ainsi que d'une puissance dite douce toujours considérable. C'est toujours la seule grande puissance qui dispose d'un potentiel évident pour un rôle de leader mondial. Toutefois, elle l'a peu exploité au cours de ces dernières années.

Il est probable que les États-Unis miseront sur les instruments de pouvoir économiques, tels que les droits spéciaux et les sanctions, également dans les années à venir. Malgré la focalisation sur sa concurrence avec la Chine, l'Europe aussi devra continuer à tenir compte d'une telle pression des États-Unis. Ce qui est particulièrement important pour le contexte de la Suisse en matière de politique de sécurité, c'est que les États-Unis continueront probablement à faire pression sur leurs alliés européens pour qu'ils augmentent leurs contributions à la défense commune.

La *Russie* reste une puissance militaire et défie ponctuellement la dominance des États-Unis. Elle est poussée par des réflexions politiques et de la méfiance vis-à-vis de l'Occident. En tant que puissance nucléaire et en raison de ses interventions militaires dans le Caucase, au Proche et Moyen-Orient et en Afrique du Nord, de son rôle dans le conflit en Ukraine et de son importance dans les organisations internationales, la Russie joue un rôle considérable dans la politique de sécurité internationale. Elle a la volonté politique et les moyens diplomatiques pour exercer son influence sur les développements régionaux et mondiaux. L'appareil du pouvoir russe n'a pas peur d'employer des moyens létaux contre les personnes qui lui sont impopulaires, aussi à l'étranger. Toutefois, la Russie ne dispose pas des moyens économiques et de l'attractivité du modèle de société pour occuper durablement un rôle de leader dans la politique mondiale. Cela ne changera pas fondamentalement, même si elle remporte des succès, par exemple dans l'approvisionnement des pays en vaccins contre le COVID-19. La Russie veut consolider une zone d'influence exclusive, en particulier le long de la frontière de l'ancienne Union soviétique. Sa politique continuera probablement de se focaliser sur l'Europe de l'Est, les Balkans et l'espace méditerranéen.

Sur le plan militaire, la Russie a considérablement renforcé son potentiel dans certains domaines au cours de ces dernières années. Cependant, dans un avenir proche, elle restera inférieure à l'OTAN sur le plan conventionnel, pour autant que les États-Unis maintiennent leur contribution à la sécurité européenne. La dissuasion stratégique entre les États-Unis et la Russie est maintenue pour les années à venir, malgré la dégradation du régime de maîtrise des armements et de désarmement. L'utilisation combinée d'une large palette de moyens – civils et militaires, apparents et secrets – pour exercer une pression est typique de la Russie. Elle continuera à essayer d'affaiblir l'OTAN et l'UE, à monter leurs membres les uns contre les autres et à promouvoir, dans ces États, des acteurs qui servent ses intérêts. Les activités de renseignement de la Russie contre les intérêts européens vont se poursuivre à un niveau élevé. La criminalité organisée russe est également importante au regard des intérêts sécuritaires de la Suisse.

La *Chine* s'est élevée au rang de deuxième plus grande économie du monde et de grande puissance planétaire. Elle impose ses intérêts de politique économique et de sécurité en Asie, en partie avec peu de considération pour les intérêts des autres pays et parfois en contradiction avec le droit international. Combinée à la modernisation de ses forces armées, la montée en puissance économique de la Chine mène à de nouveaux équilibres dans le monde. La Chine défie ponctuellement la dominance des États-Unis et ne cesse de développer son influence par des moyens économiques, politiques et propres à une grande puissance. Reste toutefois à savoir dans quelle mesure elle cherche à jouer un véritable rôle de leader mondial et si un tel rôle serait accepté sur le plan international. Le modèle de gouvernement chinois reste un État à parti unique, dirigé par le Parti communiste. Au cours des années dernières, une centralisation encore plus forte du pouvoir politique s'est mise en place. En outre, le contrôle de la société et la répression à

l'intérieur du pays ont été renforcés. L'économie surendettée et le ralentissement de la croissance pourraient constituer un défi pour le pouvoir.

La perception mutuelle de la menace des États-Unis et de la Chine, accentuée par l'apparition et l'évolution de la pandémie de COVID-19, intensifie la concurrence dans les domaines de la politique, le commerce, la technologie et l'armée. Avec l'*Initiative route et ceinture*, la Chine accède à de nouveaux marchés et investit dans des projets d'infrastructures et dans l'extraction de ressources naturelles. Elle vise à contrôler elle-même les infrastructures qui y sont liées. En Asie, par exemple en mer de Chine méridionale, la Chine utilise des moyens paramilitaires et militaires pour faire pression. En Afrique, elle joue déjà un rôle clé sur le plan économique et développe constamment son engagement économique au Proche et Moyen-Orient. Néanmoins, elle s'efforce de rester en dehors des conflits régionaux. La Chine assied son influence également en Europe par un engagement politique ou par l'acquisition d'entreprises et d'infrastructures ou parties d'entre elles. Pour les États occidentaux, il en résulte des dépendances, par exemple en raison de contrôles des infrastructures de transport, de communication et logistiques, par des entreprises d'État chinoises.

La manière de procéder au Xinjiang et à Hong Kong ainsi que la politique chinoise en rapport avec la pandémie ont provoqué des réactions répressives aux États-Unis et dans beaucoup d'États européens. Les politiques chinoises de nombreux États occidentaux sont en passe de devenir, de manière générale, plus critiques. Il faut donc fondamentalement compter sur un mélange entre dialogue et endiguement. Du point de vue de la Chine, ces développements devraient être importants, raison pour laquelle il faut s'attendre à une augmentation de ses activités de renseignement.

Organisations internationales et collaboration

L'annexion de la Crimée en 2014 a engendré des efforts supplémentaires pour l'OTAN dans l'affermissement de sa capacité de défense collective. Elle a dû renforcer sa présence sur le flan oriental et réintroduire des exercices de mobilisation et de transfert pour toute l'Alliance. Les États membres de l'OTAN ont également pris des mesures afin de pouvoir mieux gérer un conflit hybride en tant qu'alliance, par exemple en désignant les cyberattaques comme des potentiels déclencheurs pour une défense collective et en renforçant leurs capacités de gestion des crises. Cependant, la gestion des menaces hybrides est encore un défi pour l'OTAN, en particulier en ce qui concerne la mise en œuvre des obligations d'assistance prévues par l'art. 5 du Traité de l'Atlantique Nord.

Le débat concernant la répartition des charges entre les membres de l'OTAN, qui dure depuis des décennies, s'est intensifié au cours de ces dernières années. Avant la pandémie de COVID-19, de nombreux États européens avaient augmenté leurs dépenses consacrées à la défense. Il reste à déterminer si ne serait-ce qu'un certain nombre d'États de l'OTAN réduiront à nouveau leur budget d'armement et de défense pendant la pandémie, au moins temporairement.

Dans les années à venir, l'OTAN pourra continuer d'agir sur les plans politique et militaire et restera ainsi importante pour la sécurité de l'Europe, si toutefois les États-Unis ne réduisent pas leur engagement européen de manière notable. Les lignes de fracture entre ses alliés orientaux, qui exigent l'attention de l'organisation sur la dissuasion militaire russe, et les alliés qui se sentent d'avantage menacés par les

développements sur son flanc sud, continueront d'exister. Les intérêts de la Turquie dans l'espace méditerranéen sont en partie en conflit avec les intérêts d'autres États membres de l'OTAN. Ces tensions mettent également au défi la capacité d'action de cette dernière.

Au niveau mondial, l'ONU, et particulièrement le Conseil de sécurité, joue toujours un rôle important dans les questions de sécurité internationale, malgré un affaiblissement tendanciel des organisations internationales. Néanmoins, à l'heure actuelle, les normes, organisations et accords internationaux sont régulièrement contournés et affaiblis par des acteurs, qu'ils soient étatiques ou non. Cela se manifeste aussi dans la maîtrise des armements et le respect de l'interdiction du recours à la force en vertu du droit international. Lorsque les membres permanents du Conseil de sécurité montrent un intérêt direct pour une région en conflit, les organes de l'ONU pourraient souvent se trouver dans l'impasse en matière de règlement des conflits, également dans les années à venir.

Au niveau régional, il faut mentionner l'Organisation pour la sécurité et la coopération en Europe (OSCE), la seule organisation de sécurité sur le Vieux continent qui inclut la Russie et les États-Unis sans favoriser l'un par rapport à l'autre et qui reste une sphère de dialogue et d'instauration de la confiance. L'OSCE continuera à être confrontée à des difficultés pour trouver un consensus sur les questions importantes du fait du renforcement de la polarisation.

La capacité d'action limitée des organisations internationales favorise le transfert vers des coalitions ad-hoc et des groupes informels comme le G7 ou le G20. Cette tendance à s'éloigner des organisations internationales devrait se poursuivre, en particulier lorsqu'il s'agit de défendre des intérêts politiques régionaux ou relevant de la politique de puissance d'États ou de groupes d'États.

Changements importants

L'orientation des États-Unis a un impact direct sur la cohésion de l'OTAN et influence essentiellement le contexte de la politique de sécurité de la Suisse. Fondamentalement, le Conseil de sécurité de l'ONU et l'OSCE sont en mesure d'agir, mais sont en partie bloquées dans leurs prises de décisions politiques en raison des intérêts opposés des grandes puissances. L'UE est toujours confrontée à des défis politiques et économiques. Sa capacité d'action internationale dépendra de sa cohésion. La périphérie européenne est devenue encore plus instable, notamment en raison des luttes d'influence. La Chine représente un défi pour les États occidentaux en ce qui concerne la manière dont il faut traiter avec elle sur les plans politique et économique. La Russie continue de mettre fortement au défi les États européens et les États-Unis sur le plan de la politique de sécurité. Dans l'ensemble, l'effet protecteur du contexte géographique et politique de la Suisse a diminué ces dernières années.

2.3 État de la menace

Les différentes menaces qui pèsent sur la Suisse sont examinées ci-après. En outre, il faut noter que les différentes menaces agissent en même temps sur la Suisse, de manière coordonnée et mutuellement renforcées, et peuvent nuire au système politique du pays, à sa population et à son infrastructure.

2.3.1 Menaces en provenance du cyberespace

Différentes raisons justifient les cyberattaques : l'espionnage, le sabotage, la manipulation, la désinformation ou des raisons criminelles. Une pléthore d'acteurs différents commettent ces attaques ; parmi eux, des cybercriminels, des hacktivistes, des entreprises de piratage à but lucratif, des sociétés écrans ou organisations étatiques. Un certain nombre d'États accroissent fortement leurs capacités offensives dans ce domaine, que ce soit individuellement ou en lien avec des groupements non étatiques. Il faut donc s'attendre à une augmentation des cyberattaques de cet ordre, mais dont les auteurs ne sont pas clairement identifiés. La menace dans le cyberespace grandit également en raison de la volonté croissante d'utiliser offensivement les moyens cybernétiques lors de conflits et des scrupules de plus en plus ténus des cybercriminels à accepter d'occasionner des dommages.

Depuis quelques années, on peut observer en Suisse un accroissement des cybercapacités offensives de la Chine, de l'Iran et de la Russie à des fins d'espionnage. La menace que représentent les cyberattaques chinoises et russes pour les cibles économiques et politiques dans notre pays reste élevée. Parmi ces cibles, on compte, entre autres, les autorités, l'armée, les organisations internationales et les représentations étrangères sises à Genève ainsi que les secteurs financier et technologique. Dans le domaine criminel, les attaques à l'aide de rançongiciels (communément appelés *ransomwares*), lors desquelles les données sont cryptées et ainsi rendues inutilisables, sont de plus en plus fréquentes. De telles attaques peuvent fortement paralyser des entreprises et des systèmes entiers.

L'état de la menace dans le cyberespace est largement influencé par la numérisation de processus opérationnels et de production. Les moteurs sont les nouvelles technologies telles que l'industrie 4.0, la technique du bâtiment numérique ou les infrastructures urbaines en réseau, qui tirent profit de nouvelles possibilités de développement grâce à l'introduction de la nouvelle norme de téléphonie mobile 5G. Cela s'accompagne d'une délégation renforcée de processus jusqu'alors contrôlés par l'homme vers des systèmes de technologies de l'information et de la communication. Les compétences décisionnelles pour les processus ayant en partie des répercussions physiques sont de plus en plus transférées aux systèmes numériques qui prennent en toute indépendance des décisions en matière de pilotage, même au sein des infrastructures critiques. Avec l'enchaînement de ces décisions qui s'appuient les unes sur les autres, des processus décisionnels de plus en plus complexes sont exécutés par des systèmes informatiques autonomes. Ces processus ne sont plus nécessairement contrôlés par le véritable exploitant ; ils peuvent être transférés à des fournisseurs de prestations externes.

Avec la numérisation des processus de production, les solutions logicielles et matérielles nécessaires constituent une composante centrale et critique. Dans les années à venir, les pays d'origine des fabricants continueront à se limiter à certains États, à savoir la Chine et les États-Unis. Ainsi, ces derniers contrôlent la chaîne logistique mondiale des moyens informatiques et possèdent une influence considérable dans les organes internationaux de normalisation tels que l'Union internationale des télécommunications. Suite à des mesures de contrôle des exportations et des sanctions imposées par les États-Unis, deux zones distinctes sont en train de se former. Dans un cas extrême, cela pourrait signifier que la Suisse doive finalement limiter sa la coopération avec l'un ou l'autre de ces deux pays (Chine ou États-Unis) et ses partenaires, avec toutes les dépendances qui en découlent.

Les interdépendances et dépendances systémiques fortes des chaînes de logistique dispersées dans le monde conduisent à une vulnérabilité accrue et à la propagation d'effets pouvant être déclenchés par des cyberincidents. Ainsi, la menace augmente également pour les infrastructures critiques, qui peuvent être endommagées même en cas de cyberincidents ne les visant pas directement.

2.3.2 Influence et désinformation

Les activités d'influence visent à manipuler les perceptions, les pensées et les actions des individus, des groupes et des sociétés.

Ces activités sont importantes sur le plan de la politique de sécurité lorsqu'elles émanent d'États, sont dirigées contre le fonctionnement d'un État ou d'une société, ou ont comme objectif de saper l'ordre démocratique d'un État. Il peut s'agir de retarder des processus de prises de décision, d'orienter des décisions dans une direction souhaitée ou de nuire, de manière générale, à la confiance dans les processus démocratiques et les actions étatiques.

De telles activités comprennent l'utilisation coordonnée de moyens et méthodes légaux et illégaux, des activités dans le domaine de la communication, de la propagande et de la désinformation, des actions secrètes des services de renseignement et l'exercice de pressions politiques, économiques et militaires. Elles excluent les activités d'influence en lien avec la représentation habituelle des intérêts dans le cadre de la diplomatie.

Avec l'utilisation délibérée et massive d'informations falsifiées, manipulées ou dans un contexte biaisé, ces activités sont principalement dirigées contre des sociétés démocratiques qui reposent sur la confrontation honnête des idées sur une base factuelle commune.

Vu les luttes de pouvoir qui se mènent au niveau international, la Suisse doit partir du principe que le risque de voir sa société et ses autorités la cible d'activités d'influence augmente. En tant qu'État situé au cœur du continent européen et partageant les valeurs occidentales, ainsi qu'en raison de sa forte mise en réseau internationale sur les plans économique et politique, elle est une cible indirecte d'activités dirigées contre les États occidentaux. En outre, le risque existe que le territoire suisse soit utilisé à mauvais escient comme plaque tournante par des agents pour y mener ou financer des activités d'influence contre des pays tiers ou des organisations internationales.

Il faut souligner le potentiel de menace des opérations d'influence pour la Suisse en tant qu'actrice sur la scène politique internationale et comme siège de nombreuses organisations internationales. C'est ainsi que, dans le passé, certaines de ses institutions et des organisations internationales qui y sont implantées ont subi de telles activités de la part des Russes. Tout cela était en lien avec des événements politiques et des activités de renseignement qui, de prime abord, ne concernaient pas la Suisse. Ainsi, le Laboratoire de Spiez est devenu une cible dans le cadre des vastes activités d'influence menées dans le contexte de la tentative d'assassinat de l'agent russe Skripal. Des organisations sportives internationales étaient également dans le viseur.

Jusqu'à présent, la Chine et la Russie – qui ne visent pas les mêmes objectifs et emploient par conséquent des moyens différents – étaient des actrices de premier plan pour la Suisse.

Il faut toutefois s'attendre à ce que d'autres États seront aussi en mesure et auront la volonté de mener de telles activités en Suisse et contre elle.

2.3.3 Terrorisme

En Suisse, des personnes ou des cellules liées au prétendu État islamique ont été détectées, et pour certaines condamnées, pour leur implication dans des planifications d'attentats depuis notre territoire. Les investigations des autorités suisses ont montré que des voyageurs suisses à motivation djihadiste auraient suggéré des attentats contre des infrastructures situées sur le territoire suisse, voire participé à leur planification. D'autre part, la propagande des groupes djihadistes peut inspirer des personnes à passer à l'action violente en Suisse.

Comme l'ont montré les attaques de Morges (12.09.2020) et de Lugano (24.11.2020), la menace terroriste la plus probable en Suisse vient d'acteurs dont l'orientation violente s'enracinent autant dans des crises personnelles et psychiques que dans une conviction idéologique. Les personnes radicalisées les plus susceptibles de commettre des attaques sont inspirées par la propagande djihadiste sans avoir forcément de contact direct avec un groupe ou une organisation de cette mouvance. Ces attaques restent un défi sécuritaire.

Le spectre des attaques possibles va de simples attaques perpétrées par des individus ou de petits groupes isolés jusqu'à des opérations logistiques complexes (comme l'utilisation d'agents de combat chimiques, drones). Les attentats perpétrés par des auteurs isolés ou des petits groupes inspirés par le djihadisme et qui ne nécessitent que peu de moyens logistiques ne sont pas tributaires des capacités dudit État islamique ou d'Al-Qaïda. En règle générale, ces auteurs isolés ou ces petits groupes agissent spontanément, sans directives ni soutien financier extérieurs. Même les attaques complexes de plus grande envergure au moyen d'explosifs, de produits chimiques simples tels que des gaz toxiques (comme le chlore) ou d'autres substances toxiques (comme la ricine) ne nécessitent que peu de moyens et de ressources.

La menace terroriste à motivation djihadiste persistera pour notre pays. L'idéologie ayant mobilisé de jeunes Européens à se rendre en Syrie est toujours vivace, et ce malgré la destruction du califat autoproclamé de l'organisation État islamique. De plus, les conflits ayant causé l'émergence de factions djihadistes ne vont vraisemblablement pas trouver d'épilogue prochainement. La menace de ces acteurs va donc marquer durablement les prochaines années. Les voyageurs djihadistes restent une menace pour la sécurité intérieure et extérieure de la Suisse. Leur éventuel retour représente un défi pour les autorités sur tous les fronts (questions juridiques, d'intégration et de sécurité).

La Suisse devrait continuer à être une cible secondaire des attentats djihadistes, sauf si certaines de ses décisions politiques étaient perçues comme étant hostiles aux musulmans ou à l'islam. Toutefois, les organisations internationales et les intérêts de pays étrangers, jouant un rôle prépondérant dans la lutte contre le terrorisme sur la scène internationale, pourraient être la cible d'attaques sur son territoire.

Les intérêts suisses à l'étranger pourront toujours être la cible des actions opportunistes ou erratiques de groupes djihadistes, par exemple en Afrique du Nord ou au Sahel. La menace djihadiste continuera probablement à s'y étendre et pourra même toucher des pays jusqu'ici épargnés, comme les pays du Golfe de Guinée. De même, au Proche et au Moyen-Orient, les groupes djihadistes continueront de représenter une menace pour de

nombreux pays, compte tenu des tensions et des conflits mais aussi des conditions économiques et sociales défavorables.

Malgré ces développements, le territoire suisse reste principalement utilisé afin de mener des activités de propagande, de recrutement, d'appui logistique et de financement par des groupes terroristes de tous horizons idéologiques. Ces réseaux de sympathisants constituent également un vivier de candidats pour des départs dans les régions où évoluent ces groupes.

2.3.4 Extrémisme violent

Actuellement, trois scènes sont considérées comme extrémistes violentes : celles d'extrême gauche, d'extrême droite et de la cause animale. Jusqu'à présent, l'usage de la violence dans ces trois domaines reste en-deçà de la limite du terrorisme.

Les scènes d'extrême droite et gauche pourraient intensifier le recours à la violence et son niveau d'intensité, et se développer ainsi en groupes terroristes. Si la motivation au sein de ces groupes manque actuellement, le potentiel de violence et les connaissances tactiques et techniques y sont présentes. De même, des individus non affiliés à ces structures mais partageant leurs idéologies ont les capacités permettant un passage rapide à l'action. Même si ces personnes planifient et mettent en œuvre leurs actes seules, elles sont influencées par les courants sociaux, peuvent entretenir des contacts avec d'autres personnes radicalisées et correspondre avec d'autres personnes ou groupes extrémistes.

Une telle évolution de l'extrémisme violent vers le terrorisme est par exemple observée dans divers pays européens. Les attaques d'auteurs isolés à motivation d'extrême droite deviennent de plus en plus fréquentes et les moyens utilisés s'assimilent à des moyens pouvant être qualifiés de terroristes. La Suisse risque, au cours des prochaines années, d'être confrontée au même phénomène.

D'autres mouvements pourraient aussi en arriver à la violence afin d'imposer leurs idées politiques. Des partisans des idéologies extrêmes pourraient se radicaliser si leurs demandes ne sont pas prises en compte dans le cadre du processus politique actuel. Les conséquences de la pandémie de COVID-19 pourraient encore renforcer ces tendances.

2.3.5 Conflit armé

Des moyens hybrides sont de plus en plus souvent utilisés dans les conflits, comme l'engagement de troupes non identifiées ou l'utilisation de moyens cybernétiques et la désinformation. Mais la menace directe ou l'utilisation de la violence armée par des acteurs étatiques reste aussi une réalité en Europe.

La confrontation entre la Russie et les États occidentaux n'est pas un phénomène à court terme. Bien que la Russie et l'OTAN s'efforcent d'éviter un conflit armé, ce risque a augmenté au cours des dernières années. La Russie a fortement renforcé son potentiel militaire et s'efforce d'avoir la capacité à mener une guerre en Occident contre un puissant adversaire conventionnel. Cela se reflète également dans les scénarios des grands exercices stratégiques annuels. L'OTAN et les États européens neutres axent, eux aussi, à nouveau plus fortement leur politique autour d'un conflit conventionnel.

Une situation de crise importante aux frontières orientales de l'OTAN constituerait un énorme défi pour l'Europe et pourrait conduire à des instabilités politiques, économiques et sociales, ainsi qu'à des perturbations dans les chaînes d'approvisionnement et les mouvements migratoires. Mais un conflit entre l'OTAN et la Russie peut tout aussi bien naître en raison d'une montée de la violence à la périphérie de l'Europe, avec les mêmes conséquences. En cas de crise aggravée en Europe, la Russie pourrait utiliser des moyens militaires afin de changer la donne aux confins orientaux de l'OTAN. Le rétablissement du *statu quo ante* ne serait alors possible qu'avec une poursuite de l'escalade.

Une menace militaire directe due à une attaque terrestre contre la Suisse paraît peu probable à court et à moyen terme. Les répercussions d'une telle attaque seraient néanmoins tellement graves que cette éventualité ne doit pas être négligée. Cependant, dans le cas d'un conflit armé entre l'OTAN et la Russie, la Suisse pourrait être directement menacée si le conflit venait à durer et si l'une des parties au conflit voulait, avec des moyens militaires, contraindre notre pays à faire des concessions économiques, politiques ou militaires. Un adversaire pourrait donc utiliser, ou menacer d'utiliser, des armes à longue portée, des forces d'opérations spéciales et des moyens cybernétiques contre des cibles militaires et civiles sur territoire suisse. En revanche, une intervention terrestre directe apparaît comme invraisemblable, même dans un tel scénario.

Néanmoins, en raison de la conduite des conflits de plus en plus hybrides, la Suisse, en tant que membre de la communauté des États européens, serait aussi directement concernée par un conflit armé à l'extérieur de son territoire, sur le continent européen ou à sa périphérie (même sans la participation de la Russie ou de l'OTAN). Dans un tel scénario, elle serait dans tous les cas menacée par des cyberattaques, des actes de sabotage, la désinformation, la subversion, l'utilisation abusive de son territoire pour le soutien logistique ainsi que par l'espionnage. Les ressortissants suisses dans la zone de crise seraient également menacés. Il faudrait aussi prendre en compte le fait qu'elle devrait traiter des questions de neutralité en lien avec l'utilisation de son territoire et de son espace aérien pour le transit militaire.

Une attaque armée contre la Suisse ou d'autres pays européens pourrait aussi être commandée depuis des régions éloignées, à l'extérieur de l'Europe. Une telle attaque serait envisageable avec des missiles balistiques, des missiles de croisière et des armes hypersoniques. À l'heure actuelle, seuls quelques États en disposent, mais aucune intention de ce genre n'est perceptible ou prévisible parmi eux. Toutefois, la diffusion de ces systèmes d'armes va se poursuivant. Bien qu'une attaque contre la Suisse avec des armes à longue portée ne soit pas considérée comme probable dans les années à venir, la crise en Libye dans les années 2008 à 2010 a montré qu'un État pouvait prendre des mesures draconiennes contre elle sans préavis. Si un acteur de ce type disposait d'armes à longue portée, il pourrait également menacer la Suisse et la faire chanter avec des moyens militaires.

2.3.6 Développement et prolifération des systèmes d'armes

Au cours des dernières années, le contrôle des armements et le désarmement ont été fortement affaiblis par la violation d'accords existants, d'une part, mais surtout par la

résiliation d'accords importants par des grandes puissances[1], d'autre part. Il est cependant possible, mais en aucun cas certain, que le changement de gouvernement à Washington conduise à un renversement de tendance.

Les stocks d'armes nucléaires des grandes puissances, s'ils sont quantitativement stables, sont en voie de développement sur le plan qualitatif. Encouragé par le regain des tensions, des investissements important sont consentis dans la modernisation des arsenaux ou le développement de nouveau de systèmes de lancement. Les armes hypersoniques pourraient être particulièrement déstabilisantes. Il n'existe aucune défense efficace contre ces armes. Elles effacent la frontière entre un armement nucléaire et un armement conventionnel, et leur vitesse implique qu'un État doive, par manque de temps, contre-attaquer dès qu'il perçoit le moindre signe d'une attaque avec ces armes, ce qui augmente le risque d'erreurs.

Il faut s'attendre à une amélioration qualitative du potentiel de menace en raison des missiles de croisière (surtout une amélioration de la capacité de survie), comme à une nouvelle prolifération de ce genre d'armes. La Russie notamment continue de développer de tels systèmes, qui pourraient également menacer la Suisse. La hausse du nombre de plateformes d'engagement pour les missiles de croisière est également notable (sous-marins, vaisseaux de surface). D'autres États se procureront des missiles de croisière dont la portée pourra atteindre la Suisse ; toutefois, il s'agira d'engins balistiques à ogive conventionnelle. Quelques acteurs non étatiques disposent également de tels missiles, mais ne sont que de courte portée.

D'autres États auront la capacité de mener des guerres interconnectées dans des zones d'opération lointaines. Le développement de la technologie des capteurs et des drones nécessaire à cet effet progresse dans le monde entier.

La Suisse, en tant que pôle scientifique et industriel novateur, est touchée par le risque de prolifération des technologies pour les armes de haut niveau technologique et doit continuer à mettre en œuvre des mesures pour empêcher cette prolifération. L'industrie suisse dispose de capacités dans le domaine des sciences des matériaux qui, par exemple, sont importantes pour le développement d'armes hypersoniques. La robotique et le développement de drones civils en Suisse peuvent servir les développements étrangers dans le domaine militaire. Les instruments de précision font depuis toujours partie des compétences centrales de l'économie suisse. Afin d'avoir accès aux technologies, les États étrangers n'acquièrent pas uniquement des biens individuels, mais achètent des supports technologiques ou proposent des accords de coopération attractifs aux hautes écoles suisses. Il se peut également que de telles infrastructures soient utilisées pour des développements dangereux pour la Suisse.

2.3.7 Espionnage

En tant que siège d'organisations internationales et de multinationales, théâtre de négociations internationales, place financière et commerciale et pôle technologique et de recherche, la Suisse est une cible de choix pour les espions. Les membres de son corps diplomatique, ses militaires, les autorités cantonales et fédérales, les journalistes, les

[1] En particulier, l'accord de Vienne sur le nucléaire iranien (Joint Comprehensive Plan of Action, JCPoA), le Traité sur les forces nucléaires à portée intermédiaire (Intermediate Range Nuclear Forces Treaty, INF) et le traité *Ciel ouvert* pour l'autorisation de vols de surveillance (Open Skies Treaty).

savants, les responsables économiques et les personnes exposées de certaines diasporas constituent aussi des cibles pour les services de renseignement.

Il en ira de même à l'avenir. Tout porte à croire que les ressources et les capacités des services de renseignement ne cessent de croître, moyens cybernétiques offensifs compris. La digitalisation crée de nouvelles possibilités permettant de dérober des informations sensibles ou de saboter des systèmes d'information. Il faut s'attendre à ce que l'augmentation des cyberattaques observée ces dernières années en Suisse, à des fins d'espionnage étatique, poursuit sur sa lancée.

2.3.8 Grande criminalité et criminalité organisée

La criminalité en Suisse est marquée par les possibilités technologiques qui se développent rapidement. Le monde criminel adapte ses méthodes de travail et utilise ces nouveaux instruments. La criminalité numérique (cybercriminalité) utilise des technologies modernes comme les services d'internet, les médias sociaux et le cryptage, en particulier pour les délits contre le patrimoine. Ces derniers peuvent être commis aussi bien par des groupes criminels organisés que par des auteurs sans grand niveau d'organisation.

La menace de la criminalité organisée vient essentiellement d'organisations mafieuses italiennes ; celles-ci sont actives à l'échelle nationale et menacent considérablement les institutions de notre État de droit et la place financière suisse. Leur présence forte et de longue durée, leurs relations familiales en Suisse et leur langue leur permettent d'infiltrer l'administration et l'économie.

En outre, les groupes criminels provenant d'États de l'ancienne Union soviétique représentent un potentiel élevé de menace pour la Suisse. Ils disposent souvent de moyens économiques importants et, dans certains cas, d'un soutien politique dans leurs pays d'origine. Ils sont actifs dans des domaines d'infraction auxquels la Suisse est particulièrement exposée en raison de l'attrait exercé par sa place financière (p. ex. blanchiment d'argent) ou qui touchent de près à la fonction de l'État et de ses autorités (p. ex. corruption). L'importance capitale de la place financière suisse pour les élites dirigeantes de ces pays constitue aussi une source de risques en matière de politique extérieure.

Les groupes criminels originaires d'Europe du Sud-Est représentent également une menace considérable. Bien organisés et très violents, ces groupes dominent certaines formes de criminalité, comme le trafic de drogue et la traite d'êtres humains.

Changements importants dans l'état de la menace

Les menaces hybrides ont particulièrement augmenté, notamment celles en provenance de l'espace cybernétique ou de l'espace de l'information, se traduisant par des activités d'espionnage, d'influence et de criminalité numérique. Les développements technologiques et l'érosion des instruments de contrôle des armements accroissent les risques de prolifération et le potentiel d'abus des technologies qui sont étudiées ou élaborées en Suisse. Les menaces issues du terrorisme et de la criminalité organisée subsistent. La polarisation sociale accrue peut contribuer à l'aggravation de la menace de l'extrémisme violent. Actuellement, les attaques militaires conventionnelles ne sont pas

perçues par la Suisse comme une menace directe ; elles pourraient cependant le devenir si l'OTAN venait à se confronter militairement à la Russie. Dans un tel cas, l'accent serait probablement mis sur l'utilisation d'armes à longue distance, de forces d'opérations spéciales et de cyberattaques contre des cibles militaires et civiles. Mais la Suisse, sa population et ses infrastructures peuvent également être concernées de nombreuses façons par des conflits armés à la périphérie de l'Europe.

2.3.9 Catastrophes et situations d'urgence

Les catastrophes et les situations d'urgence sont des événements et des situations qui provoquent des dommages ou des dérangements tels que le personnel et le matériel ne suffisent pas à la communauté touchée pour s'en sortir. Leurs causes peuvent être d'origine naturelle, technologique ou sociétale. Les catastrophes se produisent soudainement (p. ex. tremblements de terre, coupures d'électricité) ; les situations d'urgence, quant à elles, se préparent souvent sur une longue période et durent plus longtemps (p. ex. vagues de chaleur, pénuries d'électricité ou pandémies). Il existe aussi le risque de catastrophes parallèles dues à des dangers naturels (incendies de forêt, inondations, sécheresses, vagues de chaleur, tremblements de terre, etc.) et à des situations d'urgence, telles celles provoquées par une pandémie.

La pandémie de COVID-19 a clairement démontré la vulnérabilité de la Suisse face à des catastrophes ou des situations d'urgence. Il faut s'attendre à ce que le risque que de tels événements se reproduisent suite à différentes tendances, comme le changement climatique, l'urbanisation ou la digitalisation, augmente dans les années à venir. En outre, la Suisse est aussi l'un des États les plus densément peuplés d'Europe. Cela conduit à une forte concentration d'infrastructures, ce qui peut engendrer d'importants dégâts si ces dernières sont endommagées ou détruites, par exemple par un tremblement de terre ou une inondation.

Il n'est pas un endroit dans notre pays où les *dangers naturels* ne peuvent se produire. En raison du changement climatique, les événements tels que de fortes précipitations, des inondations, des vagues de chaleur et également de plus longues périodes de sécheresse sont de plus en plus fréquents et intenses. Des périodes de sécheresse et de vagues de chaleur comme celles que nous avons connues en 2015 et en 2018 seront probablement plus fréquentes et plus violentes. Ces vagues de chaleur font partie des dangers les plus éminents pour la Suisse. Les incendies de forêt que ces vagues de chaleur déclenchent et la sécheresse, ainsi que les inondations causées par de fortes précipitations, sont également des dangers récurrents. Les tempêtes hivernales devraient continuer à provoquer des dommages importants. Les instabilités des pentes, amplifiées par le changement climatique et accompagnées de fortes précipitations toujours plus fréquentes, conduisent à des glissements de terrain et à des éboulements pouvant également endommager les zones d'habitation et les infrastructures. Les éboulements et écroulements sont des dangers grandissants. Bien que l'activité sismique en Suisse soit de niveau faible à moyen, les tremblements de terre qui s'y produisent font partie des risques les plus élevés de catastrophes naturelles en raison des dommages potentiels qu'ils peuvent provoquer.

Pour les *dangers de nature technique*, il est important 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. Les pannes et les perturbations dues à des erreurs techniques, des cyberrisques, des dangers naturels, au sabotage ou à de mauvaises manipulations ont des conséquences de plus en plus lourdes. La combinaison ou l'enchaînement d'événements est un risque particulièrement grand. Avec la délégation progressive des tâches à la technologie, les processus de décision deviennent moins transparents et l'expertise dans ces domaines diminue. Cela peut compliquer la lutte contre les catastrophes et les situations d'urgence. La pollution, des pannes dans les installations de production, des défaillances au sein des infrastructures d'approvisionnement, de transport, d'information et de communication, ainsi que la contamination des denrées alimentaires et de l'eau potable sont des conséquences possibles ; les coupures d'électricité prolongées peuvent conduire à une augmentation de la criminalité ou des troubles.

La vulnérabilité augmente entre autres en raison de la convergence accrue des différents secteurs. Également pour des raisons d'aménagement du territoire, les réseaux d'énergie, de transports et de télécommunications sont davantage mis en commun. Ainsi, les cyberattaques peuvent, par exemple, toucher en même temps plusieurs secteurs et domaines d'infrastructures et conduire à des perturbations intersectorielles et à large échelle.

Les catastrophes et situations d'urgence de nature sociétale peuvent engendrer des effets complexes et considérables, comme l'a clairement montré la pandémie de COVID-19. Une grave pandémie lourde de conséquences peut survenir à nouveau à n'importe quel moment. Les pandémies, combinées à des pénuries d'électricité sur un vaste territoire durant plusieurs semaines, comptent ainsi parmi les risques les plus grands en Suisse dans le domaine des catastrophes et situations d'urgence. En plus des pandémies qui menacent directement les êtres humains, les épizooties, comme la peste porcine africaine, peuvent également provoquer d'importants dommages. Outre ces dangers sanitaires, des attentats terroristes – aussi bien conventionnels qu'avec des moyens ABC – ou des cyberattaques complexes peuvent conduire à des catastrophes et des situations d'urgence.

Changements importants lors de catastrophes et de situations d'urgence

La pandémie de COVID-19 le montre de façon saisissante : les dangers de nature sociétale se sont accrus. Mais il faut s'attendre à ce que les catastrophes naturelles, elles aussi, deviennent de plus en plus fréquentes en raison du changement climatique. Des précipitations extrêmes ainsi que des situations d'urgence dues à une sécheresse persistante ou à des vagues de chaleur, sont également possibles. Ces cinq dernières années, la probabilité des catastrophes de nature technique a pu être globalement réduite par des mesures préventives. Cependant, en raison de la densification des agglomérations et des infrastructures ainsi que des chaînes d'approvisionnement complexes et des cyberrisques, la vulnérabilité s'est accrue simultanément.

2.3.10 Migration et politique de sécurité

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, comme le trafic et la traite d'êtres humains, la criminalité, l'extrémisme violent et le terrorisme. La migration des

régions en crise au Proche et Moyen-Orient et en Afrique du Nord présente notamment un risque d'infiltration d'acteurs djihadistes. Cependant, de nombreux États d'Europe, dont la Suisse, ont renforcé leurs contrôles auprès des requérants d'asile, en accordant une attention particulière aux djihadistes potentiels. Par ailleurs, beaucoup de routes migratoires ne sont plus aussi ouvertes et perméables qu'avant ; les pays de transit sur les principales routes migratoires ont amélioré leurs contrôles aux frontières. Les contrôles aux frontières extérieures de l'UE ont aussi été renforcés.

Les déclencheurs de la migration mondiale sont des conflits militaires, ethniques ou religieux dans certains pays, ainsi que des tensions sociales, de mauvaises situations en matière de sécurité, des persécutions politiques, la croissance démographique dans les pays à faibles revenus, une mauvaise économie, le chômage, l'absence de perspectives, la pauvreté et le manque de possibilités de formation. Le changement climatique également conduira à des flux migratoires en progression à moyen et à long terme. Dans les pays de destination, le besoin de main d'œuvre en raison du vieillissement de la population dans les pays à revenus élevés, les regroupements familiaux, les diasporas, la sécurité politique, une situation stable en matière de sécurité et des possibilités de formation favorisent l'immigration. La pandémie de COVID-19 risque de conduire à la détérioration de la situation économique et à un chômage plus élevé dans pratiquement tous les États. Toutefois, elle aura certainement des répercussions plus lourdes sur l'Afrique et le Proche et Moyen-Orient que sur beaucoup d'États européens. C'est pourquoi, en l'espace d'un à trois ans, elle pourrait conduire à une augmentation des flux migratoires.

Les demandeurs d'asile fuient d'abord vers les pays voisins des leurs. L'Europe et la Suisse sont toujours des objectifs importants pour les migrants, surtout pour ceux en provenance des pays du Proche et Moyen-Orient et d'Afrique. La route migratoire de la Méditerranée centrale (essentiellement de la Libye vers l'Italie) reste prioritaire pour la Suisse en raison de sa situation géographique. En deuxième place arrive la route orientale par la Méditerranée et les Balkans. La migration vers l'Europe de l'Ouest par la route occidentale (détroit de Gibraltar et îles Canaries) gagne de l'ampleur de manière générale, mais n'est que d'une importance mineure concernant la migration secondaire vers la Suisse. De par leur situation géographique, ces trois routes resteront les routes principales d'accès par la Méditerranée. Néanmoins, il faut s'attendre à une (nouvelle) diversification des routes ainsi qu'à une adaptation des réseaux de passeurs de même que des méthodes en fonction des mesures prises par les pays de transit et de destination. Des itinéraires alternatifs, par exemple une route nordique par la Russie et la Finlande, sont souvent trop difficiles et ont été empruntés par trop peu de migrants pour pouvoir être établis comme routes principales. Cependant, on ne peut pas totalement exclure l'apparition de nouvelles routes, surtout si d'autres États veulent utiliser la migration comme moyen de pression contre l'Europe. La migration par voie aérienne, par exemple en provenance d'Amérique du Sud, reste plutôt négligeable pour la Suisse, du moins à court et à moyen terme.

Reste à savoir si, en plus de la Turquie, d'autres États européens utiliseront également la migration comme moyen de pression. Entre-temps, on peut supposer que la Convention de Dublin restera en vigueur – cette dernière s'étant avérée être un moyen efficace de gérer la migration vers l'Europe, notamment aux yeux de plusieurs États importants de l'UE. L'incapacité à trouver des solutions durables aux frontières extérieures de Schengen et à réformer le système de Dublin risque d'affaiblir la capacité de l'Europe à gérer les

mouvements migratoires et de la rendre plus vulnérable face à l'utilisation politique de tels mouvements.

Changements importants des aspects de la migration en matière de politique de sécurité

La migration n'est, de prime abord, pas un défi pour la politique de sécurité, mais liée à la traite d'êtres humains, à la criminalité, à l'extrémisme violent et au terrorisme, elle peut avoir des conséquences importantes sur elle. Les mesures de contrôle la concernant ont été renforcées le long des routes migratoires, aux frontières extérieures de l'espace Schengen. Cependant, les causes initiales poussant les personnes à migrer subsistent. Les conséquences du changement climatique renforceront probablement les mouvements migratoires.

3 Intérêts et objectifs de la politique de sécurité

3.1 Principes

La politique suisse de sécurité se fonde sur des *principes* visant à garantir sa continuité et sa prévisibilité. Ces principes correspondent à l'idée que la Suisse se fait de sa propre politique de sécurité et créent un cadre stable pour cette politique. Ils sont présentés ci-dessous.

- *Coopération* et *neutralité* : en matière de politique de sécurité, la Suisse collabore en particulier avec des États européens, dispose d'un réseau international solide et souhaite en principe entretenir de bonnes relations avec tous les États. Le cœur du principe de la neutralité, à savoir ne soutenir aucune partie lors d'un conflit armé international, vise à rester à l'écart des conflits armés et à demeurer impartial.
- *Démocratie*, *respect du droit international public* et *État de droit* : la Suisse promeut un ordre international qui se fonde sur le droit et des règles. Elle s'engage en faveur du respect du droit international, y compris le droit international humanitaire et les droits de l'homme.
- *Fédéralisme* et *subsidiarité* : en Suisse, la politique de sécurité est une tâche commune de la Confédération, des cantons et des communes. Ces trois échelons sont importants pour assurer la sécurité de l'État, de la société et de l'économie. Dans ce cadre, le principe de la subsidiarité joue un rôle fondamental. Des structures étatiques décentralisées requièrent beaucoup de coordination, mais elles rendent aussi l'ensemble du système suisse flexible, robuste et résilient.
- *Milice* et *obligation de servir* : le système suisse de l'obligation de servir se fonde sur le principe de milice, selon lequel les personnes astreintes peuvent aussi assumer des fonctions de cadres. L'obligation de servir comprend généralement, d'une part, une instruction de base et, d'autre part, des services d'instruction ou des engagements répartis sur plusieurs années. L'armée, la protection civile, le service civil et une partie des corps de sapeurs-pompiers se fondent sur ce système, qui doit leur permettre de disposer des effectifs requis.

Ces principes fixent le cadre de la politique suisse de sécurité. Leur interprétation doit toutefois être régulièrement contrôlée à l'aune des évolutions politiques et sociétales, qu'il s'agisse des compétences en matière de sûreté intérieure ou du développement du système de l'obligation de servir.

3.2 Intérêts

Outre les principes susmentionnés, les *intérêts supérieurs à long terme* évoqués ci-dessous influencent également la politique suisse de sécurité.

1. *Non-recours à la force* et *ordre international fondé sur des règles* : les conflits entre les États et en leur sein doivent être réglés par des moyens pacifiques. Le recours à la force n'est légitime qu'en cas d'autodéfense ou sur la base d'une décision du Conseil de sécurité de l'ONU. Pour maintenir la paix et renforcer la stabilité internationale, un ordre international reposant sur des règles est primordial.
2. *Autodétermination* et *liberté d'action* : les États doivent pouvoir décider eux-mêmes de leurs propres affaires, tant au niveau intérieur que dans leurs relations

internationales. Ce principe vaut également pour l'information non faussée, la possibilité de former ses opinions sans être influencé et la prise de décisions libre et sans pressions extérieures.

3. *Sécurité de la population et des infrastructures critiques* : la population et les infrastructures critiques doivent être protégées contre le recours ou les menaces de recours à la violence ou au sabotage ainsi que contre les dangers naturels et les défaillances techniques afin que l'État, l'économie et la société puissent fonctionner durablement. La résilience face aux situations de crise est également primordiale.

3.3 Objectifs

L'objectif général de la politique suisse de sécurité consiste à protéger la liberté d'action, l'autodétermination et l'intégrité de la Suisse et de sa population ainsi que ses conditions de vie contre les menaces et les dangers, et à contribuer à la stabilité et à la paix par-delà les frontières. La sécurité est comprise dans un sens large. Outre les menaces militaires, les formes hybrides de conflits et les menaces liées au terrorisme, à l'extrémisme violent et à la criminalité, la Suisse prend en considération les conséquences sur la politique de sécurité de défis mondiaux en matière de climat, de santé et de migration. De plus, elle tient compte des interdépendances des menaces et des dangers.

Vu la situation, les principes et les intérêts, les *objectifs spécifiques* ci-dessous constituent des priorités de la politique de sécurité pour ces prochaines années.

Objectif 1 : renforcer la détection précoce des menaces, des dangers et des crises

Ces dernières années, les transformations s'accélèrent sur le plan international, et il est toujours plus difficile de garder une vue d'ensemble de la situation. Des crises et des conflits se déroulant dans des régions très éloignées peuvent rapidement avoir des répercussions directes sur la Suisse et ses intérêts. Par conséquent, il est devenu encore plus important d'identifier précocement les évolutions et les crises potentielles qui peuvent avoir un impact sur la sécurité. C'est pourquoi la Suisse continue de renforcer ses moyens et ses capacités dans les domaines de la détection précoce et de l'évaluation autonome des menaces et des dangers. Dans ce cadre, elle examine également les interdépendances croissantes entre les différentes évolutions liées à la sécurité.

Objectif 2 : renforcer la coopération, la sécurité et la stabilité au niveau international

La Suisse s'investit afin que les organisations internationales actives dans le domaine de la sécurité puissent agir et se développer, dans l'intérêt de la sécurité et de la paix. Elle s'engage en faveur d'un ordre international fondé sur des règles et de la coopération bilatérale et multilatérale, notamment avec les pays voisins et les organisations importantes pour la politique de sécurité. Elle contribue à la promotion et au renforcement de la paix et de la stabilité dans son environnement par des moyens civils et militaires et collabore au niveau international dans le domaine policier. En outre, elle soutient les efforts visant au contrôle des armements et au désarmement ainsi que les mesures de lutte contre la prolifération d'armes et de vecteurs puissants. Elle participe à la concrétisation et au développement de normes et d'instruments modernes dans le domaine du droit

international afin de réglementer les nouvelles technologies et les nouveaux systèmes d'armes.

Objectif 3 : mettre davantage l'accent sur les conflits hybrides

La Suisse tient compte de l'évolution des conflits et oriente ses instruments de politique de sécurité en conséquence afin de pouvoir identifier, prévenir et combattre tous les phénomènes liés aux conflits hybrides. Elle renforce la protection de l'État et de ses institutions, de l'économie et de la population face aux cybermenaces, aux activités d'influence, à l'espionnage, aux pressions, aux menaces de violences et au recours à la force. Pour l'ensemble du spectre des menaces hybrides et lors de tensions durables dans son environnement, l'armée doit être en mesure de protéger efficacement le pays, sa population et ses infrastructures, aussi contre les menaces dans l'espace aérien, et de soutenir les autorités civiles.

Objectif 4 : garantir la libre formation des opinions et les informations non faussées

La formation des opinions doit être libre et se fonder sur des informations transparentes, basées sur des faits et non dénaturées par de la désinformation, des tentatives d'influence ou la propagande de la part d'acteurs étatiques ou agissant pour le compte d'États. Vu la hausse des activités visant à influencer ou à désinformer des sociétés et des États, il convient d'accorder davantage d'attention à cet aspect. Par conséquent, la Suisse doit utiliser ses moyens de détection précoce et de suivi de la situation aussi afin d'identifier les activités visant à exercer une influence et, au besoin, de prendre des mesures de protection, par exemple en communiquant activement. À cette fin, il est nécessaire de renforcer la collaboration entre les organes fédéraux concernés et avec les cantons, ce qui permettra d'accroître la résilience de la Suisse et de sa population face à ce genre d'activités.

Objectif 5 : accroître la protection contre les cybermenaces

L'État, l'économie et la société doivent être protégés contre les cybermenaces. Pour remédier aux vulnérabilités, qui augmentent avec la digitalisation, la Suisse renforce ses capacités à identifier et maîtriser rapidement les cyberincidents présentant une menace pour la sécurité, même lorsqu'ils persistent sur une longue période et touchent simultanément de nombreux domaines. Elle entend mieux anticiper les développements dans le domaine cyber, notamment en ce qui concerne l'usage croissant de l'intelligence artificielle. En cas de besoin, la Confédération soutient des tiers tout en respectant le principe de la responsabilité individuelle, agit en régulatrice et crée des incitations afin d'augmenter la résilience de la Suisse dans le domaine cyber. Ce faisant, elle met également à profit les opportunités qui découlent de la digitalisation.

Objectif 6 : prévenir le terrorisme, l'extrémisme violent, le crime organisé et les autres formes de criminalité transnationale

Le terrorisme, le crime organisé, la criminalité transnationale et l'extrémisme violent, encouragé par la polarisation de la société, constituent des menaces durables. La Suisse

les considère comme prioritaires. Elle met tout en œuvre afin d'empêcher l'établissement de groupes terroristes, extrémistes violents ou liés à la grande criminalité sur son territoire. À cette fin, elle emploie des moyens de prévention, de coopération et de répression. Elle empêche également les activités visant à exporter ou à soutenir le terrorisme. Elle lutte contre la circulation irrégulière des marchandises et des personnes à ses frontières ainsi que contre les répercussions négatives de la migration clandestine.

Objectif 7 : renforcer la résilience et la sécurité d'approvisionnement en cas de crises internationales

La Suisse renforce sa capacité d'action, de résistance, d'adaptation et de régénération face aux conséquences de crises et de tensions internationales, qu'il s'agisse de risques sociétaux comme des pandémies ou de conflits armés – lesquels peuvent aussi toucher la Suisse indirectement même si elle n'est pas elle-même victime d'une agression. La Suisse doit se préparer à des problèmes d'approvisionnement de longue durée en cas de crises internationales. Elle entend accroître sa sécurité d'approvisionnement s'agissant de biens et de services critiques, de première nécessité et importants pour la sécurité tout en réduisant les dépendances et les vulnérabilités dans des domaines liés à la capacité de fonctionnement et à la sécurité du pays et de sa population. En font également partie les compétences et les capacités industrielles et technologiques en Suisse qui revêtent une importance pour la sécurité.

Objectif 8 : améliorer la protection contre les catastrophes, la préparation aux situations d'urgence et la capacité de régénération

Les risques pour la nature et la société augmentent en raison du changement climatique, tandis que la densité de l'habitat, la mobilité et la concentration des infrastructures ont tendance à s'accroître. Par conséquent, la Suisse entend améliorer ses capacités et ses moyens permettant de prévenir les dangers naturels, technologiques et sociétaux, de se protéger contre ces dangers, ainsi que de maîtriser les catastrophes et les situations d'urgence qui en découlent. À cette fin, il convient de renforcer les moyens de prévention et de gestion à l'intérieur du pays ainsi que la coopération internationale.

Objectif 9 : renforcer la collaboration entre les autorités et les acteurs de la gestion de crise

Vu la volatilité de la situation et l'interconnexion des menaces et des dangers, il convient d'améliorer la collaboration entre les domaines politiques et les instruments qui revêtent une importance pour la politique de sécurité en Suisse, et ce, tant en situation normale que lors de crises. Il s'agit de faire en sorte que la coopération et la coordination entre les autorités et les moyens de la Confédération, des cantons et des communes soient efficaces. En outre, il faut améliorer les capacités permettant une gestion efficace des crises à l'échelon national. Il convient d'utiliser les enseignements tirés de vraies crises et d'exercices afin d'optimiser les processus, les responsabilités et les interfaces entre la Confédération et les cantons.

4 Mise en œuvre : domaines politiques et instruments de la politique de sécurité

4.1 Domaines politiques et instruments

Pour atteindre ses objectifs de politique de sécurité, la Suisse dispose de différents domaines politiques et instruments qu'elle utilise de façon coordonnée. Les *domaines politiques* ci-dessous contribuent à la politique de sécurité et à la réalisation de ses objectifs.

La *politique extérieure* permet à la Suisse de défendre ses intérêts à l'étranger et de cultiver des relations. La Suisse soutient les efforts visant à améliorer la compréhension mutuelle à l'échelon international et s'engage afin que les organisations internationales soient en mesure d'agir. Elle participe au renforcement de la sécurité et de la stabilité internationales en proposant ses bons offices, en contribuant à la promotion de la paix, en s'investissant en faveur du droit international, de l'État de droit et des droits de l'homme, en luttant contre les causes de l'instabilité et des conflits au moyen de la coopération au développement et en soulageant la population civile grâce à l'aide humanitaire. La Suisse promeut le développement durable et aide les États à lutter contre le changement climatique et à s'adapter à ses effets. En outre, elle s'engage en faveur du contrôle des armements, du désarmement et d'un cyberespace libre et sûr. Le réseau extérieur de la Suisse sert tant à la défense de ses intérêts qu'à la gestion de crise.

La *politique économique* crée des conditions favorables à l'économie, à la prospérité et à un approvisionnement du pays stable et résistant aux crises au moyen de chaînes d'approvisionnement diversifiées. La Suisse s'engage en faveur de l'ouverture des marchés et de la coopération internationale et encourage les échanges commerciaux dans le domaine des biens, des services et des investissements. Dans ce cadre, elle tient compte de l'intégration de l'économie dans les chaînes de valeur mondiales et des risques liés à la politique de sécurité. En mettant en place des conditions favorables, elle contribue à maintenir et à développer en Suisse des technologies et des industries importantes pour la sécurité. Elle répond du contrôle à l'exportation d'armements et de biens à double usage ainsi que de la mise en œuvre des sanctions internationales. La politique d'approvisionnement du pays établit des directives concernant la constitution de réserves de biens et de services critiques (p. ex. produits thérapeutiques, aliments, sources d'énergie).

L'*information* et la *communication* constituent une tâche transversale dont l'importance va croissante aussi pour la politique de sécurité. Quand les autorités assurent une information véridique et une communication crédible, la robustesse et la résilience face aux tentatives d'influence s'en trouvent renforcées. La Confédération, les cantons et les communes ont le devoir de contribuer à la qualité de la formation des opinions. Le Conseil fédéral fournit activement, rapidement et régulièrement des informations factuelles, approfondies et uniformisées concernant ses évaluations de la situation, ses planifications et ses décisions. Si cette manière de procéder est particulièrement importante en temps de crise, elle promeut également la confiance de la population dans les autorités en situation normale.

Par ailleurs, la Suisse dispose aussi des *instruments* ci-dessous, qui sont spécialisés dans des tâches de politique de sécurité et contribuent à la réalisation des objectifs ad hoc.

L'*armée* est le principal instrument permettant de maîtriser des menaces qui, par leur intensité et leur ampleur, mettent en danger l'intégrité territoriale du pays, la sécurité de l'ensemble de la population ou l'exercice du pouvoir étatique. Elle doit être en mesure de contrer et de maîtriser plusieurs menaces simultanément, même lorsqu'elles revêtent des formes diverses, affichent différents niveaux d'intensité et sont durables. La défense contre une attaque armée constitue la compétence fondamentale de l'armée. Cette dernière s'adapte à l'évolution des conflits et aux différentes formes de conflits hybrides, renforçant également ses capacités dans le domaine cyber. Elle soutient les autorités civiles dans la maîtrise de situations de crise de toutes sortes et participe à la promotion internationale de la paix ainsi qu'à l'aide en cas de catastrophe à l'étranger.

La *protection de la population* est chargée de protéger la population et ses conditions d'existence en cas de catastrophes ou de situations d'urgence. Les organes de conduite, les organisations partenaires (la police, les corps de sapeurs-pompiers, les services de santé publique, les services techniques et la protection civile) et des tiers collaborent dans les domaines de la prévention et de la maîtrise des évènements. La conduite et les moyens de la protection de la population relèvent principalement de la responsabilité des cantons. La Confédération assume une fonction de coordination et se charge des travaux de fond, notamment en ce qui concerne l'analyse nationale des risques. Elle assure la conduite et la coordination lors de catastrophes et de situations de crise qui relèvent de sa responsabilité, par exemple en cas d'augmentation de la radioactivité. L'État-major fédéral Protection de la population constitue l'organe de coordination fédéral dans le domaine de la protection de la population. Il assure la communication entre la Confédération, les cantons, les exploitants d'infrastructures critiques et les autorités étrangères. L'Office fédéral de la protection de la population est responsable des systèmes d'alerte, d'alarme et d'information des autorités et de la population en cas de dangers ou d'événements. Il exploite la Centrale nationale d'alarme et le Laboratoire de Spiez, gère la coordination dans les domaines de la protection civile et de la protection des biens culturels, assure la formation des organes cantonaux de conduite, des cadres de la protection civile et des spécialistes et, en collaboration avec les cantons, répond de la conception et de la gestion des constructions protégées.

Le *Service de renseignement de la Confédération* est responsable de la détection précoce et de la prévention des menaces contre la sécurité intérieure et extérieure liées au terrorisme, à l'extrémisme violent, à l'espionnage, à la prolifération d'armes de destruction massive et à des cyberattaques visant des infrastructures critiques. En outre, il recueille et évalue des informations concernant l'étranger qui ont une incidence sur la politique de sécurité. Grâce à ses produits, il soutient la conduite de la politique de sécurité et informe les autorités de poursuite pénale. De plus, il aide les cantons à maintenir la sûreté intérieure, gère le renseignement intégré à l'échelon national (regroupant les autorités fédérales et cantonales chargées de la sécurité) et assure la collaboration avec les partenaires étrangers.

La *police* est l'instrument principal de lutte contre la criminalité, de prévention des dangers et d'application de mesures au moyen d'un usage direct de la contrainte. La souveraineté policière relève en premier lieu des cantons. Conjointement avec les polices municipales, les corps de police cantonaux assurent la sécurité publique sur leur territoire et assument des tâches de police de sûreté et de police judiciaire. S'agissant de la Confédération, ses compétences concernent la lutte contre la grande criminalité, en particulier le terrorisme, l'extrémisme violent, le crime organisé et la criminalité

transnationale. Sur mandat du Ministère public de la Confédération, l'Office fédéral de la police mène des poursuites pénales et coordonne la coopération policière nationale et internationale. En outre, il protège des personnes et des bâtiments sous la responsabilité de la Confédération et développe et exploite des systèmes d'information et des centres de compétences nationaux.

L'*Administration fédérale des douanes* (AFD) participe, dans le cadre de ses tâches à la frontière, à la lutte contre le terrorisme, l'extrémisme violent et la criminalité transnationale. Elle contribue à la lutte contre la migration illégale aux frontières intérieures et extérieures de l'espace Schengen, par exemple en identifiant des réseaux de passeurs ou en participant à des opérations de l'Agence européenne de garde-frontières et de garde-côtes (Frontex). De plus, elle contrôle le trafic transfrontalier des personnes et des marchandises et recherche des individus et des objets à la frontière. Assumant des tâches de police de sûreté, elle constate les infractions et transmet les affaires aux autorités compétentes. Dans le cadre de ses compétences, elle mène en outre des poursuites pénales à l'encontre des contrebandiers. L'AFD collabore étroitement avec ses partenaires nationaux et internationaux, notamment en prenant part à des interventions communes et en assurant un échange intensif d'informations.

Le *service civil* constitue un service de remplacement pour les personnes aptes au service militaire qui ne peuvent pas accomplir ce dernier pour des raisons de conscience. Conformément à la loi fédérale du 6 octobre 1995 sur le service civil, ces personnes effectuent des affectations lors de catastrophes ou de situations d'urgence, notamment dans les domaines de l'environnement et, s'agissant de la santé et du service social, des soins et de l'assistance. Les affectations du service civil complètent les interventions et engagements de la protection civile et de l'armée et peuvent renforcer la résilience dans le domaine de la protection de la population. Le service civil n'est pas conçu comme une organisation de première intervention et n'est pas structuré en formations. Des travaux en cours étudiant le développement à long terme du système de l'obligation de servir examinent la contribution que le service civil peut apporter lors de catastrophes et de situations d'urgence.

4.2 Mise en œuvre des objectifs de la politique de sécurité

Les sous-chapitres ci-dessous indiquent *comment* la Suisse entend poursuivre et mettre en œuvre ses objectifs en matière de politique de sécurité.

4.2.1 Renforcer la détection précoce des menaces, des dangers et des crises

La situation internationale est devenue plus volatile et imprévisible. Face aux développements liés à la politique de sécurité, les délais d'alerte se sont raccourcis. Il faut s'attendre à des évolutions et à des enchaînements d'événements surprenants. Avec les conflits hybrides, il est plus difficile d'identifier les cybermenaces contre des infrastructures critiques ou les tentatives d'influence de l'étranger à l'encontre de la Suisse. En conséquence, il est d'autant plus important que la détection précoce et l'appréciation des menaces et de leurs conséquences soient efficaces, de sorte que les évolutions importantes puissent être anticipées à temps et que des mesures appropriées puissent être prises.

C'est, en premier lieu, le rôle de la recherche et de l'évaluation d'informations par les *services de renseignement*. Il s'agit d'identifier et d'évaluer la capacité et la volonté d'acteurs civils ou militaires de déployer une politique de puissance à l'étranger, de même que les développements dans les domaines du terrorisme, de l'extrémisme violent, de l'espionnage, des cybermenaces, des activités d'acteurs étrangers visant à exercer une influence et de la prolifération.

Pour améliorer la capacité d'anticipation au niveau de la conduite politique, la *détection précoce de crises de la Chancellerie fédérale* permet également d'identifier les risques et les chances concernant l'économie, la société et la politique. De plus, les représentations suisses à l'étranger contribuent à la détection précoce de crises.

La *détection précoce des nouveaux dangers naturels et des changements parmi ces derniers* sert de suivi global de la situation dans le cadre de la gestion intégrale des risques. Les scénarios climatiques actuels permettent de quantifier les conséquences du changement climatique et donc de faire des prédictions sur des événements extrêmes (p. ex. précipitations violentes, sécheresse, vagues de chaleur).

La détection précoce des menaces, des dangers et des crises peut être renforcée en particulier au moyen des mesures ci-dessous.

- Amélioration des *capacités d'identification et d'appréciation autonome* des évolutions et des menaces ayant une incidence sur la sécurité, par exemple en participant à des systèmes d'exploration par satellite[2] ou en accroissant les *capacités permettant de traiter de grandes quantités de données*.
- Renforcement des *représentations suisses à l'étranger*, notamment en transférant de la centrale plus d'une trentaine de postes afin de contribuer sur place à la détection précoce et à l'analyse de développements importants pour la politique de sécurité.

4.2.2 Renforcer la coopération, la sécurité et la stabilité au niveau international

Fondé sur des règles, l'ordre international a contribué à la sécurité et à la prospérité de la Suisse. Cette dernière continuera de s'engager en faveur de la démocratie, de la liberté, de l'État de droit, des droits de l'homme et du droit international, ainsi que du multilatéralisme et de la capacité d'action des organisations internationales. En obtenant, comme elle le souhaite, un *siège non permanent au Conseil de sécurité de l'ONU* pour la période 2023 à 2024, la Suisse disposera d'un instrument supplémentaire afin de s'investir en faveur de ses intérêts, de ses convictions et de ses valeurs.

Au *niveau régional*, la Suisse milite pour un renforcement de l'OSCE. Elle entretient des contacts et coopère avec des organisations actives dans le domaine de la politique de sécurité dont elle n'est pas membre, dans la mesure où cela sert ses intérêts sans la placer dans une relation de dépendance. En Europe, le Partenariat pour la paix (avec l'OTAN) et la coopération avec l'UE occupent le premier plan. La *coopération bilatérale* se concentre sur les États voisins. En outre, la Suisse s'efforce de cultiver des échanges au sujet de la politique de sécurité avec des pays tels que les États-Unis, la Russie ou la Chine.

---

[2] La Suisse participe par exemple au système d'exploration par satellite français *Composante spatiale optique* (CSO).

Avec ses *bons offices* et la *promotion civile et militaire de la paix*, la Suisse contribue à la prévention et à la résolution des conflits. Tirant profit de sa réputation de médiatrice indépendante, fiable et discrète, elle est impliquée dans plus d'une dizaine de processus de paix, tant dans le cadre de missions de l'ONU, de l'OSCE ou de l'UE que de façon bilatérale. En outre, elle sert d'État hôte à des pourparlers de paix menés sous l'égide de l'ONU. La promotion civile et militaire de la paix, la *coopération au développement* et l'*aide humanitaire* sont étroitement coordonnées.

Dans le domaine de la politique de sécurité, le *contrôle des armements* et le *désarmement* contribuent à la stabilité et à la prédictibilité de l'environnement. La Suisse milite pour le désarmement nucléaire et soutient les mesures visant à lutter contre la prolifération d'armes nucléaires. Elle s'engage en faveur de l'interdiction des armes chimiques et biologiques ainsi que de l'universalisation et de l'application des interdictions concernant les mines antipersonnel et les armes à sous-munitions. Le *contrôle des exportations* et la mise en œuvre des *sanctions internationales* permettent d'éviter la prolifération de biens et de technologies d'armement sensibles. La Suisse s'accorde avec d'autres États industriels et s'engage en faveur de règles universelles. Pour ne pas prétériter son industrie, elle fonde sa politique en matière de contrôle des exportations et de sanctions sur des directives et des principes harmonisés au niveau international.

Dans le domaine de la *coopération policière internationale*, la Suisse utilise les instruments dont elle bénéfice en sa qualité de membre associé de Schengen et contribue à leur développement : échanges simplifiés d'informations de police, coopération policière transfrontalière, système d'information Schengen. De plus, elle renforce la collaboration dans le domaine policier au moyen de l'accord de coopération avec Europol. Au niveau mondial, la Suisse participe aux activités d'Interpol.

La coopération, la sécurité et la stabilité au niveau international peuvent être renforcées en particulier au moyen des mesures ci-dessous.

- *Candidature à un siège non permanent au Conseil de sécurité de l'ONU* afin de s'engager en faveur de la sécurité et de la stabilité internationales ainsi que pour le renforcement du multilatéralisme et d'un ordre international fondé sur des règles, conformément aux intérêts et aux valeurs de la Suisse.
- Élaboration et adoption de *stratégies régionales et thématiques de politique extérieure* faisant suite à la stratégie actuelle.
- Mise à profit des chances découlant du *développement de la politique de sécurité et de défense de l'UE* afin d'accroître la collaboration, y compris la coopération militaire effectuée dans le cadre de la collaboration structurée permanente.
- Engagement en faveur du maintien de la *pertinence du Partenariat pour la paix*, des échanges d'informations et d'opinions concernant la politique de sécurité et de la collaboration pratique, utile à toutes les parties, dans ce cadre.
- Développement de la *promotion militaire de la paix* en mettant l'accent sur des prestations à haute valeur ajoutée qui sont particulièrement demandées, notamment le transport aérien, la reconnaissance aérienne, et des fonctions spéciales dans les domaines de l'instruction, de la logistique ou de l'élimination des munitions non explosées.

- Engagement en faveur du *développement du contrôle des armements et du désarmement* au vu des nouvelles évolutions technologiques et de leurs conséquences sur les systèmes d'armes (p. ex. *big data*, intelligence artificielle, autonomie, nouvelles technologies réseau), élaboration d'une *nouvelle stratégie* en matière de contrôle des armements et de désarmement.

4.2.3 Mettre davantage l'accent sur les conflits hybrides

Dans les conflits hybrides, les acteurs recourent à une large palette d'instruments qui va de l'utilisation de moyens cyber à une attaque classique en passant par l'espionnage ou des activités visant à exercer une influence. Ce genre de conflit doit être saisi dans sa globalité pour pouvoir identifier et contrer les menaces, développer des contremesures et renforcer la résilience de l'État et de la population.

S'agissant des conflits hybrides, l'armée[3] doit être en mesure de couvrir une large palette de capacités et de soutenir les autorités civiles déjà dans la zone grise qui se situe entre la paix et le conflit armé ouvert. Lorsque la situation change, elle doit pouvoir réagir rapidement et assumer parallèlement différentes tâches. Même si le schéma conflictuel s'est transformé, la défense contre une attaque armée reste une tâche fondamentale, ce d'autant qu'un conflit hybride peut déboucher sur une attaque militaire. Par conséquent, l'armée doit pouvoir assumer simultanément des tâches subsidiaires de *protection* et de sécurité, fournir une *aide* en cas de catastrophe ou de situation d'urgence et *défendre* le pays, sa population et ses infrastructures, tout en étant capable de passer rapidement d'une tâche à l'autre. Il s'agit par exemple de protéger des secteurs, des installations, des axes de circulation et l'espace aérien ainsi que de défendre la population et les infrastructures critiques contre des attaques. L'armée doit donc s'orienter sur de tels engagements et, dans ce cadre, employer ses moyens de façon coordonnée et, pour les engagements subsidiaires, en fonction des besoins des partenaires civils.

De premiers pas ont déjà été faits dans cette direction avec le développement de l'armée. La disponibilité échelonnée et la réintroduction de la mobilisation ont permis d'accroître la disponibilité opérationnelle des troupes. Sur la base des capacités militaires requises, l'équipement est régulièrement renouvelé et complété dans des domaines clés. De nouveaux avions de combat et un système de défense sol-air seront acquis afin de pouvoir continuer à surveiller intensivement l'espace aérien au-delà du service quotidien de police aérienne, par exemple lors de tensions internationales durables, et à le défendre en cas d'attaque. Le développement et le renforcement des capacités militaires et des moyens cyber constituent une priorité.

L'armée se développe constamment afin de s'adapter aux transformations que connaissent les menaces. À l'avenir, ce processus se déroulera de manière continue et par petites étapes plutôt que dans le cadre de grandes réformes exigeant beaucoup de temps, et ce, afin d'accroître la flexibilité et de pouvoir réagir plus rapidement lorsque les menaces changent.

---

[3] Le présent sous-chapitre décrit la mise en œuvre de l'objectif 3 au sein de l'armée. Sa mise en œuvre par d'autres domaines politiques et instruments de la politique de sécurité figure aux ch. 4.2.4 et 4.2.5.

L'accent peut être davantage mis sur les conflits hybrides notamment au moyen des mesures ci-dessous.

- *Forces terrestres* davantage axées sur l'environnement hybride, en tenant compte de la forte densité de population et de l'urbanisation ; équipement permettant de mieux les protéger et de les rendre plus agiles, formations d'engagement structurées de manière plus flexible et modulaire.
- Développement et renforcement des *cybercapacités* de l'armée, un élément essentiel de l'attention accrue portée à l'environnement hybride ; possibilité d'utiliser aussi les moyens de l'armée pour un appui subsidiaire.

Attaque armée et défense dans le cadre de la transformation des conflits

Compte tenu de la transformation des schémas conflictuels, une attaque armée contre la Suisse n'est plus nécessairement synonyme d'incursion de forces militarisées. En effet, un adversaire peut poursuivre ses objectifs stratégiques sans user ouvertement de moyens militaires, mais en portant atteinte aux infrastructures critiques, à la conduite étatique, à l'économie ou à la vie de la société. Il peut par exemple recourir à des cyberattaques, à des activités d'influence intensives, à des mesures économiques, à des actes de sabotage, à des opérations menées par des forces spéciales ou d'autres acteurs ; sa palette de possibilités va jusqu'aux armes de longue portée. Dans une telle situation, l'objectif ne serait pas de violer physiquement l'intégrité territoriale du pays, mais de nuire au fonctionnement du pays et de ses institutions afin de miner la souveraineté de l'État et la cohésion de la société. Par conséquent, une cyberattaque peut aussi être qualifiée d'attaque armée si elle engendre des dommages considérables pour des personnes ou des objets.

Il s'agit donc de savoir si l'armée doit être engagée *dans son rôle premier* pour la défense ou *subsidiairement* pour l'appui aux autorités civiles. La réponse dépend moins de la source de l'attaque ou des moyens qu'elle utilise, mais plutôt de l'*ampleur de la menace* : si l'intensité et la portée de cette dernière sont telles que l'intégrité territoriale, la population dans son ensemble ou l'exercice du pouvoir étatique sont menacés, l'armée peut être engagée *dans son rôle premier* pour la défense. Dans un cas concret, la décision d'engager l'armée pour la défense ou dans un rôle subsidiaire revient toujours au Conseil fédéral et au Parlement.

4.2.4 Garantir la libre formation des opinions et les informations non faussées

Il est de plus en plus probable que la Suisse devienne la cible de tentatives d'influence et de désinformation. Les élections et les votations pourraient être la cible d'efforts visant à perturber ou à manipuler le processus de prise de décision politique. Cependant, plusieurs éléments indiquent que la Suisse et sa population sont relativement robustes face à ces tentatives. En plus d'une bonne éducation scolaire, qui favorise grandement les compétences médiatiques et politiques, la population suisse a l'habitude de traiter de questions politiques plusieurs fois par an lors des votations. L'organisation et le déroulement décentralisés des scrutins, ainsi que la diversité du paysage médiatique, contribuent également à la capacité du pays à résister aux tentatives d'influence extérieures.

Le Conseil fédéral informe activement, objectivement et régulièrement la population sur les activités politiques de la Suisse. Il peut corriger les informations erronées ou trompeuses, mais fait un usage modéré de cette possibilité. D'une part, les acteurs privés jouissent d'une grande liberté dans les débats politiques ; ils ne sont pas tenus de garantir l'exhaustivité, l'objectivité, la transparence et la proportionnalité de leurs propos. D'autre part, les campagnes de désinformation attirent d'autant plus l'attention si le Conseil fédéral s'en saisit. Il n'envisage donc cette possibilité que lorsqu'une campagne a pris une ampleur telle qu'elle met en péril la libre formation de l'opinion publique.

La libre formation des opinions et les informations non faussées peuvent être assurées en particulier au moyen des mesures ci-dessous.

- Les organes de *conduite de la politique de sécurité* au niveau fédéral (Délégation du Conseil fédéral pour la sécurité, Groupe Sécurité) se penchent régulièrement sur la question et, si nécessaire, soumettent aux départements ou au Conseil fédéral des mesures contre les activités d'influence. À cette fin, le Groupe Sécurité, en collaboration avec la Chancellerie fédérale, recueille régulièrement des informations afin de procéder à des *évaluations de la manière dont l'administration fédérale pourrait être affectée* par ces activités d'influence.
- Les échanges avec les *cantons* concernant la menace que représentent les activités d'influence se poursuivent.

4.2.5 Accroître la protection contre les cybermenaces

Mues par les progrès de la digitalisation et de l'intelligence artificielle, les cybermenaces évolueront de manière fulgurante. En raison de la persistance de la menace et des évolutions technologiques, il convient d'accorder une attention particulière aux interdépendances et aux vulnérabilités et de veiller à la sécurité des chaînes d'approvisionnement.

Dans sa Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, la Confédération a défini les objectifs stratégiques à poursuivre et les mesures à prendre contre les cybermenaces. L'adoption de cette stratégie a permis de clarifier les responsabilités au sein de la Confédération et de créer de nouvelles structures. Ces responsabilités se répartissent entre la cybersécurité (au DFF), la cyberdéfense (au DDPS) et la poursuite pénale de la cybercriminalité (au DFJP et dans les cantons). Afin d'améliorer la coopération interdépartementale et de renforcer la conduite, un comité cyber du Conseil fédéral a été mis en place. Il est composé des chefs du DFF, du DDPS et du DFJP, ainsi que d'un Groupe Cyber au service de ce comité. Les cantons sont également représentés dans ces organes, et un délégué fédéral à la cybersécurité a été nommé à la tête d'un nouveau centre de compétences en cybersécurité, le Centre national pour la cybersécurité (NCSC).

La collaboration avec *les cantons, l'économie et le monde scientifique* a été consolidée et institutionnalisée, notamment grâce à des échanges réguliers avec le délégué fédéral pour la cybersécurité et le NCSC. Par la création d'un campus cyberdéfense, le DDPS a mis en place une plateforme en partenariat avec les milieux scientifiques pour l'identification précoce des cybertendances, le développement de technologies contre les cybermenaces et la formation de cyberspécialistes. De plus, des organes communs de coopération entre

la Confédération et les cantons[4] ont vu le jour afin de lutter contre la *cybercriminalité* ; des formations communes sont prévues, des connaissances spécialisées ont été mises en commun et l'échange d'informations et d'expériences a été intensifié.

Dans sa stratégie actuelle de politique extérieure, le Conseil fédéral fait de la digitalisation une priorité. La Suisse s'engage au niveau international en faveur d'un *cyberespace libre, sûr et ouvert*, utilisé à des fins pacifiques et fondé sur des règles claires et une confiance mutuelle. Elle a intérêt à clarifier l'application concrète des *normes de droit international* en cas de cyberattaques, notamment en ce qui concerne les principes fondamentaux de la Charte des Nations Unies, les règles de la responsabilité internationale, le droit international humanitaire, les droits de l'homme et le droit de la neutralité. Des clarifications peuvent s'avérer nécessaires, car les cyberattaques entre parties à un conflit peuvent également affecter les infrastructures d'un État neutre du fait de la mise en réseau numérique mondiale. La Suisse veut empêcher que ses infrastructures numériques soient utilisées pour des cyberattaques contre d'autres États.

La protection contre les cybermenaces peut être renforcée en particulier au moyen des mesures ci-dessous.

- Introduction d'une *obligation d'annonce des cyberattaques sur des infrastructures critiques* afin d'améliorer la détection précoce et l'enregistrement systématique de ces attaques et d'établir une *vue d'ensemble de la situation concernant les cybermenaces* gérée par les services de renseignement, profitant également à l'économie.
- Développement et application de la SNPC, et poursuite de la mise en place et de l'extension du NCSC ainsi que des nouveaux organes fédéraux actifs dans le domaine cyber.
- Définition, par le DDPS, d'une nouvelle *stratégie de cyberdéfense* afin d'identifier les lacunes dans le dispositif de défense et de prendre des mesures supplémentaires.
- Développement de la coopération avec les *exploitants d'infrastructures critiques* afin de renforcer la protection et la résilience de ces dernières face aux cyberrisques.
- En cas de cyberattaques, conseil et déploiement de ressources du NCSC et du Service de renseignement de la Confédération ; si ces moyens sont insuffisants, l'armée peut fournir des prestations sous la forme d'un appui subsidiaire.
- Maintien et mise à profit des nouveaux organes Cyberboard et Réseau de soutien aux enquêtes relatives à la cybercriminalité pour une coopération intensive entre la Confédération et les cantons dans le domaine de la *cybercriminalité*.
- Représentation dans des organes internationaux traitant *de l'application des normes juridiques internationales* dans le cyberespace et clarification des questions ouvertes, également concernant le droit de la neutralité.
- Création d'une *division Digitalisation* au sein du DFAE et nomination d'un *représentant spécial pour la diplomatie scientifique* à Genève afin de renforcer la

[4] Cyberboard : organe réunissant toutes les autorités cantonales et fédérales de poursuite pénale participant à la lutte contre la cybercriminalité et les représentants de la prévention contre les cybermenaces. Réseau de soutien aux enquêtes relatives à la cybercriminalité : plateforme gérée par les polices cantonales et l'Office fédéral de la police (fedpol).

capacité de la Suisse à façonner les développements internationaux dans le domaine de la digitalisation.

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

La lutte contre le terrorisme, l'extrémisme violent, le crime organisé et les autres formes de criminalité transnationale reste une priorité. La Suisse combat ces menaces par la prévention et la répression grâce à une étroite collaboration entre les autorités fédérales et cantonales compétentes et les autorités étrangères partenaires. Sur la base d'une appréciation de la menace, une *stratégie de lutte contre la criminalité* est définie et actualisée[5]. Il existe également une *stratégie nationale de lutte contre le terrorisme* qui est régulièrement mise à jour.

Dans la lutte contre l'extrémisme violent et le terrorisme, la *détection précoce* de telles menaces et l'*identification des possibles fauteurs de troubles et des personnes à risque* jouent un rôle crucial. En plus des groupes connus, l'accent est mis sur les auteurs radicalisés agissant de manière autonome. Il s'agit également de tenir compte de la distinction entre terrorisme et extrémisme violent qui, dans la réalité, est parfois fluide. Le *Plan d'action national de lutte contre la radicalisation et l'extrémisme violent*, adopté par la Confédération et les cantons en 2017, sert également à prévenir la radicalisation et prévoit des mesures de prévention dans les domaines de la politique sociale et de l'éducation. Les services fédéraux et cantonaux chargés de la lutte contre le terrorisme et l'extrémisme violent consolident en permanence leur coopération pour tenir compte du caractère interdisciplinaire des menaces. Le programme TETRA (*Terrorist Tracking*), dans lequel les autorités fédérales et cantonales collaborent étroitement sous la direction de l'Office fédéral de la police (fedpol), revêt un rôle important.

Une coopération et une coordination étroites entre la Confédération et les cantons sont également essentielles dans la lutte contre le crime organisé. Sous la dénomination *Countering Organised Crime*, l'échange d'informations et d'expériences a été intensifié entre diverses autorités telles que les polices cantonales, fedpol, le Service de renseignement de la Confédération, le Ministère public de la Confédération et l'AFD, mais aussi les services sociaux, les autorités compétentes en matière de migration, les autorités financières et fiscales ainsi que les autorités responsables de la surveillance des marchés, des registres et de la concurrence.

Le terrorisme et la grande criminalité sont des menaces agiles, interconnectées et transnationales. La Suisse dépend donc d'une *coopération policière internationale* efficace. L'accord d'association à Schengen et le *Système d'information Schengen* constituent les instruments de coopération majeurs. D'autres systèmes d'information de l'UE[6] concernant la sécurité et la migration sont en cours de développement ; à l'avenir,

[5] La stratégie du DFJP de lutte contre la criminalité 2020 – 2023 définit trois priorités : le terrorisme, la criminalité organisée et les autres formes de criminalité transnationale. Elle repose sur les trois piliers de la prévention, de la coopération et de la répression et suit trois principes : pilotage des forces de police fondé sur l'analyse ; intégration du secteur privé ou d'autres secteurs extérieurs à la police ; repérage des flux d'argent acquis par des moyens criminels.

[6] Système d'information sur les visas, système européen d'information et d'autorisation concernant les voyages, système d'entrée/de sortie EES, système API (*Advance Passenger Information*), système FADO (Faux documents et documents authentiques en ligne).

les informations issues des différents systèmes seront mises en réseau, ce qui permettra aussi aux autorités suisses de contrôle des frontières, de migration et de police d'y accéder plus rapidement.

Fournissant des analyses et des plateformes opératives pour lutter contre la criminalité transnationale, *Europol* et *Interpol* sont des instruments très utiles pour la Suisse. Cette dernière coopère également avec l'ONU, l'OSCE et le Conseil de l'Europe en vue de renforcer et de développer la lutte contre la criminalité. Cette coopération multilatérale est complétée par des *traités bilatéraux de police*[7], le réseau des attachés de police, les personnes de liaison de l'AFD et les deux centres de coopération policière et douanière avec l'Italie et la France.

Afin de lutter efficacement contre la *criminalité transfrontalière, notamment la contrebande de drogues, d'armes, de médicaments, de contrefaçons, de biens culturels et de substances interdites*, l'AFD effectue des contrôles quotidiens des biens et des personnes aux frontières et à l'intérieur du pays, et mène des activités de poursuite pénale ciblées. Avec le *programme de transformation DaziT*, les processus de l'AFD sont numérisés et simplifiés afin de réduire les tâches administratives des employés et de pouvoir les affecter à davantage de tâches de contrôle grâce à un développement organisationnel, notamment un profil professionnel plus flexible[8].

La prévention du terrorisme, de l'extrémisme violent, du crime organisé et d'autres formes de criminalité transnationale peut être renforcée en particulier au moyen des mesures ci-dessous.

- Amélioration de l'*échange international d'informations policières* en adoptant les développements de l'acquis de Schengen et en concluant des accords bilatéraux de police.
- Création de moyens de prévention supplémentaires afin de gérer les possibles fauteurs de trouble et les personnes à risque avec la *loi fédérale sur les mesures policières de lutte contre le terrorisme*.
- Consolidation des instruments de prévention et de lutte contre le terrorisme et la grande criminalité par la création de la *loi fédérale sur la collecte et le traitement par la Suisse des données des dossiers passagers* (données PNR, pour *Passenger Name Record*).
- *Association avec les accords de Prüm* pour une comparaison automatique avec l'étranger des empreintes digitales, des profils ADN et des données sur les détenteurs de voitures, afin de faciliter la recherche de personnes.
- Participation à l'élargissement du mandat de l'agence *Frontex* afin de mieux protéger les frontières extérieures de Schengen et de lutter contre la criminalité transfrontalière.
- Transformation de l'AFD en *Office fédéral de la douane et de la sécurité des frontières*, qui reposera sur des processus de protection des frontières numérisés et une flexibilité en matière de personnel pour des détachements, afin d'assurer un contrôle

[7] Ces accords permettent des formes de coopération transfrontalière comme des observations en commun, des contrôles de livraison, la poursuite d'auteurs, des investigations secrètes ou des patrouilles mixtes.

[8] La nouvelle fonction de spécialiste en douane et sécurité des frontières remplace les deux fonctions de douanier et de garde-frontière.

approfondi de trois domaines cruciaux pour l'AFD, soit des personnes, des marchandises et des moyens de transport.

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

Afin d'être prête à contrer les effets directs et indirects des tensions et des crises internationales, la Suisse doit continuer à renforcer sa propre résilience, son adaptabilité et sa capacité de régénération. Elle met l'accent sur le *renforcement de la sécurité d'approvisionnement*. En Suisse, le secteur privé est le premier responsable de l'approvisionnement du pays en biens et services essentiels. Pour l'assurer même lors de crises, des chaînes d'approvisionnement stables et diversifiées sont nécessaires dans les domaines d'importance systémique (p. ex. l'alimentation, l'approvisionnement en énergie et la santé). La crise de COVID-19 a illustré des problèmes d'approvisionnement surtout structurels en période de pénurie, notamment dans les domaines des médicaments et des dispositifs médicaux. Pour réduire l'impact des retards de livraison, la flexibilité des entreprises et la coopération internationale sont déterminantes.

L'objectif est également de *réduire la dépendance pour l'équipement et l'armement de l'armée*. La Suisse doit tenir compte de cet aspect plus que d'aucuns car, en tant que pays neutre, elle ne peut pas tabler sur le soutien militaire d'autres États. L'autosuffisance en armement est impossible pour la Suisse. Cependant, dans l'intérêt de maintenir le plus haut degré d'autonomie possible, même en situation de crise, la Suisse s'efforce de réduire sa dépendance en matière d'armement vis-à-vis de l'étranger – du moins dans certains domaines – ou d'instaurer une relation d'interdépendance et de maintenir une base industrielle pertinente pour la politique de sécurité suisse. À cette fin, la Confédération soutient le développement technologique, principalement dans les instituts de recherche civils et les entreprises privées ayant des compétences pertinentes, par exemple dans les technologies de communication ou les capteurs.

Les services spatiaux tels que la *navigation ou la communication par satellite* sont déjà très répandus aujourd'hui et prendront encore de l'importance pour les États, l'économie et la société. Or, plus l'utilisation de ces services croît, plus il est fondamental de réduire les dépendances et d'augmenter la résilience face aux pannes ou aux perturbations.

Ces dernières années, les investissements directs étrangers ont suscité des craintes quant à la perte d'emplois et de savoir-faire et à la mise en péril de la sécurité nationale. En principe, la politique d'ouverture de la Suisse à l'égard des investissements étrangers favorise la place économique suisse par l'afflux de capitaux et de connaissances, contribuant ainsi à la création de valeur, à l'avance technologique ainsi qu'au maintien et à la création d'emplois. En mars 2020, le Parlement a toutefois chargé le Conseil fédéral de créer une base légale pour le contrôle des investissements étrangers.

La résilience et la sécurité d'approvisionnement en cas de crises internationales peuvent être renforcées en particulier au moyen des mesures ci-dessous.

- Vérification et réduction des dépendances au niveau de *l'approvisionnement en biens et en prestations critiques et de première nécessité*, sur la base des enseignements tirés de la pandémie de COVID-19.

- Renforcement de la *base technologique et industrielle liée à la sécurité* par des acquisitions en Suisse, des affaires compensatoires, la coopération internationale, la recherche appliquée, la promotion de l'innovation, l'échange d'informations avec l'industrie et la politique de contrôle des exportations, en tenant compte des intérêts de la politique de sécurité.
- Consolidation de l'*accès à des services utilisant l'espace* pour la communication, la navigation et l'observation de la Terre, affermissement de l'engagement international en faveur du renforcement de l'utilisation durable et pacifique de l'espace extra-atmosphérique.
- Élaboration d'une base légale pour le *contrôle des investissements étrangers* (procédure de consultation prévue pour le deuxième semestre 2021).

4.2.8 Améliorer la protection contre les catastrophes, la préparation aux situations d'urgence et la capacité de régénération

La protection de la population est l'instrument principal pour *maîtriser les risques naturels, technologiques et sociétaux*. La révision totale de la loi fédérale sur la protection de la population et sur la protection civile vise une orientation encore plus systématique vers la gestion des catastrophes et des situations d'urgence.

En cas d'événements extrêmes tels qu'un tremblement de terre ou une pandémie, les *installations sanitaires protégées* pourraient également être utilisées. Cependant, les installations existantes ne répondent pas entièrement aux exigences et aux normes actuelles. Sous la direction de l'Office fédéral de la protection de la population, des projets sont en cours pour rendre leur utilisation possible.

Une gestion réussie des événements nécessite une *communication et une transmission de données sécurisées et affichant une disponibilité élevée*, notamment entre les organisations partenaires de la protection de la population. Ces dernières années, divers projets ont été lancés pour moderniser l'infrastructure télématique et les systèmes associés. Il s'agit notamment du réseau de sécurité Polycom et du système d'échange de données sécurisé. De plus, un projet pilote est en cours pour éventuellement introduire un système de communication mobile de sécurité à large bande.

Dans le cadre de la *gestion intégrale des risques*, l'Office fédéral de la protection de la population prépare une analyse systématique des risques naturels, technologiques et sociétaux. Elle servira à déduire des mesures de prévention, de protection et de préparation à l'engagement afin de réduire les vulnérabilités et l'étendue potentielle des dommages. Ces mesures comprennent l'aménagement du territoire et des constructions techniques, par exemple en établissant des cartes de dangers et en construisant des structures de protection contre les crues.

L'Office fédéral de l'environnement soutient les cantons dans la planification et l'application de *mesures de protection* contre les crues et les éboulements, les glissements de terrain et les avalanches, ainsi que dans l'élaboration de données de base sur les dangers. Une surveillance globale en vue d'une gestion intégrale des risques soutient la *détection précoce des risques naturels nouveaux et changeants*. Les scénarios climatiques actuels peuvent être utilisés pour quantifier les effets du changement climatique, permettant des prédictions sur les événements extrêmes.

La protection contre les catastrophes, la préparation aux situations d'urgence et la capacité de régénération peuvent être renforcées en particulier au moyen des mesures ci-dessous.

- Clarification du *besoin en constructions protégées* (postes de commandement pour les organes de conduite, postes d'attente pour la protection civile, constructions protégées pour le système de santé) et définition de normes pour la mise en place, l'entretien, l'exploitation et le personnel.
- *Mise à jour des concepts de protection* de la population, par exemple dans le cas de la protection contre les dangers atomiques, biologiques ou chimiques, où les compétences et les services doivent être définis et les lacunes identifiées.
- Poursuite des travaux fondés sur les *scénarios climatiques actuels* pour évaluer les effets sur les crues, les glissements de terrain, les processus de chute et les avalanches ainsi que sur la forêt protectrice.
    - Exploitation d'un *système global de surveillance des processus de dangers naturels*, comprenant les analyses radar par satellite de l'instabilité gravitaire et des développements, ainsi qu'exploitation et consolidation *des alertes en cas de danger naturel* par les services fédéraux spécialisés réunis dans le comité de direction Intervention dangers naturels (LAINAT).

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

Vu l'interconnexion et le renforcement mutuel des menaces et des dangers, la coopération entre les domaines politiques et les instruments pertinents revêt une importance croissante. En raison du fédéralisme de la Suisse et de l'organisation de son gouvernement en départements, une bonne coordination des autorités et des ressources de la Confédération, des cantons et des communes est particulièrement importante. L'application du principe de subsidiarité en cas d'événements majeurs liés à la sécurité nécessite précisément l'*utilisation combinée de plusieurs instruments*.

Depuis des années, le *Réseau national de sécurité* sert de plateforme de dialogue et de coordination entre les différents niveaux et autorités actifs dans le domaine de la sécurité. Ses organes ne sont toutefois pas conçus comme des organes de gestion de crise. Il en va de même pour les organes fédéraux de *conduite de la politique de sécurité*, à savoir le *Groupe Sécurité* et la *Délégation pour la sécurité du Conseil fédéral*[9]. Ces organes servent à l'appréciation permanente de la situation en matière de sécurité, à la coordination des affaires interdépartementales et à la consultation préalable de ces dossiers afin de soutenir la prise de décision du Conseil fédéral. Ils peuvent toutefois jouer un rôle d'appui dans la gestion de crise si l'un des départements représentés en assume la responsabilité sur la base de sa spécialisation. Par exemple, si la Suisse devait être victime d'une cyberattaque majeure contre ses infrastructures critiques, le *Groupe Cyber* pourrait faciliter la coordination des opérations au profit du département responsable.

[9] Directives du 2 décembre 2016 sur l'organisation de la conduite de la politique de sécurité du Conseil fédéral (FF 2016 8513). La Délégation pour la sécurité du Conseil fédéral se compose de la cheffe du DDPS (présidence), du chef du DFAE et de la cheffe du DFJP. Le Groupe Sécurité se compose quant à lui de la secrétaire d'État du DFAE, du directeur du SRC et de la directrice de fedpol.

En situation de crise, les décisions doivent être prises rapidement et les processus rationalisés. Il est donc essentiel de disposer du chemin le plus court possible vers l'organe de décision politique, le Conseil fédéral. La *gestion de crise au niveau fédéral* doit tenir compte de la structure départementale du gouvernement. En la matière, la Confédération confie la *responsabilité* des opérations et la préparation des décisions à l'intention du Conseil fédéral au département le plus affecté et disposant des ressources, des compétences décisionnelles et de l'expertise nécessaires pour faire face à une situation de crise spécifique. Un *état-major sur mesure adapté aux exigences de la situation* est alors formé au niveau départemental, qui peut être complété par un *état-major opérationnel* – par exemple l'État-major fédéral Protection de la population ou l'organisation d'intervention de fedpol. En outre, les cantons et des experts scientifiques doivent être impliqués dans les processus. La *communication de crise* au niveau fédéral relève de la responsabilité du chef du département responsable ou du président de la Confédération ainsi que du porte-parole du Conseil fédéral.

La pratique a confirmé la pertinence de ces principes. Les états-majors de crise supérieurs, en place en permanence et qui ne sont pas intégré dans un département, ne se sont pas montrés efficaces du fait du manque d'expertise et de l'absence d'accès direct à la direction du département, qui peut adresser des demandes au Conseil fédéral, et en raison de l'absence d'intégration dans les processus décisionnels [10].

Compte tenu de l'instabilité de la situation et de la nature imprévisible des événements, la préparation et la gestion des crises ont gagné en importance ces dernières années. La collaboration entre les autorités fédérales, cantonales et communales dans la gestion de crises de toute nature doit donc continuer à être entraînée et améliorée lors d'*exercices réguliers*, comme lors des exercices de conduite stratégiques (ECS) en 2013 et en 2017 et du Réseau national de sécurité (ERNS) en 2014 et en 2019.

Il est tout aussi important de tirer les leçons des *crises réelles*. À cette fin, le Conseil fédéral a évalué la gestion de crise de la Confédération lors de la première vague (février à août 2020) de la pandémie de COVID-19. Il est apparu que le rôle des membres des états-majors et leurs relations mutuelles devaient être plus clairement réglés. Le Conseil fédéral souligne toutefois que plusieurs états-majors continueront d'être nécessaires aux niveaux stratégique et opérationnel. Pour les raisons mentionnées, un état-major unique qui serait responsable de toutes les affaires n'est pas judicieux, car l'expertise ferait défaut et il serait trop éloigné des directions des départements et exclu des processus décisionnels établis.

La gestion de crise et la collaboration entre la Confédération et les cantons lors d'une attaque terroriste ou une pandémie sont mieux établies que par le passé, grâce à des exercices, à des préparations et à des événements réels. Cependant, les crises peuvent avoir différents visages, notamment en raison de la nature hybride des conflits, et il importe d'appliquer les enseignements tirés des expériences passées pour gérer toutes sortes d'événements. Par conséquent, les membres des états-majors de crise départementaux et interdépartementaux ne doivent pas seulement être formés lors d'*exercices*, mais également recevoir une *formation continue* afin de pouvoir travailler selon les mêmes processus et méthodes – et avec efficacité – en cas de crise.

[10] Comme le cas de l'ancienne Délégation du Conseil fédéral pour la sécurité l'a illustré ; pour les raisons mentionnées, elle n'a pas pu apporter satisfaction et a été dissoute en 2011.

Enfin, une gestion de crise fructueuse exige que tous les instruments de la politique de sécurité soient opérationnels, y compris ceux qui reposent entièrement ou partiellement sur le *système actuel de l'obligation de servir* : armée, service civil de remplacement, protection civile et corps de sapeurs-pompiers. Pour que ces ressources soient utilisées efficacement, l'armée et la protection civile doivent disposer d'effectifs suffisants. Or, le recrutement dans la protection civile est en forte baisse depuis des années, et les effectifs de l'armée ne sont pas non plus assurés à moyen terme au vu des nombreux départs anticipés. Parallèlement, le système de l'obligation de servir doit s'adapter aux évolutions et aux besoins de la société, accordant une importance majeure à la compatibilité entre le travail, la famille et le service obligatoire.

La collaboration entre les autorités et les acteurs de la gestion de crise peut être renforcée en particulier au moyen des mesures ci-dessous.

- Vérification des *bases de la gestion de crise* en ce qui concerne les événements de longue durée, en particulier le rôle et la composition de l'état-major fédéral Protection de la population, de l'état-major de crise interdépartemental compétent au niveau du Conseil fédéral pour les événements affectant la protection de la population, et des états-majors de crise départementaux.
- Clarification et délimitation des tâches, des compétences et des responsabilités de la *Confédération et des cantons* en matière de processus, de contacts et d'interlocuteurs sur la base des enseignements tirés de la crise de COVID-19.
- Meilleure intégration des *expertises externes à la Confédération* dans sa gestion de crise, issues par exemple de la communauté scientifique, et meilleur contrôle de l'*approvisionnement en biens et produits médicaux* pendant une pandémie sur la base des enseignements tirés de la pandémie de COVID-19.
- Mise en avant et promotion de la *digitalisation*, notamment en accélérant les travaux de transmission et de traitement simplifiés des informations et d'amélioration de la comptabilité des systèmes.
- *Amélioration des effectifs* de la protection civile et de l'armée, par exemple en favorisant la convergence entre le service civil et la protection civile et en améliorant la compatibilité entre le service militaire et la vie civile ; amorce d'une discussion sur l'évolution du système de l'obligation de servir.

5 Conclusion

La Suisse est un pays sûr. Pour qu'elle le reste, il faut continuer et même intensifier nos efforts. L'environnement sécuritaire est moins stable qu'il y a dix, ou même vingt ans. Des événements survenant dans des régions éloignées peuvent avoir des répercussions immédiates sur la Suisse. De nouveaux dangers et menaces sont apparus sans que les précédents aient disparu. Les cyberattaques et la désinformation, par exemple, sont des phénomènes qui sont devenus en quelques années des menaces sérieuses pour l'État, l'économie et la société. Au vu cette situation, un suivi permanent et attentif de la situation, ouvert aux nouvelles observations, est essentiel comme base d'une appréciation indépendante qui servira de pierre de voute des mesures à prendre.

Les principes et intérêts de la politique de sécurité de la Suisse se caractérisent par leur constance. Celle-ci favorise la prévisibilité de la Suisse dans un monde qui est, lui, devenu

moins prévisible. Néanmoins, il convient de revoir périodiquement la politique de sécurité dans son ensemble. En effet, sa définition doit être adaptée à l'évolution des défis et prioriser les ressources en fonction. La pertinence de la politique de sécurité et de ses instruments se mesure à son efficacité contre les menaces et les dangers et à sa facilité à saisir les opportunités. Des révisions et des adaptations sont régulièrement nécessaires, mais elles doivent être amorcées avec prudence, a fortiori si elles concernent le personnel de milice, et elles doivent impliquer la Confédération, les cantons et les communes.

Le Conseil fédéral est convaincu que la politique de sécurité exposée dans le présent rapport est apte à assurer la sécurité de la Suisse et de sa population dans un monde peu sûr, que ce soit du point de vue de ses principes, de ses intérêts, de ses objectifs, ou encore des mesures concrètes proposées.