



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra










Service de renseignement de la Confédération SRC

LA SÉCURITÉ DE LA SUISSE



Rapport de situation du Service de renseignement de la Confédération

2026

ÉDITORIAL	5	
LE RAPPORT EN BREF	7	
ENVIRONNEMENT STRATÉGIQUE	13	
TERRORISME	35	
EXTRÉMISME VIOLENT	45	
PROLIFÉRATION	51	
ESPIONNAGE	59	
MENACE CONTRE LES INFRASTRUCTURES CRITIQUES	65	
CHIFFRES CLÉS 2025	73	
<i>TABLE DES ILLUSTRATIONS</i>	<i>84</i>	

ALERTE MAINTENUE !

Chère lectrice, cher lecteur,

Dans sa Stratégie en matière de politique de sécurité 2026, le Conseil fédéral constate que la situation sécuritaire de la Suisse s'est nettement détériorée. Cette appréciation s'appuie surtout sur les connaissances acquises par le Service de renseignement de la Confédération (SRC), dont bon nombre se trouvent mises en lumière dans «La Sécurité de la Suisse 2026». Alerte maintenue! Ces deux mots résument à eux seuls le rapport que vous tenez entre les mains. Dans le même temps, celui-ci montre comment le SRC s'engage activement pour la sécurité de notre pays et fournit ses prestations.

Pour la Suisse, la menace la plus sérieuse émane de la Russie, elle qui poursuit sa guerre d'agression contre l'Ukraine. Le conflit hybride qu'elle mène contre l'Europe gagne en agressivité, et la Suisse s'en trouve directement concernée. Aux rivalités et tensions entre grandes puissances s'ajoutent les incertitudes liées à l'engagement américain pour la sécurité européenne ainsi que les crises et conflits en recrudescence à la périphérie de l'Europe qui se traduisent par des menaces dans le domaine du terrorisme et de l'extrémisme violent. Afin de protéger la société et l'État, la politique suisse en matière de sécurité doit tenir compte de ce contexte politico-sécuritaire, et sous toutes ses facettes.



Serge Bavaud
Directeur du Service de
renseignement de la Confédération

Le SRC joue un rôle critique lorsqu'il s'agit d'empêcher et de contrer des menaces qui relèvent de la politique de sécurité. La notion de «première ligne de défense» ne sort pas de nulle part. Afin que le SRC puisse continuer à exercer cette fonction, il a besoin de compétences qui soient adaptées à l'évolution de la situation sécuritaire. Avec les mesures qu'elle comprend, la Stratégie en matière de politique de sécurité 2026 vise justement à améliorer les capacités en matière de renseignement, afin d'identifier les menaces aussi tôt que possible et de les éviter. La révision actuelle de la loi fédérale sur le renseignement (LRens), qui date de 2017, vise à mettre à jour ces compétences. Son objectif est d'assurer que la première ligne de défense de la Suisse soit toujours aussi efficace à l'avenir également.

Comme l'illustre l'appréciation de la situation du SRC, le prix de notre sécurité et de notre autonomie augmente, un enjeu sur lequel le présent rapport apporte un éclairage aussi solide que précieux.





LE RAPPORT EN BREF



L'environnement en matière de politique de sécurité et la situation sécuritaire de la Suisse se sont nettement détériorés. La Russie reste la menace la plus sérieuse et la plus aiguë pour la sécurité, la stabilité et la paix en Europe. La tendance stratégique globale la plus importante est la rivalité systémique entre les États-Unis et la Chine, même si les États-Unis ont repositionné leur politique étrangère et leur politique de sécurité. Comme la Chine et la Russie, ils suivent désormais une logique davantage imprégnée de l'idée de sphères d'influence. Ce faisant, ils affaiblissent l'ordre mondial fondé sur des règles, que l'Europe continue, elle, à défendre.

Malgré des difficultés économiques croissantes, le système Poutine s'avère stable. La **Russie** poursuit ainsi sa guerre d'agression contre l'Ukraine pour la cinquième année consécutive, et il ne se profile ni accord de cessez-le-feu stable ni accord de paix durable. Depuis qu'elle a attaqué l'Ukraine en 2022, la Russie brandit de surcroît la menace nucléaire. En Europe, elle a fortement intensifié son conflit hybride, en particulier au moyen d'activités de sabotage, mais aussi d'influence. Elle veut ainsi mettre à l'épreuve l'article 5 du Traité de l'Atlantique Nord, tout en affaiblissant les démocraties occidentales et l'unité transatlantique. Pour sa part, l'OTAN considère qu'une attaque de la Russie contre un État membre est un développement réaliste d'ici à la fin de la décennie en cours, raison pour laquelle elle développe sa capacité de défense en conséquence. La question de savoir de combien de temps l'Europe dispose pour être concrètement en mesure de se défendre contre la Russie dépend de plusieurs facteurs, à savoir pour l'essentiel, la crédibilité de la dissuasion de l'OTAN, le positionnement des États-Unis vis-à-vis de cette dernière et le cours que prendra la guerre contre l'Ukraine. Les délais de préalerte pour une guerre contre un membre européen de l'OTAN se sont considérablement raccourcis.

La **Chine** travaille à un nouvel ordre mondial, axé sur ses propres intérêts. Signe de tensions

accrues, elle se sert des dépendances occidentales à son égard comme moyens de pression. Ayant fait de la Russie son premier partenaire politique, elle joue un rôle clé dans la poursuite de la guerre contre l'Ukraine. Son ambition de devenir la plus grande puissance économique, technologique et militaire au monde se traduit par un accroissement de la menace hybride qu'elle représente. Plusieurs États occidentaux poursuivent désormais des stratégies visant à réduire leurs vulnérabilités économiques à son égard et à renforcer leur propre résilience. L'UE considère la Chine comme un partenaire commercial, mais aussi comme un rival systémique. Il existe toutefois des dépendances économiques réciproques, raison pour laquelle les relations sino-européennes restent relativement stables en dépit de la situation politique tendue.

Avec son idée d'un nouvel ordre mondial, la **Chine** courtise et séduit. Son rapprochement avec la **Russie, l'Iran et la Corée du Nord** s'appuie sur le rejet de l'ordre marqué par les conceptions occidentales. Ces quatre États ne forment cependant pas une alliance militaire, et leur collaboration est marquée par des divergences, voire de la méfiance. Politiquement parlant, la Corée du Nord n'est plus aussi isolée que par le passé. Vis-à-vis de son partenaire commercial majeur qu'est la Chine, elle a gagné en marge de manœuvre, tout en intensifiant encore sa collaboration avec la Russie. La Corée du Nord poursuit son programme nucléaire et produit toujours de l'uranium enrichi et du plutonium. La Chine, tout comme la Russie, essaient par ailleurs de rallier les États du Sud global à leurs intérêts.

La **guerre en Iran** et l'escalade régionale qui y est liée mènent à un nouvel affaiblissement de l'«axe de la résistance» dirigé par l'Iran, mais aussi à une déstabilisation régionale plus étendue. Dans cette guerre, l'Iran n'a pas reçu de soutien politique ou militaire décisif, ni de la part de la Russie, ni de la part de la Chine. Les événements les plus récents ont pour toile de fond une longue série de

conflits non résolus au Proche et Moyen-Orient, en particulier entre Israël et les Palestiniens, en Irak, au Yémen, au Liban et en Syrie. La stabilité des pays du Golfe s'est vue ébranlée par la guerre en Iran, qui a aussi intensifié les tensions entre les États-Unis et leurs alliés européens en matière de politique de sécurité. Le blocage du détroit d'Ormuz a conféré à cette guerre une dimension supplémentaire, puisque ses conséquences économiques et politico-sécuritaires sont d'ordre mondial et qu'elles se traduiront dans la durée. Il faudra également compter avec des restrictions supplémentaires qui toucheront la production mondiale de biens militaires rares, en particulier dans les domaines de la défense aérienne et de la défense anti-drones.

À l'instar de la Chine et de la Russie, les **États-Unis** aspirent à apporter des changements à l'ordre mondial. L'administration américaine veut se concentrer sur la politique intérieure et l'«hémisphère occidental», relativisant de ce fait les rivalités stratégiques avec la Chine et la Russie dans ses documents programmatiques. Vis-à-vis de l'Europe, le propos se durcit par moments, prenant alors des accents de combat de civilisation. Globalement toutefois, la politique américaine en matière d'affaires étrangères et de sécurité est pour l'heure fortement marquée par la personnalité du président. Au gré de l'évolution de la situation, elle continue de revêtir des traits clairement mondialistes, hégémoniques et interventionnistes, tout en portant l'exigence que l'Europe assume désormais seule la responsabilité de sa propre sécurité.

Dans les années à venir, l'**Europe** veut réduire sa dépendance vis-à-vis de la Chine, comme décrit ci-dessus, mais aussi vis-à-vis des États-Unis. Les investissements de l'UE en matière de défense ont fait un saut quantique en 2025. Le chemin vers une Europe post-américaine reste toutefois long. Sa défense et sa capacité de dissuasion restent dépendantes des compétences militaires de pointe des États-Unis, qui

s'avèrent critiques, et les investissements européens consentis pour la recherche sont largement inférieurs aux investissements américains. Quant à la fragmentation du marché européen de l'armement, elle réduit l'efficacité du réarmement militaire qui s'est amorcé.

Les tendances mondiales impliquent des menaces et des attaques contre la Suisse:

- Les actions de sabotage s'inscrivent dans le conflit hybride mené par la Russie contre l'Europe. Des activités d'espionnage, des cyberattaques et des activités d'influence sont aussi menées contre la Suisse. Jusqu'à présent toutefois, aucun sabotage n'a été perpétré contre les **infrastructures critiques** suisses. La Suisse est toutefois susceptible de subir à tout moment des dommages collatéraux de telles actions commises à l'étranger, tandis que des infrastructures critiques en Suisse pourraient se voir sabotées pour nuire aux États ou aux alliances qui en dépendent.
- La Suisse est particulièrement touchée par les efforts de la Russie en matière de **prolifération**. La Chine tente quant à elle de se procurer des avantages en Suisse dans le cadre de la rivalité pour la suprématie technologique: la place de recherche suisse constitue une cible attrayante à ses yeux. En prenant des mesures destinées à lutter contre la prolifération et l'espionnage, la Suisse sécurise les connaissances et contribue à renforcer l'Occident dans la préparation de sa défense. En l'absence de telles mesures, la Suisse s'exposerait à des tentatives de pression, voire à une intervention directe comportant des sanctions de la part d'États occidentaux.
- Les facteurs qui favorisent l'**espionnage** en Suisse restent stables. La menace liée à l'espionnage en général est très élevée. Les services de renseignement étrangers continuent de s'intéresser à une multitude de thématiques et de domaines, parmi lesquels figurent en priorité la politique étrangère,

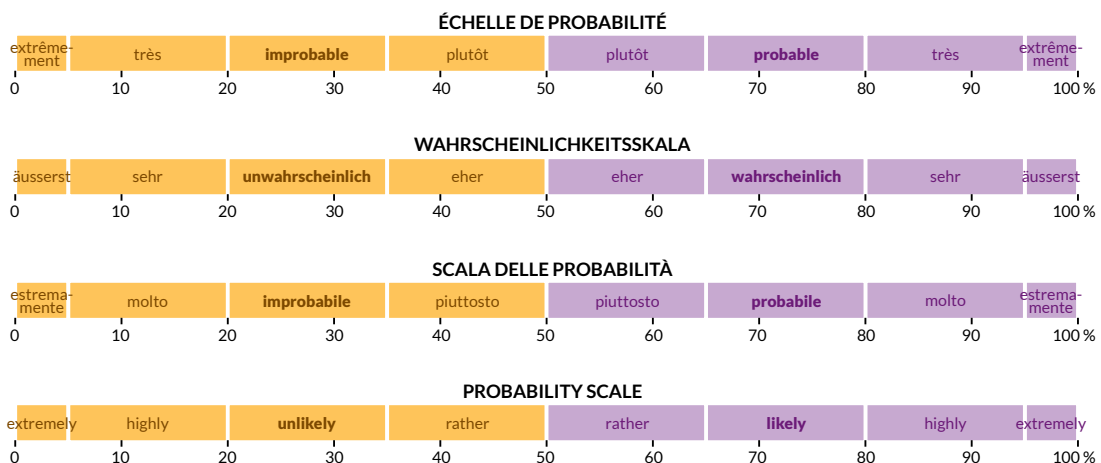
la politique commerciale et la politique de sécurité, mais aussi les capacités de l'armée, l'industrie de l'armement et la recherche de pointe ainsi que des organisations, des groupes ou des personnes qui sont vus comme des menaces. Des autorités, des organisations et des personnes sont espionnées par des sources humaines, mais aussi au moyen de cyberattaques. La menace principale en matière d'espionnage émane de la Russie et de la Chine.

- En Suisse, la **menace terroriste** reste avant tout marquée par le mouvement djihadiste, principalement par des sympathisants de l'«État islamique» ou des personnes inspirées par la propagande djihadiste. L'attaque au couteau commise le 28 mai 2026 à Winterthur par un individu radicalisé confirme cette appréciation. La menace terroriste demeure élevée, ce qui signifie qu'il y a des informations sur des acteurs terroristes en Suisse et/ou sur des intentions terroristes contre la Suisse. Elle devient de plus en plus diffuse. Le phénomène de la radicalisation en ligne reste virulent. La dynamique persistante des conflits au Proche et Moyen-Orient accroît la probabilité d'actes de violence contre des intérêts juifs, israéliens ou américains en Europe. Cela est valable pour la Suisse également. Les lieux difficiles

à protéger dans l'espace public ainsi que les rassemblements de personnes à l'occasion d'événements sportifs ou culturels restent exposés en tant que potentielles cibles d'attentat. La guerre en Iran a en outre des conséquences directes sur la menace terroriste en Europe et en Suisse. Les acteurs qui sont potentiellement susceptibles de passer à l'acte sont en majorité extérieurs au spectre djihadiste. Il s'agit notamment de partisans ou de sympathisants de l'Iran, d'acteurs entretenant des relations proches avec ce pays, de sympathisants du Hamas, ou de criminels spécialement recrutés et rémunérés pour commettre des attentats.

- L'**extrémisme violent** menace également la Suisse. Le potentiel de violence des milieux d'extrême gauche violents demeure élevé. Outre l'antifascisme, les causes kurde et palestinienne font partie des principaux sujets pour lesquels ils s'engagent. La menace émanant des extrémistes de droite violents persiste également. Les milieux d'extrême gauche et d'extrême droite violents poursuivent leurs activités et les développements observés ces dernières années se confirment. À l'avenir, ils resteront essentiellement axés sur les priorités thématiques qu'ils ont suivies jusqu'à présent.

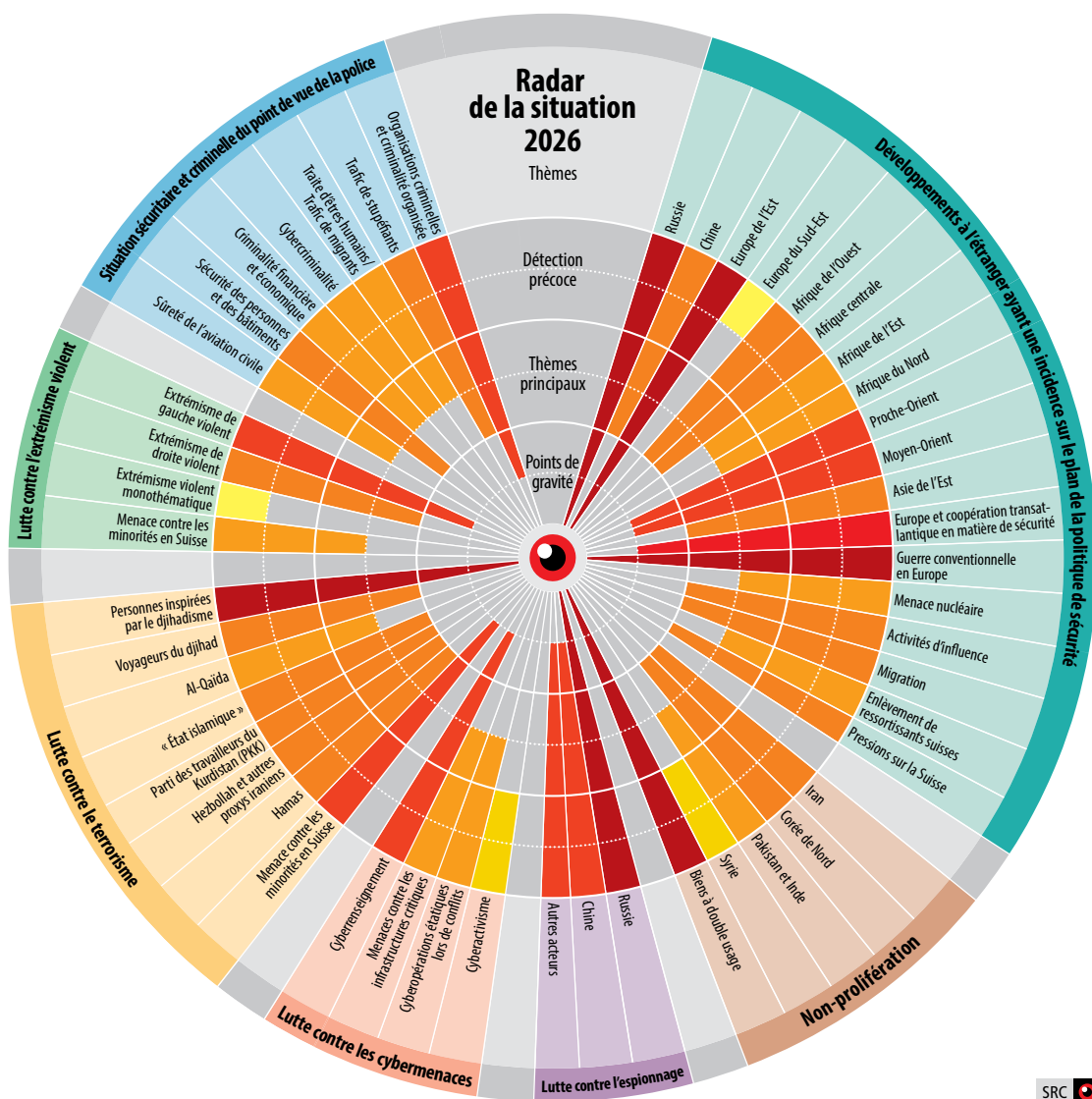
Aperçu des indications de probabilité utilisées dans ce rapport



LE RADAR DE LA SITUATION

Le SRC utilise l'instrument du radar de la situation pour présenter les menaces importantes qui pèsent sur la Suisse. Dans sa version simplifiée, sans données confidentielles, il est une des composantes du présent rapport. Cette version

publique contient les menaces qui relèvent du domaine d'activité du SRC et de l'Office fédéral de la police. Le présent rapport n'aborde pas les thèmes traités par d'autres organes fédéraux, mais il renvoie à leurs évaluations.





ENVIRONNEMENT STRATÉGIQUE



TENDANCES GLOBALES



La Russie reste la menace la plus sérieuse et la plus aiguë pour la sécurité, la stabilité et la paix en Europe. Comme en attestent les cyberattaques, les actes de sabotage, les violations de l'espace aérien et les activités d'influence, ainsi que, probablement, les mystérieux incidents impliquant des drones, la Russie a fortement intensifié son conflit hybride en Europe.

La Russie a fortement intensifié son conflit hybride en Europe. La Suisse est directement touchée par ce conflit hybride.

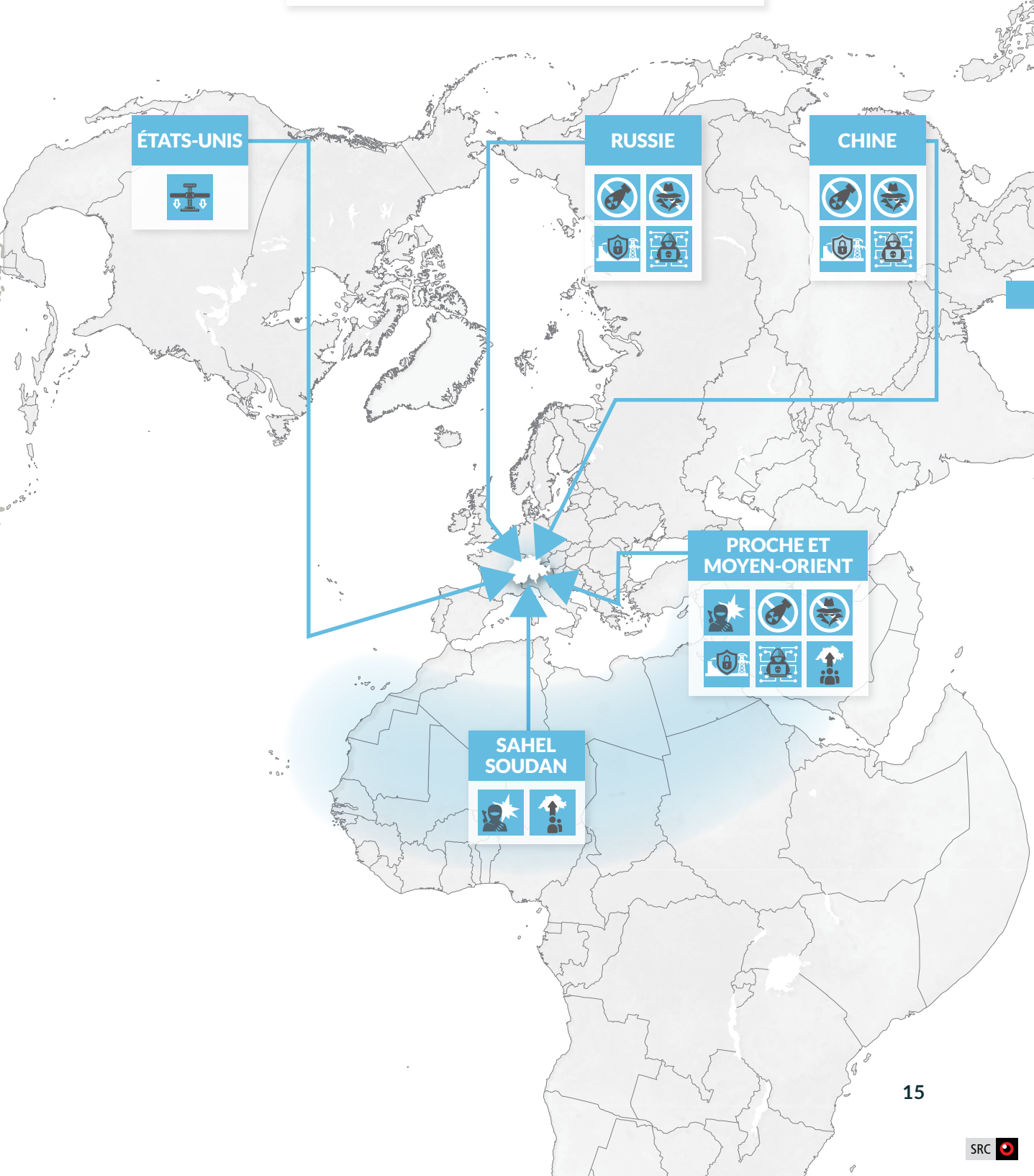
(voir à cet égard le chapitre «Russie», p.22). Compte tenu des intentions qu'on lui connaît de longue date, le fait que la Russie soit partiellement passée à une économie de guerre et qu'elle opère un réarmement continu représente, au-delà de la guerre contre l'Ukraine, une menace pour l'Europe. Pour le régime russe, cette guerre reste pour l'heure hautement prioritaire. La Russie a développé des stratégies complexes et efficaces pour continuer à s'approvisionner en marchandises et technologies occidentales. Elle contourne pour ce faire les règles et les sanctions, en Suisse également.

La guerre contre l'Ukraine est une guerre d'usure. Aucune décision militaire susceptible d'y mettre un terme n'est en vue, et il ne se profile ni accord de cessez-le-feu stable ni accord de paix durable. Tant la Russie que l'Ukraine semblent prêtes à continuer cette guerre, d'agression pour l'une, de défense pour l'autre. C'est désormais l'Europe qui assume la responsabilité principale du soutien occidental à l'Ukraine, mais elle n'a qu'une influence indirecte sur les efforts diplomatiques visant à la paix. Du côté russe, c'est surtout grâce au rôle clé que joue la Chine que la guerre peut se poursuivre.

L'année 2022 a aussi été marquée par l'ouverture d'une nouvelle ère nucléaire. Comme lors de la guerre froide, les armes nucléaires jouent à nouveau un rôle prédominant. Depuis le début de la guerre contre l'Ukraine, la Russie brandit régulièrement la menace de l'arme nucléaire, et l'idée de reprendre leurs essais nucléaires est revenue à plusieurs puissances, qui, après des décennies, envisagent à nouveau des tests. La Chine renforce quant à elle son arsenal nucléaire. Dans ce contexte, la prolifération nucléaire se trouve désormais à un tournant, et l'expiration du traité New Start en février 2026 a marqué la disparition du dernier accord américano-russe restant en matière de contrôle stratégique des armements. Cette situation contribue à la détérioration marquée et durable de l'environnement politico-sécuritaire de la Suisse.

La Chine constitue également une menace hybride croissante. Sa projection de puissance englobe des instruments militaires, politiques, institutionnels, idéologiques, informationnels, économiques et technologiques. Elle veut mobiliser le système dans son entier afin de devenir une grande puissance économique, technologique et militaire de premier plan. C'est dans cette perspective qu'elle travaille à un nouvel ordre mondial. Son rapprochement avec la Russie, la Corée du Nord et l'Iran s'appuie sur le rejet de l'ordre marqué par les conceptions occidentales. Ces quatre États ne forment cependant pas une alliance. La Russie a réagi avec beaucoup de réserve aux attaques américano-israéliennes contre l'Iran; c'est aussi le cas de la Chine en particulier, qui ne veut pas s'exposer aux représailles américaines ni mettre en danger ses relations avec les États du Golfe. Entre la Chine, la Russie, la Corée du Nord et l'Iran, il existe par ailleurs des divergences, voire de la méfiance. L'unité entre ces


	Terrorisme djihadiste et ethno-nationaliste		Cyber
	Prolifération		Migration
	Espionnage		Tentatives de pression
	Menace contre les infrastructures critiques		



États repose notamment sur le fait qu'ils rejettent l'ordre mondial marqué par les conceptions occidentales et la démocratie libérale. En lieu et place, ils misent sur une souveraineté étatique illimitée et une forme de gouvernement autocratique. Cette unité va vraisemblablement perdurer. La Chine, mais aussi la Russie, essaient en outre de rallier les États du Sud global à leurs propres intérêts. Les tensions et les conflits en Europe, en Afrique et en Asie, en particulier au Proche et Moyen-Orient, se multiplient et mettent à l'épreuve la capacité de réaction des États occidentaux, celle des États-Unis surtout. Un arc de crises se dessine autour de l'Europe depuis l'Afrique du Nord et la zone du Sahel jusqu'au Proche et Moyen-Orient. Les conséquences pour la sécurité de la Suisse en sont considérables.

Les États-Unis poursuivent leurs propres intérêts sur le plan géostratégique et économique, même si cela doit provoquer des tensions avec leurs alliés et partenaires traditionnels. Depuis 2025, l'Europe se trouve dans une position particulière, car elle cherche à préserver un ordre que même les États-Unis ne portent plus intégralement. Or, cet ordre a garanti la sécurité et la prospérité pendant des décennies, à la Suisse également.

La soif de pouvoir ainsi que les conflits géopolitiques compliquent les approches coopératives lorsqu'il s'agit de relever les défis régionaux et mondiaux de politique de sécurité. Les principes de l'ordre mondial et les forums internationaux sont fortement mis à contribution dans le but de développer de l'influence et de générer un impact. Cela vaut en particulier pour les régimes internationaux de non-prolifération des armes de destruction massive ou des armes conventionnelles, dont la modernisation est bloquée par la rivalité entre les grandes puissances.

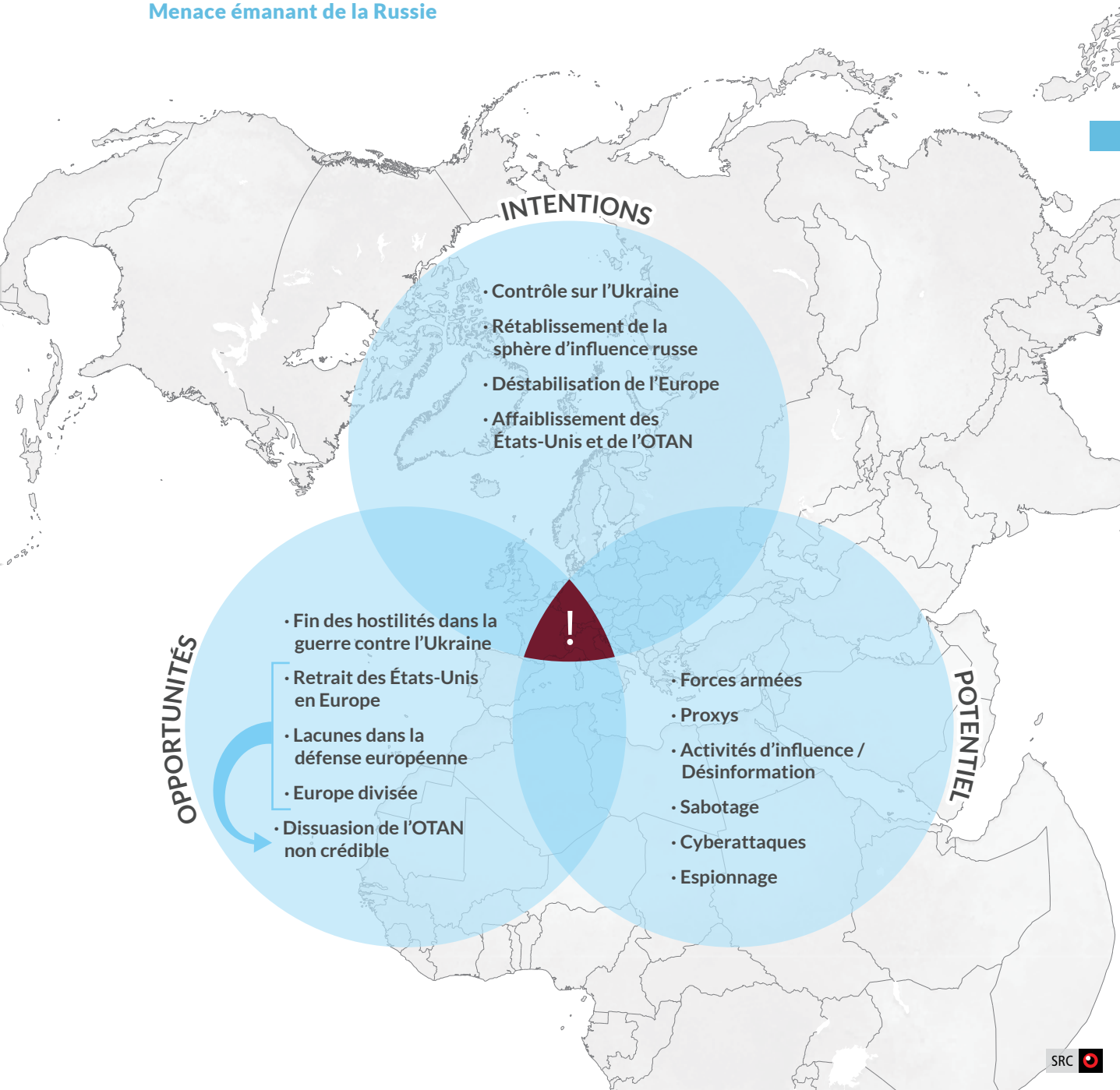
 L'ordre international traverse un bouleversement et se trouve dans une phase de transition. Les contours d'une confrontation globale se dessinent, en premier lieu entre les États-Unis et la Chine, allant vers un monde partagé entre deux sphères caractérisé par une lutte stratégique pour la suprématie. Les grandes puissances usent de plus en plus fréquemment de sanctions, de contrôles à l'exportation, de subventions, d'instruments financiers ou d'autres moyens de pression - qu'elles appliquent aussi à des États tiers - afin tant de tenir leurs adversaires à l'écart de marchandises et de technologies clés que de préserver et promouvoir leurs capacités propres. Toujours plus de secteurs et de catégories de biens peuvent avoir une importance aussi bien civile que militaire et se voient de ce fait classés comme critiques ou stratégiques. C'est le cas des terres rares, des semi-conducteurs, de l'intelligence artificielle, de la robotique, des énergies renouvelables ainsi que des technologies quantiques, des biotechnologies, mais aussi des drones et des données en général. Dans le domaine de la défense, il s'agit notamment de la navigation non dépendante de réseaux satellitaires, des canaux de communication sécurisés contre les écoutes ou des moyens qu'implique le champ de bataille dit transparent. Cette mise à niveau géoéconomique a des implications mondiales sur le plan de la politique de sécurité, raison pour laquelle les États intègrent la sûreté économique et technologique dans leurs concepts de sécurité nationaux.

Les interconnexions économiques et les réseaux créent des dépendances, lesquelles sont de plus en plus utilisées comme des moyens de pression et des armes lors de conflits afin d'atteindre des objectifs politiques et militaires. Des acteurs non étatiques se servent également de certaines vulnérabilités, comme le montrent par exemple les attaques des Houthis yéménites contre une route maritime revêtant une

importance centrale pour le commerce mondial. Ainsi, les développements survenant dans l'arc de crises situé à la périphérie méridionale de l'Europe continueront à la mettre au défi. Ils ouvrent une marge de manœuvre pour

divers acteurs étatiques et non étatiques hostiles à l'«Occident», et donc à la Suisse. L'Europe est menacée, et il est très probable que cette menace ne s'atténuera pas dans les années à venir.

Menace émanant de la Russie



ÉTATS-UNIS



Le président Donald Trump maintient sa politique disruptive en matière d'affaires étrangères et de sécurité. Par rapport à son premier mandat, l'influence stabilisatrice d'internationalistes républicains traditionnels au sein de son cabinet a disparu, le président s'étant à la place entouré surtout de loyalistes.

La politique menée par les États-Unis a pour objectif la recherche de leurs propres intérêts économiques, même vis-à-vis d'alliés traditionnels. Ces derniers doivent déboursier davantage pour que soient remplies des obligations en matière de sécurité. Rhétoriquement, les rivalités stratégiques avec la Chine et la Russie sont relativisées, au profit d'un accent stratégique plus prononcé placé sur la politique intérieure et l'«hémisphère occidental». Le plus grand tournant en matière de politique de sécurité, les États-Unis l'ont pris en exprimant le souhait de revenir à une relation de coopération avec la Russie. Cela reste pour l'heure sans succès, en raison de l'inflexibilité du président Vladimir Poutine par rapport aux objectifs maximaux qu'il a fixés dans la guerre contre l'Ukraine. Le président Donald Trump n'a lui-même de cesse de relativiser la rivalité systémique avec la Chine. En marge du sommet avec le chef de l'État et président du Parti communiste Xi Jinping à l'automne 2025, il avait annoncé la naissance d'un «G2», un groupe exclusif de deux superpuissances appelées à régner sur le monde. Or, même si le ton vis-à-vis de la Chine s'est nettement adouci, la rivalité systémique avec la Chine et la région Asie-Pacifique reste un point fort stratégique des États-Unis. Bien qu'elle s'explique par des raisons économiques principalement, cette position n'est pas sans conséquences sur le plan de la politique de sécurité: pour exercer une dissuasion vis-à-vis de la Chine, les États-Unis souhaitent renforcer leurs forces armées dans la région ainsi que l'autonomie de leurs alliés militaires. Cette dis-

suasion vise avant tout les interventions militaires chinoises dans la région, qui, surtout en cas de conflit autour de Taïwan, mettraient en péril la stabilité des chaînes d'approvisionnement.

À ce jour, la politique américaine en matière d'affaires étrangères et de sécurité est notablement interventionniste, même si, durant la campagne électorale, Donald Trump s'était présenté comme un isolationniste souhaitant donner la priorité aux États-Unis et les maintenir éloignés d'autres «guerres sans fin». Différentes écoles de pensée sont certes représentées parmi les plus proches conseillers de la présidence, mais c'est avant tout le président en personne qui détermine la politique américaine en matière d'affaires étrangères et de sécurité. Dans la pratique, celle-ci continue de revêtir, au gré de l'évolution de la situation, des traits clairement mondialistes, hégémoniques et interventionnistes, cela même si des principes fondamentaux divergents sont mis en avant dans plusieurs documents stratégiques et si la guerre contre l'Iran en particulier est loin de faire l'unanimité parmi les Républicains partisans de la ligne politique «America First».

Les crises, conflits et guerres simultanés se déroulant en Amérique latine, en Europe, au Proche et Moyen-Orient ainsi que dans la région Asie-Pacifique sollicitent de plus en plus les forces des États-Unis. S'y ajoute un affaiblissement des alliances traditionnelles, dont ils sont à l'origine - début 2026, les menaces d'une annexion du Groenland brandies par le président américain contre le Danemark, membre de l'OTAN, ont par exemple amoindri la confiance de l'Europe envers les États-Unis..

Les crises, conflits et guerres simultanés sollicitent de plus en plus les forces des États-Unis. S'y ajoute un affaiblissement des alliances traditionnelles, dont ils sont à l'origine.



Le président Donald Trump va poursuivre ses efforts visant à mettre un terme à la guerre contre l'Ukraine. La possibilité d'y parvenir dans les mois à venir dépendra de plusieurs facteurs dynamiques. Il faudrait pour ce faire qu'un cessez-le-feu apparaisse plus avantageux aux deux parties que la poursuite de la guerre, ce qui dépendra notamment du soutien occidental à l'Ukraine, de la situation militaire sur le front et de l'évolution de l'économie russe. Un cessez-le-feu stable ou un accord de paix durable restent toutefois très improbables d'ici la fin 2026.

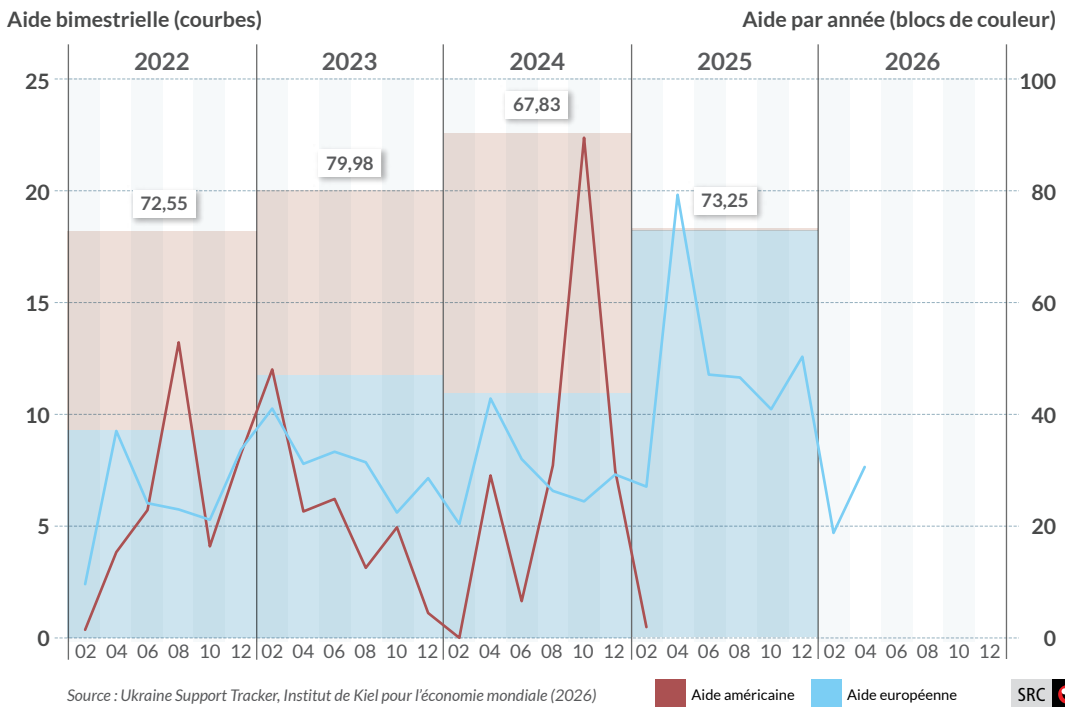
Les États-Unis ont initié une nouvelle répartition des charges, exigeant que l'Europe assume à l'avenir une plus grande partie des dépenses liées à la dissuasion et à la défense de l'OTAN. Il est probable que la présence militaire américaine en Europe sera réduite, mais sans doute pas de manière abrupte et significative. De plus, les États-Unis vont pour l'instant maintenir le bouclier nucléaire pour l'Europe, tout comme ils ne retireront pas soudainement leurs capacités militaires clés au vu du rôle incontournable

qu'elles endossent pour l'heure. Sur le fond, une présence en Europe leur est nécessaire, puisqu'elle leur permet de projeter leur puissance militaire à l'échelle mondiale. Néanmoins, le propos vis-à-vis de l'Europe se durcit par moments, prenant alors des accents de combat de civilisation. Pour certaines parties de l'administration Trump, qui envisagent l'Europe à travers le prisme de la politique intérieure américaine, le Vieux Continent est en effet menacé d'une extinction civilisationnelle.

La rivalité systémique entre les États-Unis et la Chine va s'accroître et se manifestera avant tout dans les domaines de l'économie, de la politique douanière ainsi que de la technologie. Cela impliquera des conséquences directes sur l'Europe et la Suisse (voir « *Chine: sécurité économique* », p.28). Sur le plan militaire, les deux nations vont poursuivre le renforcement de leurs armements ainsi que leurs tentatives de se surpasser mutuellement en termes de capacités et de puissance.

Aide américaine et européenne à l'Ukraine depuis janvier 2022

(en milliards d'euros)



EUROPE



Après le sommet américano-russe en Alaska, dont aucun résultat n'a émané, la Russie a intensifié son conflit hybride contre l'Europe à partir de la fin de l'été 2025. Au contraire de la tactique qu'elle avait adoptée en 2024 entre le début de l'année et l'automne, elle a cette fois-ci misé avant tout sur des violations de l'espace aérien au moyen de ses avions de combat ainsi que vraisemblablement sur des vols de drones au-dessus d'aéroports civils et militaires. Il y a toutefois aussi eu des actes de sabotage (physiques et cybernétiques), notamment contre l'infrastructure ferroviaire et énergétique polonaise.

La menace russe persistante et l'attitude de la nouvelle administration américaine ont amené l'Europe à accepter d'endosser nettement plus de responsabilité pour sa propre défense, tant à des fins de dissuasion vis-à-vis de la Russie que de soutien pour l'Ukraine. Depuis les débuts de la guerre froide, les États-Unis n'ont eu de cesse d'exiger une telle redistribution transatlantique des charges. Au sommet de l'OTAN à La Haye en juin 2025, les pays membres se sont engagés à un nouvel objectif en termes de dépenses en matière de défense, correspondant à cinq pour cent de leur produit intérieur brut respectif. En parallèle, avec Baltic Sentry, Eastern Sentry et Arctic Sentry, l'OTAN a lancé trois nouvelles missions. Depuis janvier 2025, la première permet de surveiller et protéger les câbles sous-marins en Mer Baltique. Avec Eastern Sentry, mise en place en septembre 2025, l'OTAN a de plus réagi à la série de violations de l'espace aérien et de mystérieux incidents de drones au-dessus de son territoire. Cette nouvelle mission teste la Ligne de dissuasion du flanc oriental annoncée par l'OTAN en juillet 2025, un réseau complexe de capteurs visant à détecter des moyens ennemis et à s'en protéger. En février 2026, au vu des revendications territoriales du président Donald Trump vis-à-vis du Groenland, l'OTAN a par ailleurs lancé la mission Arctic Sentry, afin de démontrer la respon-

sabilité accrue des États européens membres de l'OTAN dans le Grand Nord. Concrètement, les patrouilles dans la région ont été intensifiées.

Entre janvier 2022 et fin avril 2026, l'Europe a, selon la banque de données consacrée à l'Ukraine de l'Institut de Kiel pour l'économie mondiale (Kieler Ukraine Support Tracker), dépensé au total 215 milliards d'euros pour l'Ukraine, soit nettement plus que les États-Unis, qui ont de leur côté déboursé 115 milliards d'euros. Les principaux bailleurs de fonds sont l'Allemagne et la Grande-Bretagne. L'Ukraine reste néanmoins dépendante des États-Unis, avant tout pour ce qui est des systèmes de défense aérienne et des informations relevant du renseignement. Avec la liste dite des besoins priorités pour l'Ukraine, il existe depuis 2025 un mécanisme grâce auquel l'Europe paie pour des armes américaines au profit de l'Ukraine. Dans ce cadre, des systèmes de défense aérienne Patriot ainsi que des systèmes d'artillerie à longue portée ont notamment été livrés.

Ensemble, les États européens sont désormais les principaux soutiens de l'Ukraine. Leur aide militaire a ainsi dépassé de 67 pour cent la moyenne enregistrée entre 2022 et 2024. En 2025, l'Ukraine a pourtant dû s'accommoder d'un soutien international plus faible, car les États-Unis ont fortement réduit leur appui durant cette année-là. À plusieurs reprises, les États européens se sont par ailleurs trouvés dans la situation de devoir réagir rapidement face au développement dynamique des initiatives américaines en faveur de la paix en Ukraine. Toutefois, aucune normalisation des relations américano-russes ne se dessine et les efforts en vue d'un accord de paix arrangé entre les États-Unis et la Russie n'ont jusqu'à présent pas aboutis.

Entre l'Europe et la Chine, les rapports restent tendus, même si les deux parties s'efforcent d'entretenir des relations stables et constructives.

L'UE considère la Chine comme un partenaire commercial, mais aussi comme un rival systémique. Le rejet par la Chine de l'ordre mondial marqué par les conceptions occidentales, son modèle économique basé sur le soutien par l'État, les distorsions du marché, les transferts de technologies et les dépendances stratégiques constituent tout à la fois des menaces et des risques pour la concurrence européenne, le commerce équitable, la sûreté des chaînes d'approvisionnement ainsi que pour la souveraineté industrielle et technologique. En 2025, l'UE a élargi de manière significative sa stratégie en matière de sécurité économique. Elle se concentre à cet égard sur la maîtrise des risques découlant de changements géopolitiques, sur les évolutions technologiques et les dépendances vis-à-vis d'États tiers, la Chine en particulier. Le soutien continu de celle-ci aux efforts de guerre russes reste par ailleurs un élément de conflit central entre les deux parties. En raison de la politique commerciale et économique parfois agressive des États-Unis, qui privilégient davantage leurs intérêts nationaux, certains États européens tentent de compenser leurs pertes économiques en renforçant leur coopération avec la Chine.



Les investissements en matière de défense de l'UE ont fait un saut quantique en 2025. Néanmoins, la principale initiative prise par les Européens sur le plan politico-militaire cette année-là, à savoir la planification d'une mission militaire européenne sur territoire ukrainien comme possible garantie de sécurité pour l'Ukraine, n'a pas été réalisée sous l'égide de l'UE, mais dans le cadre d'un format ad hoc dirigé par la Grande-Bretagne, qui n'est pas membre de cette dernière.

Le chemin menant vers une Europe autonome en matière de défense reste donc encore long. Même si pratiquement tous les États européens membres de l'OTAN ont dans l'intervalle atteint l'ancien objectif consistant à consacrer deux pour cent de leur produit intérieur brut aux dépenses liées à la défense, les capa-

cités de défense et de dissuasion de l'Europe restent dépendantes des compétences militaires de pointe des États-Unis. Celles-ci s'avèrent critiques, car les investissements européens

consentis pour la recherche sont largement inférieurs aux investissements américains. Des problèmes de recrutement se posent par ailleurs en de nombreux endroits.

Le marché européen de l'armement fragmenté réduit l'efficacité du réarmement militaire qui s'est amorcé. La tendance pour les prochaines années est néanmoins claire: l'Europe veut réduire sa dépendance vis-à-vis des États-Unis et constituer sa propre capacité de dissuasion militaire. Sur le long terme, les efforts d'harmonisation sur le marché de l'armement et l'approche de plus en plus intégrée de la politique de sécurité et de défense commune devraient porter leurs fruits. La réponse à la question de savoir si le renforcement de la cohésion actuelle en matière de politique de sécurité en Europe perdura ou si cette cohésion se fragmentera à nouveau à l'avenir n'est toutefois pas claire.

En 2026, il est probable que l'UE contrecarera plus activement la menace économique constituée par la Chine et qu'elle poursuivra ses efforts visant à minimiser les risques qui en découlent. La stratégie de l'UE en matière de sécurité économique englobe des instruments tels que des examens des investissements, des contrôles à l'exportation pour les technologies critiques, des règles anti-subsidies ainsi que des droits de douane antidumping. À l'inverse, certains pays européens vont malgré tout continuer à s'ouvrir économiquement vis-à-vis de la Chine. La Suisse se trouve confrontée aux mêmes choix (voir «Chine: sécurité économique», p.28).

Le chemin menant vers une Europe autonome en matière de défense reste encore long. Les capacités de défense et de dissuasion de l'Europe restent dépendantes des compétences militaires de pointe des États-Unis.

RUSSIE



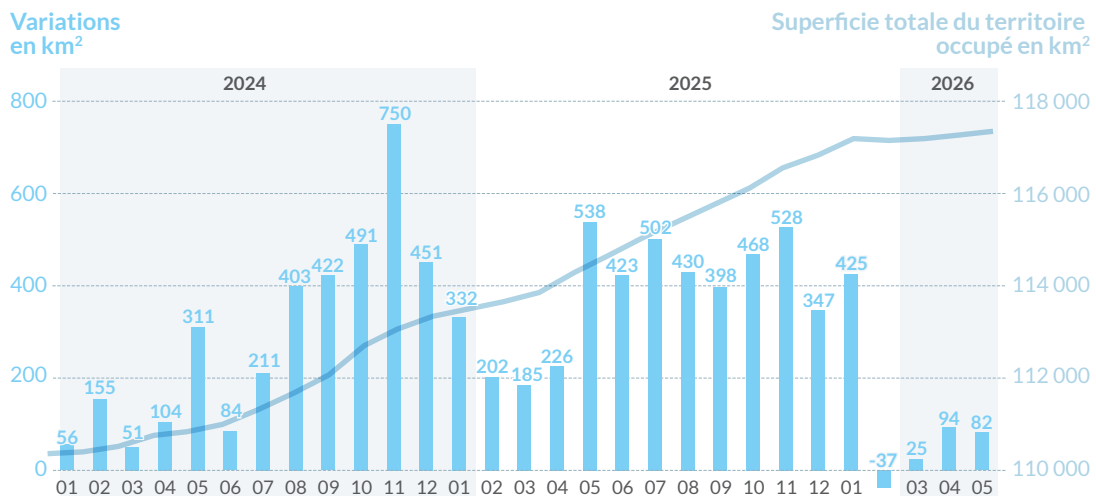
Malgré des difficultés économiques croissantes, le système Poutine s'avère stable. Les personnalités clés, dont beaucoup ont plus de 70 ans, lui restent loyales. Misant sur la stabilité, le président russe ne veut pas les remplacer, d'autant moins pendant la guerre en cours. Depuis plusieurs années, le pouvoir forme toutefois une nouvelle génération, constituée en partie d'enfants de fidèles de Vladimir Poutine, mais aussi de technocrates qui lui ont témoigné une loyauté sans faille. L'opposition en Russie est toujours plus fortement réprimée, répression qui s'accompagne d'une propagande plus agressive dans les médias et le système de formation ainsi que d'une augmentation de la surveillance, de la répression et de la militarisation au sein de la société.

Les problèmes économiques se sont accentués. Le produit intérieur brut n'a progressé que d'un pour cent en 2025. L'inflation et les taux d'intérêts élevés ainsi que la pénurie de main d'œuvre ont des répercussions négatives, tout particulièrement sur les secteurs civils. Quant aux dépenses de l'État, elles continuent de croître, tandis que le bas prix du pétrole et les nouvelles sanctions ont entraîné un affaiblissement

des recettes issues du secteur énergétique. Tous ces éléments ont contribué au fait que le budget fédéral 2025 s'est clôturé sur un déficit d'au moins 50 milliards de francs. Même s'il est probable que ce déficit ait en réalité été plus élevé encore, le financement des dépenses de guerre a néanmoins été assuré. Le Trésor public russe engrange certes des recettes supplémentaires grâce à la hausse mondiale des prix du pétrole et du gaz causée par la guerre en Iran. Mais il faudrait que le prix du pétrole se maintienne à plus de cent dollars le baril sur plus d'une année pour que la Russie soit en mesure de financer son déficit budgétaire à travers des revenus additionnels émanant du secteur énergétique.

Dans cette guerre, la Russie est supérieure à l'Ukraine tant sur le plan du matériel qu'en termes d'effectifs. Le manque de personnel induit des points faibles dans la défense de l'Ukraine, lesquels mènent à des pertes de territoire. Bien que la situation des forces ukrainiennes se soit légèrement améliorée depuis début 2026, les forces armées russes progressent, très lentement toutefois. L'Ukraine s'est en revanche montrée très innovante dans la

Gains territoriaux mensuels de la Russie



production et l'engagement de drones. Elle fabrique désormais elle-même la plus grande partie des drones utilisés et les déploie avec succès dans la défense aérienne, sur le front et contre des cibles de choix en territoire russe. Elle partage désormais son expertise dans ce domaine non seulement avec l'OTAN, mais aussi avec les pays du Golfe. Malgré cela, elle a toujours besoin du soutien de l'étranger, avant tout pour ce qui est du financement, de la défense aérienne, de l'artillerie et des moyens de longue portée, mais aussi en matière d'informations relevant du renseignement. Or, ce soutien a récemment diminué. La Russie quant à elle recrute suffisamment de nouveaux soldats pour compenser les pertes et constituer de nouvelles formations.

La Russie veut affaiblir les démocraties occidentales et l'unité transatlantique. Son conflit hybride concerne aussi la Suisse, et représente une menace à son égard.

- La Russie vise directement la Suisse au moyen de désinformation et de propagande. En 2025, le nombre de messages relatifs à notre pays diffusés par la branche germanophone du média d'État russe RT a augmenté d'un quart par rapport à 2024.
- Des cyberattaques contre des cibles à l'étranger s'effectuent également à travers des infrastructures suisses.
- La Russie utilise par ailleurs vraisemblablement la Suisse sur le plan logistique ainsi que pour préparer des actions de sabotage et de déstabilisation ailleurs en Europe.
- En recourant à l'espionnage, la Russie essaie d'obtenir des informations confidentielles relevant des autorités suisses.
- La Russie utilise notre pays pour acquérir clandestinement des biens et technologies sous sanctions afin d'augmenter sa capacité de production de matériel de guerre et de munitions.



La population russe ressent de plus en plus les effets de la guerre, d'où un mécontentement croissant. Grâce à la surveillance et à la répression, l'État russe parvient cependant à le gérer et à éliminer à la source toute velléité de résistance. Dans la perspective de l'élection à la Douma prévue en septembre 2026, des arrangements ont cours pour que le parti au pouvoir, Russie unie, obtienne un succès sans discussion, l'objectif étant de garantir une stabilité sur le long terme à l'interne.

D'un point de vue économique, 2026 sera une année difficile pour la Russie. La population ressentira de plus en plus les difficultés économiques. Le Kremlin donnera malgré tout la priorité au financement de la guerre, de sorte que les dépenses pour la défense et la sécurité resteront élevées. Proportionnellement, les recettes émanant du secteur pétrolier et gazier ont diminué au cours de ces dernières années dans le budget de l'État. En lieu et place, le Kremlin a augmenté la TVA depuis janvier 2026, et il mise sur une régulation de la zone grise économique. Malgré une situation économique plus difficile, rien n'indique jusqu'à présent que la capacité de résistance de la Russie dans la guerre contre l'Ukraine ne s'en trouvera entravée.

Il est extrêmement probable que la Russie intensifiera son conflit hybride en Europe. À cet égard, les infrastructures critiques suisses constitueraient une cible attrayante : la Russie

Il est extrêmement probable que la Russie intensifiera son conflit hybride en Europe. À cet égard, les infrastructures critiques suisses constitueraient une cible attrayante.

pourrait mener des actions de sabotage ou de destruction, non pas pour nuire prioritairement à la Suisse mais bien plutôt pour porter atteinte aux États membres de l'UE et de l'OTAN.

Les forces armées russes pourront probablement poursuivre la guerre contre l'Ukraine jusqu'à fin 2026, même si le prix à payer pour l'économie russe sera plus élevé. Sur la base du rythme actuel des gains territoriaux réalisés par la Russie, les forces armées russes auront encore besoin de plusieurs années pour conquérir le Donbass dans son entièreté. S'il est extrêmement probable que les forces armées russes garderont l'initiative jusqu'à fin 2026, il est extrêmement improbable que les forces armées ukrainiennes s'effondrent d'ici là.

La Russie est en mesure d'afficher publiquement le maintien de ses exigences maximales. Elle peut aussi retarder les négociations à dessein et miser sur la carte militaire jusqu'à ce qu'elle parvienne à obtenir des concessions ou des avantages concrets. L'intention du pouvoir russe sur le long terme - prendre le contrôle de l'Ukraine -, reste inchangée, même si le Kremlin pourrait, pour des considérations d'ordre tactique, accepter un cessez-le-feu ou un «deal» avantageux pour lui. Le gouvernement russe reste confiant quant au fait que la situation de l'Ukraine va continuer à se dégrader, sur le triple plan intérieur, militaire et diplomatique, et que le soutien occidental ne durera pas.

La position de l'Ukraine dans le «processus de paix» dépend des développements qui surviendront sur le plan de la politique intérieure. Le président Volodymyr Zelensky est fragilisé par des scandales de corruption. Il n'acceptera des concessions territoriales dans le Donbass que s'il obtient des garanties de sécurité internationales. Sans un cessez-le-feu conclu avec la Russie, il est improbable qu'une élection présidentielle ou un référendum sur les négociations de paix aient lieu en Ukraine, sauf si le président Donald Trump augmente tellement la pression que l'Ukraine se trouve contrainte à accepter les conditions russes.

Les points de vue fondamentalement différents de la Russie et de l'Ukraine quant à la paix et le fait en particulier que la Russie s'en tienne à ses exigences maximales empêcheront une résolution du conflit en 2026 également. Cet état de fait perdurera du moins aussi longtemps que la situation sur le front ne se sera pas détériorée de manière marquée pour l'une ou l'autre des parties. *(Pour les conséquences pour la Suisse, voir l'encadré ci-contre «Une guerre entre l'OTAN et la Russie en Europe d'ici à 2030 ?»)*

UNE GUERRE ENTRE L'OTAN ET LA RUSSIE EN EUROPE D'ICI À 2030?

Depuis 2022, les autorités de sécurité des États occidentaux mettent en garde, publiquement, quant à la possibilité d'une attaque militaire de la Russie contre l'OTAN. L'Alliance atlantique se prépare à une attaque de la Russie, qui pourrait, selon plusieurs services de renseignement européens, intervenir avant la fin de la décennie en cours. Les délais de préalerte pour une guerre en Europe se sont ainsi considérablement raccourcis, y compris pour la Suisse. Alors qu'ils étaient d'au moins dix ans par le passé, ces délais ne sont désormais plus que de quelques années. Il est donc d'autant plus important de minimiser les possibilités qu'a la Russie en Europe - et en Suisse également.

La question de savoir jusqu'à quand l'Europe doit être prête à se défendre contre la Russie fait entrer en ligne de compte beaucoup de variables et de nombreux impondérables, si bien qu'on ne peut pas y répondre en citant une année précise. La manière dont la guerre contre l'Ukraine se poursuivra ainsi que le positionnement des États-Unis vis-à-vis de l'OTAN font partie de ces variables :

- La Russie acquiert en Ukraine une expérience précieuse en matière de guerre. Son potentiel militaire reste toutefois essentiellement absorbé par cette guerre. Une fois celle-ci terminée, la reconstitution des forces armées russes pourrait s'accélérer, incluant celle de son corps d'officiers, qui s'est considérablement amoindri. La Russie développe par ailleurs des stratégies pour soutenir ses propres efforts en matière de réarmement à l'aide de biens et technologies occidentales.
- La réduction de la présence américaine en Europe n'a jusqu'ici été ni significative ni abrupte, même si des changements ont désormais été annoncés. Des questions se posent ainsi, à propos tant de la fiabilité des garanties sécuritaires des États-Unis que de la stabilité

de l'UE sur le plan de la politique intérieure et de la politique de sécurité. On ne sait pas non plus combien de temps encore les États clés que sont la France et l'Allemagne vont maintenir leur position favorable à l'Ukraine et à l'OTAN. Avec ses attaques hybrides, la Russie vise à diviser les sociétés occidentales, afin d'affaiblir leur cohésion politique et leur capacité de décision.

Lorsqu'il s'agit d'examiner la probabilité d'une guerre entre la Russie et l'OTAN, l'unité politique de l'Europe, celle des États-Unis et celle de l'OTAN sont des variables importantes, tout comme les capacités de la Russie pour l'heure encore engagées en Ukraine. Cependant, il faut aussi tenir compte d'une autre variable tout aussi importante : la question de savoir dans quelle mesure le président russe Vladimir Poutine et son cercle de pouvoir considèrent la dissuasion et la défense de l'OTAN comme crédibles.

Aussi longtemps que les forces armées russes resteront absorbées en Ukraine et que les États-Unis continueront à jouer un rôle dans la défense de l'Europe, l'appréciation de probabilité suivante restera valable :

- Il est extrêmement probable que la Russie va intensifier son conflit hybride en Europe, dans l'intention notamment de mettre à l'épreuve l'article 5 du Traité de l'Atlantique Nord. **Une escalade peut survenir en tout temps, et rapidement.** Une escalade peut survenir en tout temps, et rapidement.
- Il est très improbable que la Russie mène une attaque militaire contre un État européen.
- Il est extrêmement improbable qu'une guerre étendue survienne entre la Russie et l'OTAN.

CHINE



Avec son quinzième plan quinquennal, la Chine vise une croissance économique sur le long terme et une domination technologique à travers l'innovation et les contrôles des chaînes d'approvisionnement critiques. Dans le même temps, son armée doit être modernisée et la fusion militaro-civile approfondie. La Chine étend influence à l'échelle mondiale, cherchant ainsi à renverser les rapports de force en sa faveur et à rivaliser avec les États-Unis principalement. Ces ambitions et la rivalité entre grandes puissances induisent l'utilisation d'instruments économiques comme moyens de pression et comme armes. La fragmentation géoéconomique s'en trouve accélérée. Cette situation entraîne des menaces et des risques pour la sécurité économique, pour la Suisse également.

En 2025, la Chine s'est servie comme elle ne l'avait jamais fait auparavant des dépendances occidentales comme moyens pour exercer une contre-pression, par exemple en réaction aux droits de douane américains. Jusqu'en octobre 2025, Pékin a par exemple restreint les exportations de douze des dix-sept terres

Avec son idée d'un nouvel ordre mondial, la Chine courtise et séduit. Elle a fait de la Russie son premier partenaire politique.


monial, la Chine courtise et séduit, en essayant de rallier les États du Sud global à sa cause.

La Chine a fait de la Russie son premier partenaire politique. Elle joue un rôle clé dans la poursuite de la guerre contre l'Ukraine en lui achetant du pétrole et du gaz. Elle lui vend par ailleurs des biens à double usage et, même si elle s'en défend, soutient ainsi de fait l'intervention militaire russe. Des biens achetés en Suisse, par exemple des machines-outils, sont également exportés vers la Russie depuis la Chine, ou sont

utilisés sur place pour la production destinée à la Russie. En raison de l'importance politique de son partenariat avec la Russie, Pékin ne souhaite pas que Moscou se voie affaibli par une défaite contre l'Ukraine. Une telle défaite signifierait en effet une modification de la répartition stratégique du pouvoir en défaveur de la Chine. L'effondrement du pouvoir de l'État en Russie créerait en outre un risque sécuritaire à sa propre frontière.

C'est dans la région Asie-Pacifique que l'ascension de la Chine au rang de puissance mondiale est la plus manifeste. Elle y combine de manière accrue les instruments économiques et diplomatiques dont elle use aussi ailleurs dans le monde à des moyens militaires et paramilitaires. La modernisation et le développement des forces armées chinoises se poursuivent. Environ douze pour cent des dépenses militaires mondiales sont désormais le fait de la Chine. Les tensions élevées qu'elle génère en Mer de Chine méridionale, en Mer de Chine orientale et autour de Taïwan continuent de croître. Avec ses activités militaires en partie agressives, la Chine viole régulièrement le droit international et elle harcèle ses voisins pour faire valoir ses propres revendications territoriales.

Les États-Unis essaient de former un contre-poids à la projection de puissance de la Chine dans la région Asie-Pacifique. Ils essaient aussi d'y renforcer leurs alliances. Les États de la région ne sont toutefois pas toujours sûrs de savoir quelle est la position de l'administration Trump, tant en Asie-Pacifique ainsi que vis-à-vis de la Chine. Ils ne parviennent pas non plus à s'unir contre Pékin. De nombreux États de la région adoptent au contraire de plus en plus une approche pragmatique, axée sur leurs propres intérêts nationaux, sans se positionner clairement comme partenaire de la Chine ou des États-Unis.

 La Chine va poursuivre ses ambitions économiques, ce qui perpétuera la rivalité systémique avec les États-Unis.

En Europe, la Chine continuera de soutenir la Russie sur le plan politique et économique, ainsi qu'avec des biens à double usage. Mais elle sait tirer profit des rapports de force et achète à la Russie du pétrole et du gaz à bas prix. Pour la Chine, la Russie constitue un atout majeur dans la perspective d'un nouvel ordre mondial. Elle poursuivra ainsi ses efforts visant à soustraire les États du Sud global de l'influence des États-Unis ou à les en tenir à l'écart. Parallèlement, elle tente de prendre une position dirigeante vis-à-vis de ces États, sans toutefois s'exposer trop.

Sous Xi Jinping, la Chine continuera d'accroître son influence dans la région Asie-Pacifique, tout en tentant de réduire celle des États-Unis. Afin d'accroître les dépendances existantes, elle misera sur des investissements. Tirant parti des incertitudes que causent les États-Unis avec leur politique douanière, la suspension de l'aide

au développement ou la réorientation rigoureuse de leur politique de sécurité, elle pourra se présenter comme un partenaire fiable. Elle n'hésitera pas à s'immiscer au niveau politique pour exercer une influence sur les gouvernements de la région en étouffant toute critique.

Cette politique va de pair avec le renforcement de l'Armée populaire de libération. D'ici à 2049, la Chine entend devenir la plus grande puissance militaire au monde. Si la destitution de cadres pourrait affaiblir l'Armée populaire de libération, du moins provisoirement, les activités militaires chinoises dans la région Asie-Pacifique vont s'accroître. L'intégration de Taïwan reste la priorité pour la Chine, même s'il est probable qu'elle ne cherchera pas encore à forcer une décision. Les risques politiques, militaires et économiques sont en effet encore trop élevés pour elle. Il n'en demeure pas moins que les risques d'escalade restent considérables. L'attitude erratique des États-Unis en matière de politique étrangère et de politique de sécurité représente un défi pour la Chine également.

CHINE : SÉCURITÉ ÉCONOMIQUE



De nombreux États considèrent désormais la sécurité économique et technologique comme faisant partie intégrante de leurs concepts de sécurité nationaux. Ils veulent ainsi réduire leur vulnérabilité économique et renforcer leur propre résilience, particulièrement vis-à-vis de la Chine.

Tout comme d'autres États, la Suisse est fortement dépendante des chaînes d'approvisionnement chinoises. La Chine subventionne ses propres entreprises et les traite de manière préférentielle. Principal pays producteur de technologies clés, elle domine la production ainsi que le traitement de matières premières critiques. La production mondiale de terres rares est contrôlée par la Chine à hauteur de 80 à 90 pour cent. En 2025, elle a introduit de nouveaux mécanismes de contrôle qui ont provoqué des incertitudes ainsi que des retards de livraison. À long terme, la sécurité d'approvisionnement pour des produits importants est remise en question. Pour qu'elle autorise l'exportation de terres rares, la Chine exige que le but de l'utilisation lui soit divulgué dans le détail. Grâce à ce droit de regard, elle peut identifier des dépendances. Elle pourrait se servir de ces données de manière ciblée pour sanctionner ou exercer une pression.

À l'inverse, la Chine est dépendante de l'Europe dans certains secteurs. Des entreprises européennes lui fournissent des matériaux sophistiqués, des produits chimiques ainsi que des technologies de pointe. C'est le cas en particulier pour les équipements aérospatiaux, les machines de précision et les équipements servant à fabriquer des semi-conducteurs. S'y ajoutent des investissements et un savoir-faire technologique. Du fait de son économie axée sur l'exportation, la Chine est vulnérable vis-à-vis de la politique commerciale européenne. Néanmoins, le caractère limité de ces dépendances ainsi que, probablement, l'incidence de la politique douanière américaine, ont contribué à la relative stabilité des relations sino-européennes en 2025.

La Chine est intéressée à accéder aux résultats en matière de recherche et développement obtenus en Suisse. Afin de permettre le transfert de technologies en sa faveur, elle investit dans des entreprises innovantes, recrute des talents et encourage la collaboration avec des institutions scientifiques occidentales, par exemple en finançant des bourses de recherche et d'études. Le transfert de technologies se fait toutefois aussi par le recours à l'espionnage. Du point de vue de la politique de sécurité, ce sont surtout les biens à double usage qui revêtent une importance centrale.



Les tensions entre la Chine et l'Europe sont d'ordre structurel et vont perdurer. Dotée

d'un quinzième plan quinquennal, la Chine ne modifiera

Les tensions entre la Chine et l'Europe sont d'ordre structurel et vont perdurer.

pas ses objectifs. Elle continuera à utiliser l'étranger comme un facteur essentiel d'appui à la modernisation de son économie et de son armée ainsi qu'au développement de capacités d'influence à l'échelle internationale. S'agissant des biens et des matières premières importantes sur le plan stratégique, la Chine étendra sa domination. Les surcapacités de son industrie lui permettront de continuer à inonder le marché européen, mettant la base industrielle de l'Europe sous pression.

Au surplus, la sécurité économique en Suisse comme en Europe reste dépendante des relations entre les États-Unis et la Chine. D'une part, parce que les décisions chinoises, même si elles visent prioritairement les États-Unis, ont aussi des effets sur l'Europe. D'autre part, parce qu'il est très probable que les États-Unis continueront à pousser les États européens à réduire leur collaboration avec des acteurs considérés comme problématiques, les entreprises chinoises en particulier.

Depuis 2024, le SRC dispose d'une plateforme participative : «Kompass DDPS». Celle-ci sert à la détection précoce et à l'appréciation des développements pertinents sur le plan de la politique de sécurité. La plateforme est ouverte à tous les collaborateurs de l'administration fédérale. La diversité cognitive, les différentes perspectives et connaissances représentées dans l'administration fédérale peuvent ainsi être mises à profit. Des études empiriques ont confirmé à plusieurs reprises l'efficacité d'une telle approche. Les prévisions effectuées dans le cadre de «Kompass DDPS» sont visualisées grâce à des graphiques réalisés de manière

automatisée et elles sont analysées partiellement à l'aide de l'intelligence artificielle (IA). L'IA résume par exemple les justifications qui sont avancées par les utilisateurs pour étayer leurs pronostics.

La Chine mettra-t-elle en œuvre un blocus de Taïwan l'année prochaine ? Les utilisateurs de la plateforme participative ont jugé cela improbable en mai 2026. Les coûts économiques et politiques qu'une telle démarche impliquerait pour la Chine l'empêchent à leurs yeux de prendre une telle mesure.

La République populaire de Chine mettra-t-elle en œuvre un blocus de Taïwan d'ici le 31.03.2027 ?

A DÉBUTÉ 21 avr. 2026 08:00
SE TERMINE 31 mars 2027 23:59 (dans 10 mois)

CHALLENGES: Kompass DDPS - Armed Conflict, Kompass DDPS
MOTS-CLÉS: Chine, Forces armées
SAISONS: Saison 2026, Saison 2027

Résumé de la justification actuelle

ⓘ Ce résumé des justifications fournies par les prévisionnistes pour cette question a été généré par l'IA. Il peut contenir des erreurs ou des inexactitudes. Veuillez l'utiliser avec discernement et vérifier tout détail important de manière indépendante.

Dernière mise à jour 01.06.26 14:04

Arguments expliquant pourquoi l'événement se produira :

- Certains prévisionnistes estiment qu'un blocus serait une stratégie pour la Chine afin d'exercer une pression sur Taïwan et d'autres puissances internationales sans recourir à une invasion directe.
- Le climat géopolitique, y compris les conflits internationaux et les dynamiques de pouvoir, pourrait inciter la Chine à envisager un blocus comme moyen d'affirmer sa domination.

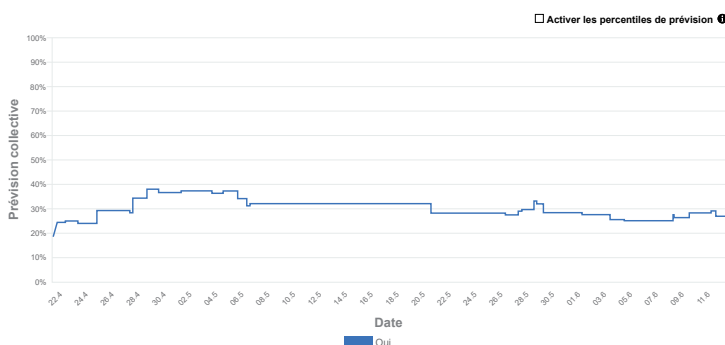
Arguments expliquant pourquoi l'événement n'aura pas lieu :

- Des prévisionnistes soulignent les risques économiques et géopolitiques important ce qui pourrait dissuader la Chine de prendre une telle mesure.
- Les intérêts stratégiques actuels de la Chine et l'interconnexion mondiale rendent un blocus contre Taïwan moins probable.

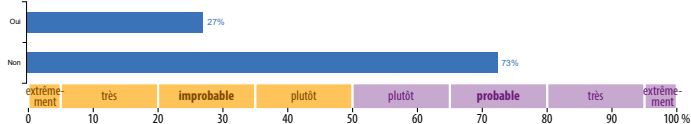
Bien qu'une minorité de prévisionnistes considère qu'un blocus par la Chine est plausible la majorité juge cela improbable en raison des importantes répercussions économiques

Développement du consensus


ⓘ Cliquez sur n'importe quel point du graphique pour voir la distribution des prévisions à ce moment-là.



Pronostic collectif actuel



PROCHE ET MOYEN-ORIENT

 Les conflits non résolus continuent de marquer la situation au Proche et Moyen-Orient. Au centre se trouve le conflit entre Israël et les États-Unis d'une part, et l'Iran et ses proxys et alliés régionaux d'autre part. Il se déroule en différents endroits.

Dans leur stratégie de sécurité nationale 2025, les États-Unis ont déclaré vouloir à l'avenir se concentrer moins sur le Proche et Moyen-Orient. En février 2026, le président Donald Trump a cependant décidé de lancer une attaque militaire de grande envergure contre l'Iran en collaboration avec Israël. L'objectif minimal de cette attaque était de limiter les capacités iraniennes à se projeter comme une puissance régionale, son objectif maximal de créer les conditions pour un changement de régime.

Les dirigeants iraniens ont réagi selon une logique de forte escalade. Ils ont ordonné des frappes contre des cibles dans plus d'une dizaine de pays et ont ainsi provoqué la fermeture de facto du détroit d'Ormuz. La participation d'acteurs de «l'axe de la résistance», dirigé par l'Iran, a contribué à la régionalisation du conflit. Israël a de son côté réagi aux attaques répétées du Hezbollah en reprenant son offensive d'ampleur au Liban, son but restant de démanteler le Hezbollah.

La Russie profite certes à court terme de la guerre en Iran grâce à la hausse des prix de l'énergie et à l'assouplissement des sanctions dans le secteur pétrolier. Bien qu'elle soit liée à l'Iran par un accord de partenariat stratégique depuis 2025, son soutien politique et militaire est resté limité. Pour sa part, la Chine voit ses intérêts menacés, mais elle calibrera son soutien de manière à éviter une détérioration de ses relations bilatérales avec les États-Unis et les États du Golfe.

En ce qui concerne Gaza, les États-Unis ont annoncé en janvier 2026 le lancement de la deuxième phase du plan Trump. Ils ont nommé un «Conseil de paix» ainsi que d'autres instances chargées de la future administration de la bande de Gaza. La mise en œuvre ne progresse toutefois que très lentement. Malgré son affaiblissement et son isolement, le Hamas reste la force palestinienne la plus puissante sur place.

La fait que les États-Unis demeurent l'acteur externe le plus influent dans la région se constate également en Syrie. Ils y soutiennent le gouvernement de transition dirigé par Ahmed al-Charaa, au détriment même de leurs alliés kurdes de longue date. Bien que le gouvernement de transition syrien jouisse désormais d'une large reconnaissance et d'une légitimité internationale, sa prétention au pouvoir continue d'être contestée sur le plan intérieur.

La stabilité du régime en Iran s'articule à plusieurs niveaux





La guerre en Iran et son issue marqueront profondément la région au cours des prochaines années. L'avenir du pouvoir iranien en particulier sera un enjeu crucial. Il s'agit pour lui non seulement de faire face à la menace militaire américano-israélienne, mais aussi d'assurer le contrôle de sa propre population. La répression sanglante des manifestations de janvier 2026 a accéléré la perte de légitimité du régime. La manière dont se recomposera le pouvoir après la fin de la guerre jouera un rôle déterminant. Comme le guide suprême de longue date Ali Khomeini, de nombreux dirigeants politiques et militaires du régime sont morts. Il est probable que le pouvoir et l'influence du Corps des gardiens de la révolution islamique (CGRI) continueront à croître. Pilier central du système, le CGRI s'est certes montré résilient pendant la guerre, mais sa pérennité n'est cependant pas assurée. Le but prioritaire des dirigeants restera d'assurer leur maintien au pouvoir. Ils se verront ainsi inévitablement confrontés à la question de savoir si les efforts au niveau de

Quant au programme de missiles iraniens, sa poursuite impliquerait qu'une grande partie du territoire européen, bases américaines y incluses, se trouverait d'ici quelques années à portée des systèmes d'armement iraniens.

l'armement nucléaire doivent être poursuivis. Si un renversement de pouvoir devait se produire en Iran, il est très probable qu'il ne se déroulerait pas de manière pacifique.

Quant au programme de missiles iraniens, sa poursuite impliquerait qu'une grande partie du territoire européen, bases américaines y incluses, se trouverait d'ici quelques années à portée des systèmes d'armement iraniens.

Israël poursuivra son objectif stratégique visant à un changement de régime en Iran. Il s'efforcera d'affaiblir davantage l'«axe de la résistance», dont en particulier le Hezbollah

au Liban, qui est déjà fortement diminué sur le plan militaire et isolé sur le plan politique. Pour y parvenir, il est très probable qu'Israël mettra aussi prioritairement sur sa puissance militaire à l'avenir. Un large soutien de la part des États-Unis restera très probablement assuré tant que Donald Trump sera président. Du fait de la dépendance militaire, politique et économique d'Israël envers eux, les États-Unis peuvent néanmoins imposer des limites. Lors de la guerre à Gaza, le président Donald Trump a par exemple montré qu'il était prêt à le faire.

Pour les États du Golfe, la flambée de violence au Proche et Moyen-Orient représente un défi majeur. La guerre sape leur modèle économique, qui repose sur la stabilité régionale. Au lieu de pouvoir se concentrer sur leur développement économique, ils doivent désormais réfléchir à la manière dont ils comptent gérer à l'avenir l'Iran et la menace qu'il représente. Il est très probable qu'ils maintiendront leurs liens étroits avec les États-Unis sous la présidence de Donald Trump. Il est aussi très probable qu'ils renforceront leurs propres capacités de défense. Cette situation entraînera une pénurie accrue de biens militaires déjà rares à l'échelle mondiale, notamment dans le domaine de la défense aérienne et de la défense anti-drones. Eu égard à la normalisation des relations entre les États du Golfe et Tel-Aviv, il est improbable que des progrès rapides soient réalisés. Exception faite des pays ayant déjà signé les accords d'Abraham, ce processus se heurte en effet au fait qu'Israël est majoritairement perçu dans la région comme un pouvoir déstabilisateur et qu'il ne laisse apparaître aucune disposition à faire des concessions dans sa politique à l'égard des Palestiniens.

Après la fin de la guerre, l'avenir de la bande de Gaza dépendra largement de l'engagement des États-Unis et de la volonté du Hamas de

👁️ Que voit le SRC?

🔮 Que prévoit le SRC?

faire des concessions concernant son désarmement. En cas d'échec, il est prévisible qu'Israël maintienne une occupation permanente de certaines parties de la bande de Gaza et que la division de celle-ci en deux parties se pérennise. La situation en Cisjordanie, où les conditions de vie de la population palestinienne continuent de se détériorer et où le contrôle israélien s'oriente vers une annexion, présente également un risque d'escalade. Un renversement de cette tendance est très improbable.

En Syrie, le processus de transition reste fragile. Outre le soutien international, l'aptitude du gouvernement de transition à trouver un équilibre entre les minorités du pays sera déterminante. Si la construction d'une nouvelle structure étatique devait échouer, la Syrie risquerait de se fragmenter davantage, voire de sombrer dans une nouvelle guerre civile. Des acteurs terroristes tentent déjà de tirer parti des marges de manœuvre qui s'offrent à eux.

AFRIQUE



Le terrorisme, les guerres civiles et l'instabilité des gouvernements représentent d'importants défis pour l'Afrique en matière de politique de sécurité. Le terrorisme reste la principale menace dans ce domaine. Elle émane notamment de groupes djihadistes tels que le Jamaat Nusrat al-Islam wal-Muslimin, affilié à Al-Qaïda, et des provinces de l'«État islamique». Leurs ambitions expansionnistes exercent une pression croissante sur divers États. Du point de vue européen, c'est la menace qui pèse sur ses propres ressortissants sur place qui est actuellement au premier plan, car ni les appels répétés de l'«État islamique» à se rendre en Afrique, ni, à défaut, à commettre des attentats en Europe n'ont trouvé d'écho.

La rivalité entre les grandes puissances s'intensifie en Afrique, comme le montrent les investissements économiques, la présence militaire, les initiatives diplomatiques et l'influence technologique. Les États-Unis y renforcent leur présence afin de contrer l'influence croissante de la Chine et de la Russie. Ils ont annoncé un soutien économique et militaire de grande envergure. La loi sur la croissance et les possibilités économiques en Afrique (African Growth and Opportunity Act) accorde

aux pays africains un accès privilégié au marché américain. De son côté, la Chine continue également de consolider sa présence, en particulier par le biais de projets d'infrastructures. Elle a de plus conclu d'importants accords commerciaux et d'investissements avec plusieurs États africains. Quant à la Russie, elle prévoyait d'étendre sa présence militaire en Afrique grâce à une base militaire au Soudan destinée à servir de point d'appui stratégique pour des opérations dans la région. Fin 2025, ce projet a toutefois été «temporairement suspendu». La Russie entretient des relations étroites avec des pays tels que l'Afrique du Sud, l'Égypte et le Nigeria. Dans la zone du Sahel, des juntes militaires ont opéré des coups d'État et remplacé la présence militaire occidentale par des troupes russes et les sociétés minières occidentales par des entreprises russes ou chinoises.

De nombreux pays d'Afrique sont en proie à une instabilité politique, voire à une guerre civile. Les conflits au Soudan, en République démocratique du Congo et en République centrafricaine ont entraîné des crises humanitaires et des déplacements de population. Ces conflits peuvent conduire à une déstabilisation accrue de certaines régions d'Afrique, favoriser l'émer-

gence de groupes terroristes et de réseaux criminels et contribuer à une augmentation des flux migratoires vers l'Europe. À cet égard, les développements qui surviennent dans les pays d'Afrique du Nord comme la Libye, l'Algérie ou le Maroc jouent également un rôle important.



La population en Afrique va doubler entre 2020 et 2050 pour atteindre deux milliards de personnes. Outre le terrorisme et les conflits, le changement climatique qui progresse et les catastrophes environnementales qui en résultent représentent une menace grandissante. Les sécheresses et les inondations entraînent une insécurité alimentaire, des pénuries d'eau et des déplacements de population. Des phénomènes météorologiques extrêmes peuvent contribuer à des troubles sociaux et des conflits.

L'Afrique reste un théâtre important de la politique de puissance mondiale. Les grandes puissances et les puissances régionales émergentes défendent leurs intérêts dans la région

L'Afrique reste un théâtre important de la politique de puissance mondiale.

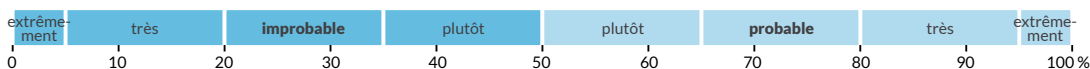
par le biais d'initiatives économiques, diplomatiques et militaires. Dans les années à venir, la Chine pourrait manifester son intérêt pour des bases militaires en Tanzanie, à Madagascar et peut-être en Guinée équatoriale sur la côte atlantique. Pour sa part, la Russie vise à développer sa présence militaire. Quant à la Turquie, elle a envoyé des troupes en Somalie et en Libye. En règle générale cependant, le «non-alignement» s'est à nouveau imposé comme la stratégie privilégiée sur le continent africain. Il permet en effet d'éviter les dépendances et de jouer sur la concurrence

entre grandes puissances pour obtenir une aide économique et des concessions politiques.

Avec la numérisation croissante, les cybermenaces se multiplient également en Afrique. Des cyberattaques peuvent toucher et affecter des infrastructures critiques telles que l'approvisionnement énergétique et les communications. La prolifération de drones est également une tendance qui menace d'aggraver les conflits et de déstabiliser encore davantage l'Afrique. En raison d'infrastructures insuffisantes et de ressources limitées, le continent africain est particulièrement exposé aux risques sanitaires. Les facteurs susmentionnés - effets du changement climatique, famines, augmentation du nombre de personnes déplacées à l'intérieur de leur propre pays, conflits liés aux matières premières et campagnes de désinformation menées par des acteurs extérieurs à l'encontre de l'Europe - aggravent encore la situation sécuritaire dans divers États africains. Les organisations terroristes en tireront profit pour étendre leur emprise territoriale et tenter de supplanter les institutions étatiques.

Ces développements et ces tendances en Afrique ne représentent pas une menace directe pour la Suisse, mais ils ont au fil du temps une incidence sur son environnement en matière de politique de sécurité. Ils jettent de premières ombres sur l'Europe et pourraient évoluer en menaces sérieuses au cours des prochaines décennies.

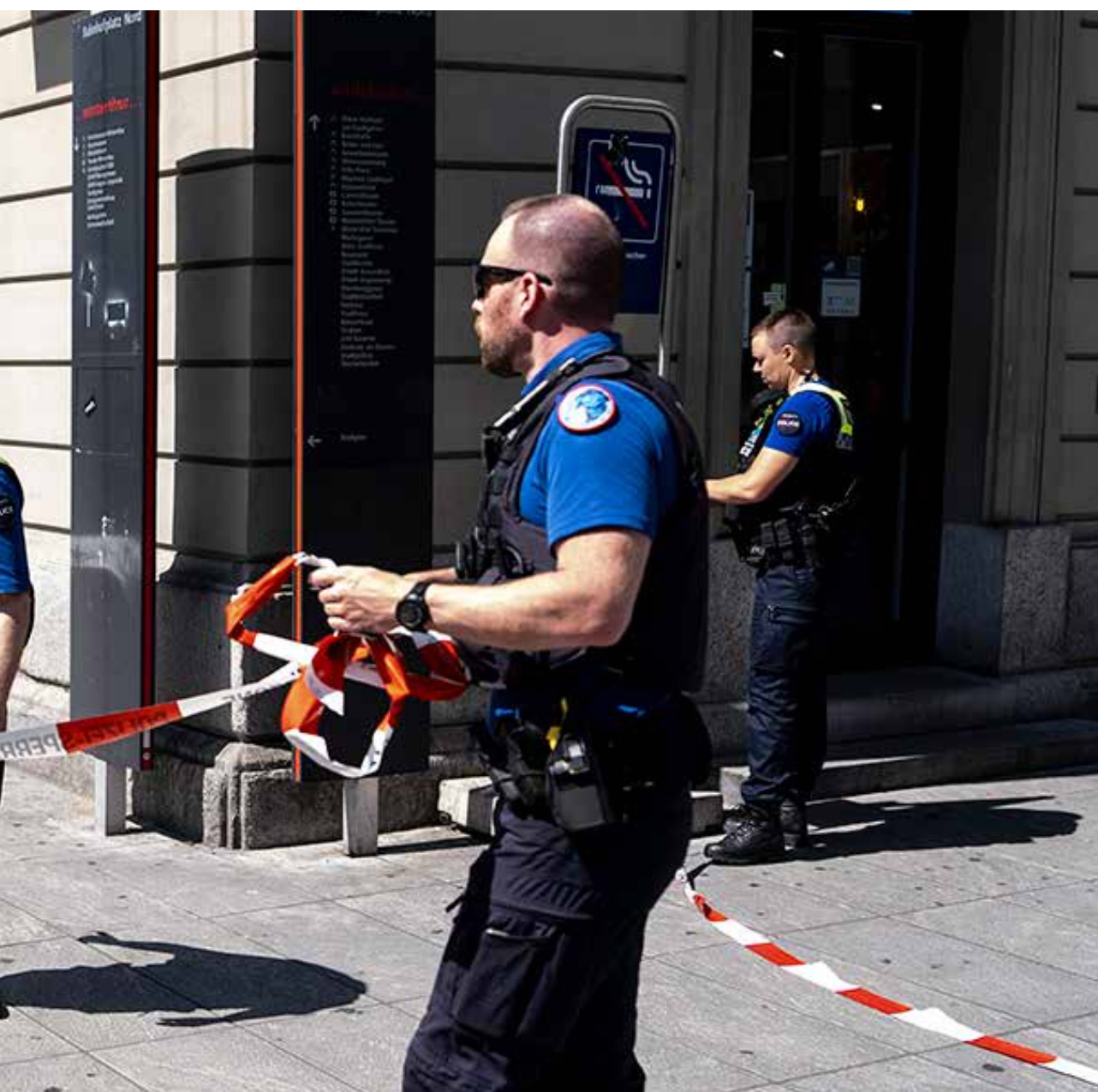
Échelle de probabilité



👁 Que voit le SRC?
🔮 Que prévoit le SRC?



TERRORISME



MENACE TERRORISTE EN SUISSE ET EN EUROPE



La menace terroriste en Suisse est élevée, ce qui signifie qu'il y a des informations sur des acteurs terroristes en Suisse et/ou sur des intentions terroristes contre la Suisse. La menace continue à être marquée avant tout par le mouvement djihadiste, plus particulièrement par des sympathisants de l'«État islamique» ou par des personnes inspirées par la propagande djihadiste. L'attaque au couteau commise le 28 mai 2026 à Winterthur par un individu radicalisé confirme cette appréciation.

Le phénomène de la radicalisation en ligne est prédominant en Suisse comme dans toute l'Europe. Dans le cyberspace, les courants extrémistes violents continuent de drainer à

Dans le cyberspace, les courants extrémistes violents continuent de drainer à eux les jeunes en particulier.

eux les jeunes en particulier. Dans le même temps, les radicalisations en ligne

s'opèrent de moins en moins souvent sous l'influence de groupes extrémistes violents et de l'idéologie qu'ils véhiculent. La fascination pour la violence, largement répandue, les parcours personnels, souvent marqués par des crises, ainsi que les conditions générales prévalant actuellement dans la société sont autant de facteurs qui touchent spécifiquement les jeunes. Un processus de radicalisation entamé sous ces auspices peut néanmoins aboutir à des actes de violence inspirés par le djihadisme.

Dans le domaine du djihadisme, la propagande de l'«État islamique» reste prépondérante en Suisse et en Europe. Toutefois, la majeure partie des contenus djihadistes qui circulent dans le cyberspace ne sont plus générés par les organes de communication centraux de l'«État

islamique» mais par des personnes ou de petits groupes agissant de manière décentralisée et autonome qui épousent sa cause.

Depuis la mi-mai 2025, le SRC a recensé, à l'échelle européenne, douze attentats en lien avec le terrorisme djihadiste. Le plus souvent, les victimes de telles attaques sont des personnes seules ou rassemblées dans une foule présentes par hasard sur le lieu de l'attentat. La totalité de ces attentats ont été commis avec des moyens rudimentaires et la plupart de leurs auteurs n'étaient pas connus des autorités de sécurité avant leur acte. Tous ont agi de manière autonome et sans lien direct avec l'«État islamique» ou une autre organisation terroriste. Aucun de ces attentats n'a été revendiqué par un groupe djihadiste.

Même après l'attaque terroriste de grande ampleur perpétrée par le Hamas le 7 octobre 2023, le conflit au Proche-Orient n'est pas un thème central pour les individus concernés par la radicalisation djihadiste en Suisse et en Europe. Ce conflit attise toutefois des actions antisémites qui, à l'étranger, ont parfois débouché sur des actes de violence djihadistes - comme le 2 octobre 2025 lors de l'attaque contre une communauté juive à Manchester (Royaume-Uni) et le 14 décembre 2025 lors d'une célébration de la fête juive de Hanoukka à Sydney (Australie). En Europe, ce conflit a donné lieu à maintes déclarations exprimant des intentions d'attentat et, à plusieurs reprises, des projets d'attentat contre des cibles juives ou israéliennes ont été déjoués. Dans ce contexte, tant l'«État islamique» qu'Al-Qaïda ont appelé de manière répétée à commettre des attentats contre des cibles juives et israéliennes. Le 18 septembre 2025 par exemple, l'«État

islamique» a lancé un appel adressé spécifiquement à ses jeunes partisans les incitant explicitement à commettre des attentats contre des cibles juives et chrétiennes en Europe. L'appel le plus récent de l'«État islamique» à commettre des attentats contre des cibles juives date du 2 avril 2026.

Depuis 2022, le nombre de voyages en lien avec le djihad entrepris depuis l'Europe augmente à nouveau quelque peu. Plusieurs dizaines de cas d'individus qui voulaient rejoindre un groupe de l'«État islamique» en Afrique, au Proche-Orient ou en Asie ont été constatés à l'échelle européenne. La plupart du temps, leurs projets ont échoué en raison de conditions générales difficiles ou de l'intervention des autorités de sécurité. En Suisse, un tel cas a été relevé pour la dernière fois en juillet 2024, lorsqu'un Suisse de 21 ans a été arrêté alors qu'il avait l'intention de rejoindre l'«État islamique» en Somalie. À l'heure actuelle, des dizaines de ressortissants européens qui avaient rejoint l'«État islamique» en Syrie et en Irak dès 2014 en tant que combattants djihadistes ne se trouvent plus dans les camps et les prisons kurdes du nord-est de la Syrie, mais sont détenus par les autorités irakiennes. Parmi eux figurent trois ressortissants suisses. Une Suissesse accompagnée de sa fille se trouve encore dans un camp kurde au nord-est de la Syrie.



Le phénomène de la radicalisation djihadiste en ligne continuera de marquer la menace terroriste en Suisse. Cette menace reste diffuse, en particulier dans le cyberspace. En effet, la fascination pour la violence ou des problèmes personnels ou psychologiques deviennent de plus en plus souvent des facteurs déterminants chez les suspects,

alors que les motivations idéologiques perdent en importance. Il demeure par ailleurs difficile d'évaluer le sérieux des menaces de violence, notamment lorsqu'elles sont proférées par des jeunes dans le cyberspace. Dans le cas d'actes de violence en Europe, on constate que le soupçon initial de terrorisme s'avère de plus en plus souvent erroné, respectivement que les motifs ne relèvent pas clairement du djihadisme. Il est probable que cette tendance se poursuive.

En Suisse, la menace terroriste la plus importante émane toujours d'individus isolés ou de petits groupes inspirés par le djihadisme qui commettraient spontanément des actes de violence avec des moyens simples. Les cibles difficiles à protéger sont les plus susceptibles d'être visées. Pour les djihadistes, de grandes manifestations ou des événements attirant une foule dans l'espace public restent des occasions idéales de traduire leurs intentions d'attentat en actes.

La dynamique persistante des conflits au Proche et Moyen-Orient dans lesquels Israël est impliqué accroît le risque d'actes de violence à motivation djihadiste contre des intérêts juifs ou israéliens en Europe. Cela est également valable pour la Suisse.

Les djihadistes libérés de prison ainsi que les individus qui se sont radicalisés au cours de leur détention représentent un facteur de risque qui perdure. La problématique du retour éventuel de voyageurs du djihad ayant des liens avec la Suisse reste également d'actualité, car la manière dont se développera la situation des personnes anciennement détenues dans le nord-est de la Syrie reste peu claire.

**ACTES VIOLENTS AVEC
SOUPÇON DE TERRORISME**

- Motivation djihadiste
- Motivation djihadiste pas claire

- Incendie criminel
- Attaque au couteau
- Attaque à la voiture-bélier
- Emploi d'armes à feu

Espace Schengen

MANCHESTER
02.10.2025

GOLDERS GREEN
29.04.2026

DUBLIN
25.07.2025

DUBLIN
29.07.2025

BIELEFELD
18.05.2025

ESSEN
05.09.2025

WINTERTHOUR
28.05.2026

MADRID
22.11.2025

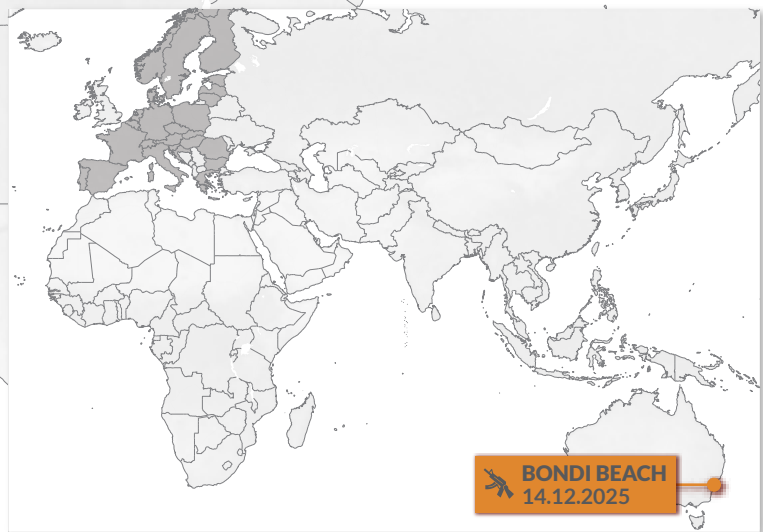
ISTANBUL
07.04.2026

SKOPJE
12.04.2026

PARIS
13.02.2026

LYON
10.09.2025

**ÉVÉNEMENTS DANS LE DOMAINE DU TERRORISME
À MOTIVATION DJIHADISTE EN EUROPE DEPUIS MAI 2025**



LES NOUVELLES TECHNOLOGIES MODIFIENT LA MENACE TERRORISTE

Bien souvent, les acteurs terroristes réagissent rapidement à l'émergence de nouvelles technologies qui sont accessibles au grand public, peu réglementées et ont un prix abordable, ou sont gratuites. L'«État islamique», par exemple, a dès le début résolument misé sur l'utilisation de la toute dernière génération de réseaux sociaux et d'applications de communication gratuites comme Telegram, décision qui s'est avérée un facteur de succès essentiel pour l'organisation terroriste: ses capacités en matière de propagande, de recrutement et de sécurité des communications se sont considérablement accrues. Les cryptomonnaies, auxquelles les acteurs terroristes recourent de plus en plus, sont un autre exemple.

en particulier lorsqu'elle se verra associée à d'autres technologies. C'est le cas par exemple dans le domaine de la technologie des drones utilisés à des fins offensives. Ayant connu un développement fulgurant depuis le début de la guerre contre l'Ukraine, cette technologie est en partie accessible au grand public. Depuis 2023, des groupes islamistes violents au Proche-Orient, en Afrique et en Asie recourent eux aussi de plus en plus à des drones armés. Les capacités de ces groupes ne cessent de s'accroître en raison de l'évolution rapide de la technologie des drones et d'un intense transfert de connaissances.

Pour toutes les nouvelles technologies, des efforts sont certes déployés au niveau international grâce à des réglementations légales et des mesures de protection mises en place par des entreprises privées pour contrer les abus commis par des acteurs terroristes. Ces dernières années, la régulation étatique des grandes plateformes en ligne a fait des progrès significatifs. Conséquence: les exploitants de ces plateformes ont adapté leurs directives et intensifié la lutte contre les contenus djihadistes. Toutefois, jusqu'à présent, ces mesures n'ont guère permis d'endiguer le phénomène de la radicalisation en ligne. Les raisons peuvent en être multiples. Reste que les djihadistes, compte tenu du développement rapide des technologies et du marché dans ce domaine, sont toujours à même de se tourner vers des produits alternatifs ou d'utiliser de nouvelles technologies pour dissimuler leurs activités en ligne. De plus, les jeunes générations acquièrent tôt et plus facilement de nouvelles compétences technologiques.

Le développement exponentiel de l'intelligence artificielle recèle un important potentiel par rapport au renforcement de la menace djihadiste à l'avenir.

Le développement exponentiel de l'intelligence artificielle recèle un important potentiel par rapport au renforcement de la menace djihadiste à l'avenir. Le problème ne réside pas seulement dans l'utilisation déjà quotidienne de l'IA par les djihadistes mais aussi dans son emploi par des entreprises technologiques dans le domaine des réseaux sociaux. L'expérience montre notamment que l'emploi de l'intelligence artificielle dans les algorithmes de plateformes telles que TikTok favorise les processus de radicalisation.

À l'avenir, l'intelligence artificielle aura des répercussions dans de nombreux domaines et posera vraisemblablement de nouveaux défis en matière de lutte contre le terrorisme,

ACTEURS DJIHADISTES HORS D'EUROPE



Les groupes terroristes liés à l'«État islamique» ou Al-Qaïda influencent directement la menace en Europe avec leurs activités de propagande et de recrutement. En même temps, leur capacité à préparer ou commettre des attentats en Europe de manière autonome est très limitée. Ils sont en effet largement tributaires de partisans résidant sur sol européen qu'il s'agit de trouver et d'inciter à commettre des actes violents, voire de guider à cette fin.

L'«État islamique» en Syrie met à profit le vide de pouvoir créé par la chute du régime de Bachar el-Assad et la situation sécuritaire toujours précaire dans de vastes régions du pays pour se restructurer et se renforcer, notamment en intensifiant son recrutement. L'avancée de l'armée syrienne dans les zones kurdes a entraîné des mouvements de fuite depuis les camps et les prisons du nord-est de la Syrie. Il est cependant plutôt probable que l'«État isla-

mique» ne dispose pas des capacités suffisantes pour accueillir toutes les personnes qui se

Les fugitifs pourraient tenter de retourner dans leur pays. Aucun signe d'une vague de retours n'est toutefois constaté pour l'instant.

sont enfuies. Les fugitifs pourraient par ailleurs tenter de retourner dans leur pays. Aucun signe d'une vague de retours n'est toutefois constaté pour l'instant.

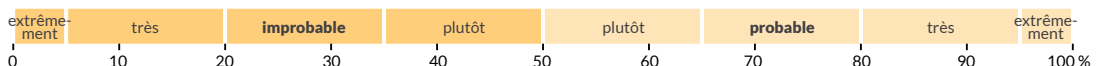
Le gouvernement de transition syrien tente certes, comme il l'a officiellement annoncé, de lutter contre les groupes radicaux ou djihadistes. Le manque de contrôle sur de vastes zones de la Syrie ainsi que l'insuffisance des ressources humaines et financières rendent toutefois difficile toute action efficace. Aujourd'hui comme hier, il faut donc attendre de l'«État islamique»

qu'il mène plutôt des attaques surprises faciles à réaliser. Reste qu'il n'abandonnera pas ses tentatives de commettre des attentats contre des cibles à haute valeur ajoutée. Outre les représentants du gouvernement de transition syrien, ce sont les ressortissants d'États occidentaux et les intérêts occidentaux en Syrie qui se trouvent dans sa ligne de mire.

Les capacités de l'État islamique au Khorasan à mettre en œuvre des plans d'attentat contre des cibles en Europe ont atteint leur niveau le plus bas en 2025 en raison de la forte pression internationale exercée contre cette organisation basée en Afghanistan et au Pakistan. L'arrestation d'Özgür Altun au Pakistan en avril 2025 a signifié une interruption de la parution de son magazine en ligne en anglais *Voice of Khorasan*, cela jusqu'en janvier 2026. Ce magazine en ligne offre des adresses de contact et constitue donc un point d'accès direct pour les personnes radicalisées sur sol européen. En Europe, l'État islamique au Khorasan reste tributaire de partisans vivant sur le continent et susceptibles de se laisser inciter à commettre des actes violents. Les réseaux internationaux de ce groupe ne présentent que des liens marginaux avec la Suisse.

En Afrique, les provinces de l'«État islamique» se sont étendues et établies de manière croissante. Malgré les pertes humaines et matérielles causées par les opérations antiterroristes, les structures des provinces africaines de l'«État islamique» restent opérationnelles et leurs réseaux presque intacts. Des structures étatiques faibles, tant en termes de légitimité que de garantie de la sécurité, offrent des conditions favorables à l'expansion des groupes djihadistes. D'autres facteurs tels que les effets du changement climatique, les famines, les migrations, les conflits ethniques, la raréfaction des

Échelle de probabilité



ressources, la croissance démographique, ainsi que l'influence militaire et économique et les campagnes de désinformation anti-européennes d'acteurs extérieurs, s'affermissent mutuellement et aggravent la situation sécuritaire dans plusieurs États africains.

Ces dernières années, le noyau dur d'Al-Qaïda et ses sous-groupes se sont principalement concentrés sur des agendas régionaux. Les plateformes médiatiques d'Al-Qaïda et les portails proches de cette organisation appellent régulièrement à des actions violentes aux États-Unis et en Europe, ainsi qu'à des atteintes aux intérêts israéliens dans le monde. Néanmoins, comparée à celle de l'«État islamique», la propagande d'Al-Qaïda n'obtient toujours que peu d'écho en Europe.



La situation ne se modifiera pas de manière significative d'ici la fin 2026 : il est probable que les organisations terroristes djihadistes au Proche-Orient, en Afrique et en Asie continueront à suivre en priorité un agenda à l'échelle régionale. Il est cependant plutôt probable qu'elles accroissent en même temps leurs ressources et développent leurs capacités opérationnelles. Cela accentuera la menace qui pèse sur les intérêts occidentaux dans ces régions.

Il est très probable que l'«État islamique» en Syrie tirera profit de la situation instable et des animosités croissantes entre les différents groupes de population, ce qui lui permettra d'accélérer son nouvel essor. Il est aussi probable qu'un État islamique renforcé incitera des individus radicalisés à le rejoindre – et cela pas uniquement en Syrie. Grâce aux contacts suprarégionaux avec ses provinces, le transfert de combattants, de savoir-faire et de moyens

financiers est facilité. Avec l'Europe, des contacts sporadiques existent; ces contacts pourraient devenir plus nombreux à l'avenir et accroître le potentiel de menace à l'encontre de la Suisse et de l'Europe. Les personnes de retour de zones de djihad représentent également une menace pour la sécurité de l'Europe et de la Suisse.

Les informations laissant présumer que l'État islamique au Khorasan est en phase de réorganisation et que l'affaiblissement de ses réseaux internationaux n'est peut-être que temporaire se multiplient. Cependant, même s'il parvient à reconstruire son appareil de propagande et son réseau international, il lui faudra du temps pour retrouver le niveau des capacités qu'il avait en 2024.

Il est probable que les provinces africaines de l'«État islamique» ainsi que les sous-groupes africains d'Al-Qaïda continueront de profiter de l'amélioration de leurs conditions générales. Ces groupes intensifieront le recrutement et l'acquisition de moyens financiers et matériels.



LUTTE CONTRE LE TERRORISME

Le SRC publie deux fois par année sur son site Internet des chiffres en rapport avec la lutte contre le terrorisme (personnes représentant un risque, voyageurs à motivation djihadiste et monitoring de sites Internet présentant un contenu djihadiste).

www.src.admin.ch
> Sécurité > Renseignement > Terrorisme

PKK

- 👁️ Le Parti des travailleurs du Kurdistan (PKK) a annoncé sa dissolution en mai 2025, annonce qu'il a fait suivre de mesures symboliques communiquées de manière à trouver un large écho dans les médias. Ses structures persistent toutefois et restent actives. En tant que représentant autoproclamé des Kurdes en Europe, le PKK aspire à la reconnaissance de l'identité kurde en Turquie, en Syrie, en Irak et en Iran. En Suisse, comme ailleurs en Europe, il continue de collecter des fonds clandestinement, de mener des actions de propagande et d'organiser des camps destinés à la formation idéologique et au recrutement.
- 🕒 Le PKK maintient son objectif de se voir retiré de la liste des organisations terroristes de l'UE. Il continuera de respecter son principe de renoncement à la violence en Europe tout en poursuivant ses activités parfois clandestines. Suite à l'annonce de sa dissolution, le PKK s'efforce d'empêcher les luttes de pouvoir internes et les scissions qui pourraient en résulter. Selon la pression exercée par le gouvernement turc et l'évolution de la situation dans les régions kurdes du nord de la Syrie, des tensions et des manifestations de protestation sont également à prévoir en Suisse.

TERRORISME ETHNO-NATIONALISTE ET D'AUTRE PROVENANCE

HAMAS

- 👁️ La loi fédérale interdisant le Hamas et les organisations apparentées est entrée en vigueur le 15 mai 2025. Les autorités fédérales ont ainsi obtenu les instruments nécessaires pour lutter contre les activités du Hamas ou le soutien apporté à cette organisation en Suisse – notamment en matière de financement et de propagande. Cette organisation n'envisage officiellement aucun acte terroriste en Europe, cela ne fait pas partie de sa doctrine. Le réseau international du Hamas se concentre principalement sur la politique et le financement. Des rapports font état de plans d'attentat en Europe à fin 2023 ainsi qu'en 2025 qui seraient en lien avec le Hamas, mais les relations entre leurs auteurs et l'organisation n'ont pas encore été clairement établies. Ces dernières années, certains dirigeants du Hamas ont toutefois appelé à attaquer des Israéliens et des juifs en dehors d'Israël et du territoire palestinien.
- 🕒 Une confirmation que le Hamas planifie des attentats en Europe représenterait une nouvelle menace pour les intérêts juifs et israéliens en Suisse également. Pour l'heure, il est plutôt improbable que le Hamas ou une partie de cette organisation commettent un attentat terroriste en Europe.

IRAN

👁️ Les services de renseignement iraniens et plusieurs proxys de l'Iran ont ces dernières années été impliqués dans la préparation d'activités terroristes en Europe.

🕸️ L'Iran pourrait réagir de manière asymétrique aux attaques israéliennes et américaines. Les méthodes asymétriques comprennent des attentats terroristes, par exemple contre des cibles israéliennes, juives ou américaines. Les services iraniens, des proxys ou des réseaux criminels à leur solde pourraient commettre de tels attentats. Il est en outre probable que les services iraniens renforcent leur surveillance des membres de l'opposition résidant en Suisse et qu'ils agissent de manière plus agressive à leur encontre. Des menaces, voire des atteintes à l'intégrité physique, entrent alors en ligne de compte.

Des actions spontanées pourraient en outre être menées par des personnes radicalisées qui partagent l'idéologie du régime iranien sans être liées à celui-ci sur le plan organisationnel. De telles attaques viseraient principalement des cibles de manière opportuniste.

HEZBOLLAH

👁️ Le Hezbollah entretient au sein de la diaspora chiite libanaise en Suisse un réseau qui soutient l'organisation dans ses affaires communautaires et politiques. Certaines de ces personnes pourraient également être mobilisées pour soutenir le Hezbollah lors d'actions terroristes. En décembre 2024, les deux Chambres fédérales ont adopté une motion visant à interdire le Hezbollah en Suisse et ont chargé le Conseil fédéral de sa mise en application.

🕸️ La menace que représente le Hezbollah libanais en Europe dépendra de l'intensité du conflit entre Israël et le Hezbollah, d'une part, entre l'Iran et les États qu'il considère comme hostiles, d'autre part. Le Hezbollah pourrait certes étendre le conflit en menant des attentats en dehors du Proche-Orient, mais il se concentrera plus probablement sur des opérations menées sur territoire libanais et contre l'armée israélienne.



EXTRÉMISME VIOLENT



LE POTENTIEL DE VIOLENCE RESTE ÉLEVÉ

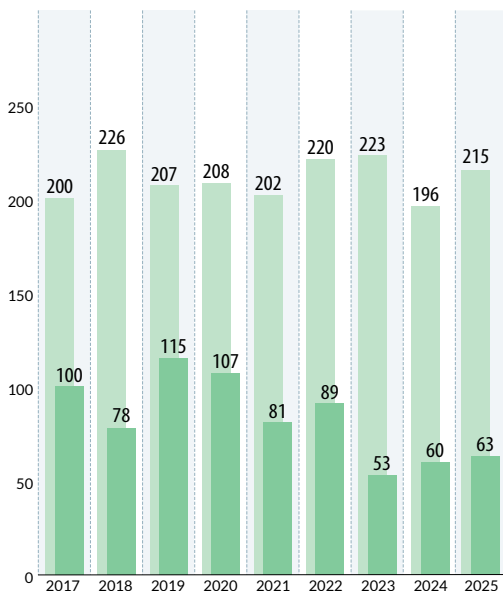


Les extrémistes de gauche et de droite violents poursuivent leurs activités. Les tendances observées ces dernières années se confirment : ces deux milieux se concentrent essentiellement sur les thèmes qu'ils exploitent depuis des années et ils s'en tiennent à leurs modes d'action habituels pour attirer l'attention sur eux. Lorsque la violence est visible dans l'espace public, ce sont principalement des membres des milieux d'extrême gauche qui en sont à l'origine. Cependant, ni l'extrême gauche ni l'extrême droite violentes ne parviennent à affaiblir de manière perceptible la démocratie et les principes de l'État de droit ou à influencer notablement les processus politiques. Les membres des deux camps suivent des entraînements aux sports de combat.

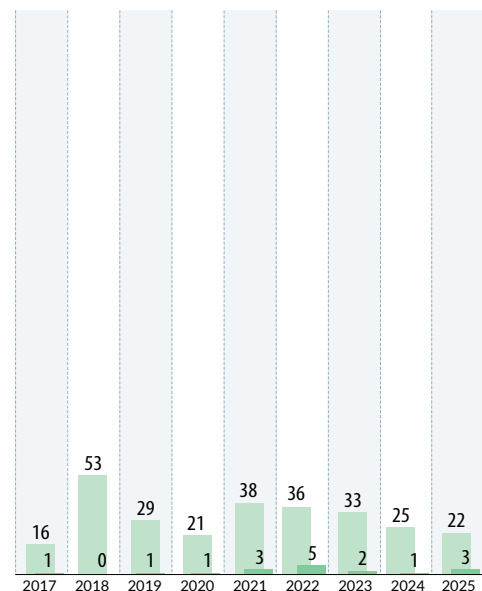
Le potentiel de violence dans les milieux d'extrême gauche violents est élevé. Actuellement, le thème qui domine est celui des conflits au Proche et Moyen-Orient et leurs multiples facettes, comme par exemple la cause palestinienne et kurde, ainsi que l'anti-impérialisme et l'anticapitalisme. Ces sujets sont de nature à inciter également de nombreuses personnes modérées à participer à des rassemblements de protestation. Les milieux d'extrême gauche violents instrumentalisent ces manifestations, les employant comme plateformes pour faire usage de violence. Les actions violentes sont dirigées en particulier contre des institutions associées aux États-Unis et à Israël ou liées à leur armement et à leur financement. Le groupe Action Palestine, interdit en Grande-Bretagne, appelle par exemple à des actions

Événements motivés par l'extrémisme violent annoncés au SRC depuis 2017 (sans les graffitis)

Extrémisme de gauche



Extrémisme de droite



violentes contre les entreprises d'armement et les ministères de la défense dans le monde entier. La lutte contre le fascisme bénéficie en outre toujours d'une priorité élevée. L'actualité internationale influence les activités des milieux d'extrême gauche violents plus fortement que celles des milieux d'extrême droite violents. Les grands événements, en particulier ceux ayant une orientation économique marquée comme le Forum économique mondial (World Economic Forum, WEF) ou un sommet du G7, requièrent le plein engagement des autorités de sécurité, y compris la mise en place du Réseau de renseignement (voir « chiffres clés 2025 », p. 73), afin de se prémunir contre ce potentiel de violence.

Certains groupes d'extrême droite violents se manifestent souvent par des actions publiques et diffusent des séquences vidéo de ces actions sur des canaux librement accessibles en ligne. Des actions violentes sont menées contre des hommes que certains membres des milieux d'extrême droite violents accusent de pédophilie.

En Suisse, le phénomène des *Staatsverweigerer*, qui ne reconnaissent pas les autorités et contestent la légitimité de l'État démocratique, est représenté par un certain nombre de personnes. Parmi elles, certaines sont d'extrême droite et sont prêtes à faire usage de violence pour s'opposer à des actes administratifs relevant de la souveraineté étatique.

L'évolution de la situation dans le domaine de l'extrémisme violent a conduit le Conseil fédéral à proposer, dans le cadre de la révision en cours de la loi sur le renseignement, l'introduction de mesures de recherche soumises à autorisation, telles que la surveillance de la correspondance par poste et télécommunication, l'utilisation d'appareils de localisation et d'autres appareils de surveillance, y compris dans des lieux qui ne sont pas publics ou qui ne sont pas librement accessibles, ou l'intrusion dans

des systèmes informatiques et des réseaux informatiques, également pour détecter et contrer les menaces que représentent les activités extrémistes violentes.



Les membres des deux milieux extrémistes violents en Suisse poursuivront leurs activités. Ils s'orienteront pour ce faire essentiellement suivant les thèmes et les points forts qui les ont guidés jusqu'à présent.

Les thèmes en lien avec les conflits au Proche et Moyen-Orient, la cause palestinienne en particulier, continuent de gagner en importance pour les milieux d'extrême gauche violents, leur donnant même un nouvel élan. Si aucun apaisement notable ne se produit dans ces conflits, les groupes qui n'hésitent pas à faire usage de violence lors de manifestations resteront actifs. Les violentes émeutes qui ont eu lieu lors de la manifestation pro-palestinienne à Berne en octobre 2025, avec de nombreux blessés et de très importants dégâts matériels, l'ont clairement démontré. Les auteurs de violences, dont un nombre important provenaient de Suisse romande, n'ont pas hésité à commettre des atteintes à l'intégrité physique, attaquant des membres des forces de sécurité et mettant en danger des passants. La question de savoir si les voix qui se sont élevées pour désapprouver ces actes de violence parviendront à s'imposer au sein de ces milieux reste ouverte. L'existence d'un débat à ce propos montre toutefois que l'extrême gauche violente dispose d'une large base et qu'elle est diversifiée.

Les thèmes en lien avec les conflits au Proche et Moyen-Orient, la cause palestinienne en particulier, continuent de gagner en importance pour les milieux d'extrême gauche violents, leur donnant même un nouvel élan.

La violence et le sabotage sont considérés comme des moyens éprouvés également lors

d'actions menées, par exemple, contre des entreprises commerciales et des infrastructures ferroviaires ou de télécommunications en Suisse et dans d'autres pays européens. En témoigne l'incendie criminel perpétré par un groupe anarchiste contre le réseau électrique berlinois en janvier 2026. Bien que moins présente, la cause kurde reste importante pour les milieux d'extrême gauche violents.

À maintes reprises, des extrémistes de gauche violents ont entravé directement des processus démocratiques en perturbant, voire en empêchant, des interventions de magistrats ou de personnes issues du monde des affaires. Les changements qui surviennent dans la situation internationale servent alors de motif de mobilisation.

Comparé aux années précédentes, les membres des milieux d'extrême droite violents se montrent souvent plus discrets et plus réfléchis dans leur propos. Cela attire de nouveaux partisans vers certains groupes. La menace émanant des extrémistes de droite violents persiste : les personnes agissant en dehors des structures organisées de l'extrême droite représentent une menace plus importante que les groupes dans leur ensemble. Les cas de jeunes adultes

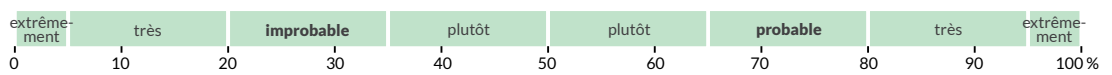
ou de mineurs qui se radicalisent en ligne via les réseaux sociaux et les plateformes de jeux continuent en particulier d'augmenter. L'espace numérique reste un vecteur central pour la diffusion de propagande.

Dans des groupes de discussion fermés liés à l'accélérationnisme, des représentations d'une violence extrême continuent d'être partagées. On y exprime aussi des intentions d'utiliser la violence. Les partisans de l'accélérationnisme croient que la société démocratique est vouée à l'effondrement et que cet effondrement doit être précipité par l'usage de la violence afin que soit établi un nouvel ordre autoritaire. Ce développement laisse présager la formation de réseaux en ligne où des éléments idéologiques se mêlent à des représentations occultes et marquées par la cruauté. De plus en plus fréquemment relégué au second plan, l'aspect idéologique ne sert plus qu'à légitimer la violence.

L'intérêt déjà marqué des extrémistes de droite violents pour les entraînements aux sports de combat devrait se maintenir, voire s'accroître.

Certains *Staatsverweigerer* continueront de s'opposer à des actes relevant de la souveraineté étatique, en usant ponctuellement de violence.

Échelle de probabilité





SITUATION GÉNÉRALE



La tendance mondiale au réarmement se manifeste aussi bien dans le domaine des armes conventionnelles que dans celui des armes nucléaires, biologiques et chimiques et de leurs vecteurs. Les États investissent des sommes considérables dans leur développement et leur modernisation, ce qui renforce également l'importance stratégique de certaines technologies clés: divers acteurs étatiques cherchent par exemple à accéder à la technologie quantique, à l'intelligence artificielle, à la robotique, aux biotechnologies et aux technologies spatiales, tout en tentant d'en priver d'autres acteurs étatiques.

Dotée d'un haut degré de spécialisation, la place industrielle et de recherche suisse est particulièrement touchée. La Russie s'efforce par exemple de contourner les sanctions et d'acheter des machines-outils en Suisse pour le compte de son complexe militaro-industriel. La Chine, quant à elle, prospecte notre pays à la recherche de connaissances et de technologies revêtant un potentiel stratégique et militaire. L'Iran et la Corée du Nord s'intéressent également à des biens suisses pour leurs programmes d'armes stratégiques.

Les réseaux et méthodes d'acquisition sont toujours plus complexes et mieux dissimulés. Au niveau international, les mécanismes et instruments de lutte contre la prolifération ont été affaiblis par la remise en question du multilatéralisme. La Russie, ainsi que des intérêt

nationaux marqués par toujours plus de divergences, entravent les efforts visant à faire évoluer les régimes de contrôle à l'exportation de manière appropriée. Par ailleurs, le développement de multiples technologies potentiellement disruptives complique nettement la lutte contre la prolifération. Cette situation se reflète clairement à plusieurs niveaux: les listes de biens à double usage deviennent plus longues et plus complexes, et la tension entre l'attrait de la recherche scientifique internationale et le besoin de protéger les intérêts nationaux s'accroît. Face à cette évolution, les intérêts économiques se heurtent de plus en plus à des risques de prolifération.



La concurrence mondiale dans les domaines industriels et technologiques se poursuivra. La majorité des États occidentaux continueront à tenter d'empêcher la Russie de renforcer ses capacités militaires et la Chine d'acquérir des avantages technologiques décisifs. Toutes les parties maintiendront une forte pression sur la Suisse: il deviendra plus difficile de préserver sa souveraineté en matière de lutte contre la prolifération et de contrôle des exportations. La portée des instruments traditionnels de maîtrise des armements continuera de faiblir. Les réseaux d'acquisition resteront actifs en Suisse.

Toutes les parties maintiendront une forte pression sur la Suisse.

RUSSIE



La Russie poursuit la modernisation de son arsenal nucléaire, et en particulier de ses vecteurs. Les problèmes rencontrés lors de la conception du missile balistique lourd de portée intercontinentale n'ont toutefois pas été résolus. Le dernier essai en date, réalisé en 2025, s'est également soldé par un échec.

Les drones jouent un rôle déterminant dans le cadre de la guerre contre l'Ukraine, même s'ils ne remplacent pas entièrement les armes à longue distance conventionnelles comme l'artillerie, les missiles balistiques et les missiles de croisière. Ce phénomène accélère le développement de ces systèmes d'armes et de la guerre électronique. Il en découle un besoin important en biens industriels, dont la Russie doit parfois faire l'acquisition dans des États occidentaux.

La Russie a élaboré des stratégies complexes pour soutenir son effort de guerre, y compris à l'aide de biens et de technologies suisses. Ses services de renseignement font partie intégrante de ces stratégies, tout comme le recours à des réseaux spécifiques en Suisse et à l'étranger. Les transferts de biens suisses vers la Russie depuis des pays tiers augmentent. Il en va de même pour l'utilisation dans des pays tiers de produits suisses afin de fabriquer des biens destinés à la Russie. Les États qui n'ont pas adopté les sanctions contre la Russie, à l'instar de la Turquie, des Émirats arabes unis et de la Chine, sont utilisés pour contourner les sanctions et les mesures de contrôle en matière d'exportation de biens à double usage. L'industrie des machines-outils est particulièrement touchée, de même que les secteurs du matériel de laboratoire et de la microtechnique.

La Russie n'annonce plus les vols d'essai de missiles balistiques comme le prévoit l'instrument multilatéral qu'est le Code de conduite de La Haye. En Ukraine, elle a eu recours à

plusieurs reprises à la chloropicrine, une arme chimique. Ces violations du droit international et d'autres normes ont des effets déstabilisants et illustrent parfaitement l'érosion des accords multilatéraux.



La Russie poursuivra ses efforts en vue d'approvisionner son complexe militaro-industriel en biens et technologies suisses. Il est probable que le recours à des pays tiers pour contourner les sanctions et règlements en matière de biens à double usage augmentera. Des biens suisses peuvent être réexportés depuis ces pays tiers, ou des biens peuvent être élaborés au moyen de produits et technologies suisses dans ces pays tiers, puis livrés à la Russie.

La Russie poursuivra ses efforts en vue d'approvisionner son complexe militaro-industriel en biens et technologies suisses.

Des États qui fournissent un soutien militaire à l'Ukraine et qui œuvrent à affaiblir la Russie pourraient estimer que la mise en œuvre par la Suisse des sanctions contre la Russie est insuffisante, ce qui pourrait se traduire par des conséquences négatives pour l'économie et la collaboration en matière de politique de sécurité.

La Russie ne renouera pas avec le respect des accords internationaux dans un avenir proche. Ainsi, le traité New START de réduction des armes nucléaires stratégiques conclu entre la Russie et les États-Unis est arrivé à expiration en février 2026. La Russie va en revanche continuer à moderniser son arsenal de missiles balistiques intercontinentaux. Les tests réussis de ces vecteurs seront exploités dans le cadre de sa propagande.

CHINE



La Chine se sert de ses atouts économiques comme d'un levier géopolitique. La stratégie de fusion militaro-civile élaborée sous la direction de Xi Jinping, chef de l'État et du Parti communiste, encourage l'utilisation de technologies potentiellement disruptives à des fins militaires. Dès lors, les contrôles à l'exportation harmonisés au niveau international dans le domaine des biens à double usage et la sécurité des connaissances gagnent en importance, tandis que le blocage et l'affaiblissement des régimes multilatéraux traditionnels profitent à la stratégie chinoise.

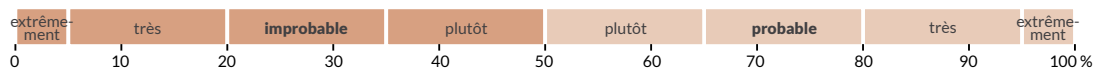
Pour de nombreux pays, dont la Suisse, la Chine est un partenaire commercial et technologique de premier plan, voire indispensable. Si cette collaboration porte ses fruits à bien des égards dans le domaine commercial et scientifique, elle comporte toutefois des risques. Dotés d'un niveau de spécialisation élevé, l'industrie et le potentiel d'innovation disponibles en Suisse offrent des opportunités particulièrement intéressantes en matière d'acquisition technologique.

Les acteurs chinois intéressés par l'acquisition de connaissances et de technologie suisses peuvent recourir à un large éventail de méthodes légales et illégales :

- L'espionnage, le vol de propriété intellectuelle et les abus dans le cadre de collaborations scientifiques sont une réalité pour les instituts de recherche, les universités, les entreprises industrielles, les start-ups et les spin-offs suisses.
- L'acquisition de connaissances par des moyens légaux constitue un défi encore plus important. Que ce soit via des exportations de biens, des investissements étrangers dans des entreprises, la collaboration dans le domaine de la recherche académique, les bourses de recherche ou le recrutement de talents, l'acquisition de connaissances technologiques prend de l'ampleur. Les acteurs chinois actifs dans ces domaines s'appuient sur une bonne compréhension des bases juridiques et des réglementations locales.

Depuis 2010, la Chine a considérablement développé son arsenal nucléaire et en a constamment modernisé la qualité grâce à de nouveaux systèmes d'armes. On ignore encore jusqu'où elle ira dans cette voie. Officiellement, elle s'en tient à sa doctrine, qui consiste à s'abstenir de recourir en premier aux armes nucléaires.

Échelle de probabilité





En Europe, les milieux politiques, économiques et scientifiques multiplient les efforts pour contrôler les transferts de technologie vers l'étranger, et vers la Chine

en particulier. En Suisse, malgré des initiatives encourageantes, les mesures et mécanismes visant à sécuriser les connaissances et à contrôler les investissements

En Europe, les milieux politiques, économiques et scientifiques multiplient les efforts pour contrôler les transferts de technologie vers l'étranger, et vers la Chine en particulier.

font face à des défis toujours plus importants compte tenu de la complexité croissante des méthodes d'acquisition indésirable de technologies. Or, les failles restantes pourraient être exploitées par des acteurs malveillants. Une augmentation du nombre d'incidents en rapport avec l'acquisition de technologies suisses ou étrangères dans notre pays comporterait non seulement des risques en termes de réputation, mais pourrait aussi entamer la volonté de coopération de partenaires internationaux. Le potentiel d'innovation et de recherche de la Suisse pourrait en subir des répercussions.

La Chine poursuivra le développement et la modernisation de son arsenal nucléaire. Officiellement, elle vise à assurer la dissuasion minimale nécessaire, sans pour autant indiquer au reste du monde ce qu'elle entend par là. Le réarmement et les interrogations quant à ses intentions réelles pourraient inciter l'Inde et les États-Unis notamment à étendre leurs propres arsenaux. Cette situation complique également les négociations bilatérales sur le désarmement entre les États-Unis et la Russie.

IRAN



Les attaques israéliennes et américaines contre des installations du programme nucléaire iranien ont, au moins temporairement, mis un coup d'arrêt à la capacité d'enrichissement d'uranium de l'Iran. Elles ont par ailleurs détruit certaines installations clés qui, en cas de décision en ce sens, auraient facilité une orientation militaire du programme nucléaire iranien. Malgré l'assassinat ciblé de plusieurs scientifiques nucléaires de haut rang, l'Iran dispose encore d'un savoir-faire suffisant pour relancer son programme nucléaire. Ce qu'il est advenu de ses quelque 440 kilos d'uranium enrichi à 60 pour cent reste partiellement inexplicé.

Les tentatives d'acquisition iraniennes se poursuivent en Suisse, indépendamment de la reconstitution des capacités qui ont été détruites en 2024 et 2025. Bien que l'Iran ait pu réduire sa dépendance vis-à-vis des États occidentaux eu égard à plusieurs technologies clés, l'acquisition de biens occidentaux demeure attrayante à ses yeux en raison de l'expérience accumulée en la matière ou de leurs propriétés techniques. Dans la mesure du possible, l'Iran s'approvisionnera toutefois ailleurs.

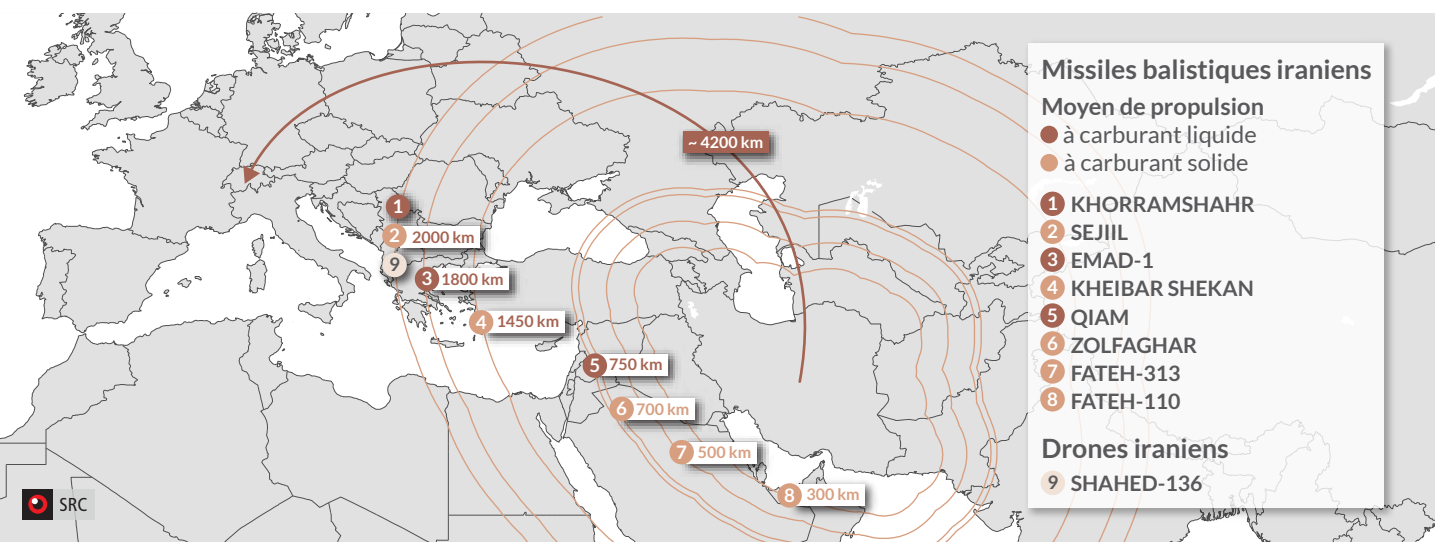


La pression accrue exercée par les sanctions et les confrontations militaires avec Israël et les États-Unis renforceront l'imbrication économique et militaire de l'Iran avec des États non occidentaux. Étant donné la vulnérabilité stratégique persistante de l'Iran, les dégâts de grande ampleur infligés à son programme nucléaire ainsi que les coûts de reconstruction qui en découlent ne font que renforcer l'importance de son programme de missiles en tant que moyen de dissuasion. Ce programme de missiles continue de représenter une menace considérable, en particulier pour Israël. Si l'Iran devait à l'avenir augmenter la portée de ces missiles - un développement réalisable rapidement grâce à l'expérience amassée dans son programme spatial -, il pourrait alors menacer directement l'Europe centrale.

Si l'Iran devait à l'avenir augmenter la portée de ses missiles, il pourrait alors menacer directement l'Europe centrale.

Le pouvoir iranien actuel accorde encore une grande importance au programme nucléaire du pays. Il est donc improbable que l'Iran y renonce entièrement. La menace que cela représente dépend avant tout de la capacité de l'Iran à déterrer ses stocks existants d'uranium hautement enrichi. Une décision en ce sens appartiendrait au nouveau guide suprême.

Portée estimée de certains missiles iraniens



CORÉE DU NORD



La Corée du Nord n'est plus aussi isolée politiquement qu'il y a quelques années. En septembre 2025, le dirigeant du régime nord-coréen Kim Jong-un s'est ainsi rendu à Pékin en même temps que le président russe et de chefs d'État de pays du Sud global. Cette visite a permis à la Corée du Nord d'améliorer ses relations avec la Chine. Celles-ci étaient tendues en raison de la signature d'un traité d'alliance avec la Russie et de l'envoi de troupes pour soutenir cette dernière dans sa guerre contre l'Ukraine. La Chine demeure de loin le principal partenaire commercial de la Corée du Nord.

Malgré tout, la Corée du Nord a encore renforcé sa coopération avec la Russie. Elle continue de lui fournir des missiles balistiques de courte portée et collabore plus étroitement avec elle dans le domaine des drones. Il est probable que la Corée du Nord apporte son soutien à la Russie dans le cadre de la production de drones du type Shahed 136 d'origine iranienne, ce qui lui permet d'acquérir elle-même le savoir-faire et la technologie nécessaires à la fabrication de tels drones. De même, il est probable que la Russie aide la Corée du Nord à former ses pilotes de drones.

La Corée du Nord poursuit son programme nucléaire et continue de produire de l'uranium enrichi et du plutonium. En 2025, elle a mené au moins 14 tests de missiles, un chiffre largement inférieur à celui des années précédentes. Lors de ces tests, plus de 24 missiles ont été lancés. Ces tests portaient à nouveau principalement sur des systèmes à carburant solide de courte portée pouvant servir de vecteurs à l'arme nucléaire, ainsi que sur des missiles de croisière et des missiles sol-air. Contrairement aux années précédentes, la Corée du Nord n'a procédé à aucun test de missile balistique intercontinental.

On constate ponctuellement des tentatives d'acquisition de biens suisses pour lesquels des substituts adéquats ne sont pas disponibles en Chine.



Malgré l'amélioration de leurs relations, la Corée du Nord maintiendra sa liberté d'action vis-à-vis de la Chine. Si nécessaire, elle continuera de soutenir la Russie en lui fournissant des troupes et des munitions. Kim Jong-un sera peu enclin à rencontrer le président américain, du moins tant que celui-ci continuera d'exiger que Pyongyang renonce à l'arme nucléaire.

La Corée du Nord présentera son nouveau plan quinquennal en 2026. Elle réaffirmera son intention de disposer de sa propre capacité de reconnaissance satellitaire. Dans ce but, elle perfectionnera notamment son lanceur de satellites en le différenciant davantage de ses missiles balistiques. Elle poursuivra également ses programmes d'armement stratégiques, en particulier en ce qui concerne les véhicules de rentrée avancés, les sous-marins à propulsion nucléaire et les systèmes de drones. La Corée du Nord va en outre poursuivre l'opérationnalisation des systèmes de vecteurs à carburant solide de toutes les portées.

À l'égard de la Corée du Sud, et bien qu'un président ouvert au dialogue vienne d'y prendre ses fonctions, la Corée du Nord poursuivra une ligne dure. Cette attitude se manifestera également par la poursuite des essais de missiles balistiques. La Corée du Sud réagira aux efforts d'armement de son voisin en augmentant considérablement son budget de la défense. Son objectif déclaré consiste à être en mesure de se défendre de manière autonome contre la Corée du Nord.

Les besoins en biens suisses spécialisés vont se maintenir. Il est extrêmement probable dans ce contexte que de nouvelles tentatives d'acquisition aient lieu.

Il est extrêmement probable que de nouvelles tentatives d'acquisition aient lieu.

👁️ Que voit le SRC?

🔭 Que prévoit le SRC?



ESPIONNAGE



MENACE LIÉE À L'ESPIONNAGE EN GÉNÉRAL



La Suisse reste confrontée à une menace très élevée en lien avec l'espionnage. Celle-ci émane principalement de services de renseignement étatiques. Parallèlement à l'espionnage, divers services de renseignement pratiquent également d'autres activités clandestines en Suisse, comme la désinformation, la propagande, les activités d'influence, l'acquisition de biens et la préparation d'actes de sabotage à l'étranger. Ils s'en prennent également à leurs ressortissants établis en Suisse (répression transnationale).

La Suisse reste confrontée à une menace très élevée en lien avec l'espionnage.

Les services de renseignement s'intéressent avant tout aux intentions et aux capacités d'acteurs étatiques et non étatiques qu'ils considèrent comme des menaces. Certains États emploient aussi leurs services de renseignement pour déterminer les intentions et capacités de concurrents économiques, voire de partenaires dans le cadre d'alliances militaires. Les informations obtenues de cette manière visent à leur procurer un avantage.


L'une des principales raisons du très haut niveau de la menace réside dans la multitude de cibles présentes en Suisse. L'État en fait partie, tout comme les organisations internationales et leur environnement, les représentations diplomatiques et consulaires, les entreprises actives à l'international, les hautes écoles, les universités, les instituts de recherche, les diasporas, les membres de l'opposition et les journalistes. Ce type de cibles existent dans bon nombre d'autres pays, mais la Suisse compte parmi les États d'Europe, et probablement du monde, dans lesquels leur présence est particulièrement dense.

Cette menace s'explique aussi par la situation centrale de la Suisse en Europe et par son ouverture. L'espace Schengen facilite les voyages et la Suisse dispose de bonnes liaisons internationales. Des événements à forte résonance internationale y sont régulièrement organisés. Les entreprises, universités, instituts de recherche et organisations non gouvernementales attirent des experts du monde entier. Tous ces facteurs sont mis à profit par les services de renseignement étrangers: ils tirent parti de la situation pour espionner aussi bien des entités suisses qu'étrangères.

De nombreux services de renseignement étrangers possèdent des antennes clandestines sur sol suisse, souvent dans des représentations diplomatiques ou consulaires. Les différences de taille entre ces antennes sont parfois flagrantes. Une poignée d'États emploient des dizaines d'officiers de renseignement présumés, dont la plupart sous couverture diplomatique, consulaire et administrative-technique. À ceux-ci s'ajoutent les collaborateurs de services de renseignement et les agents qui ne disposent pas d'un domicile fixe en Suisse et qui s'y rendent temporairement pour y pratiquer des activités de renseignement.

À l'étranger également, des personnes et organisations sont touchées par l'espionnage à des degrés divers, en particulier lorsqu'elles séjournent ou s'établissent dans des pays dotés de services de renseignement puissants. Sur leur territoire national, les services de renseignement disposent généralement de possibilités d'exploration beaucoup plus étendues et ne doivent pas toujours agir dans la clandestinité. Les représentations diplomatiques et consulaires de la Suisse comptent parmi les principales cibles des services de renseignement locaux. Mais les personnes et organisations qui sont basées à proximité d'infrastructures dévolues

à la sécurité de l'État ou qui ont affaire à des organes de sécurité ou à leurs membres doivent également s'attendre à se retrouver dans le viseur des services de renseignement locaux.

 Les facteurs qui favorisent l'espionnage demeurent en grande partie les mêmes, mais il est très probable que l'intensification du conflit hybride en Europe et les tensions croissantes entre les grandes puissances et certaines puissances régionales se traduisent par une menace liée à l'espionnage accrue pour la Suisse. Elle restera ainsi une importante zone d'opération pour de nombreux services de renseignement étrangers, qui continueront de manifester un intérêt constant pour une multitude de thématiques et de domaines propres à notre pays ces prochaines années. Parmi ceux-ci figurent en priorité la politique extérieure, la politique commerciale et la politique de sécurité, les capacités actuelles et futures de l'armée, l'industrie de l'armement, la recherche de pointe, ainsi que les organisations, groupes et personnes basés en Suisse qui sont considérés comme des menaces par d'autres États.

La numérisation offrira aux services de renseignement la possibilité de collecter davantage d'informations. Dans le même temps, il est extrêmement probable que les services de renseignement investissent de plus en plus dans l'automatisation de la collecte, du traitement et de la transmission des données. L'utilisation de l'intelligence artificielle et des appareils connectés à Internet, en particulier lorsqu'ils sont dotés de fonctions d'enregistrement audio et vidéo, constituera un défi de taille pour les particuliers, les entreprises, les organisations non gouvernementales et les institutions publiques. Les personnes et organisations qui travaillent avec des données sensibles sont particulièrement concernées. Parmi elles figurent des services de l'État, des fournisseurs de services cloud et d'accès à Internet, des entreprises de télécommunications, des banques, des assurances, des hôtels, des administrations fiscales, des cabinets d'avocats, des firmes comptables et des entreprises de conseil.

COURT MÉTRAGE SUR L'ESPIONNAGE ÉCONOMIQUE EN SUISSE

www.src.admin.ch

> Sécurité > Renseignement > Espionnage économique



MENACE LIÉE À L'ESPIONNAGE PAR LA RUSSIE



Parmi tous les États qui disposent d'antennes clandestines en Suisse, la Russie reste en tête de liste. La majeure partie du personnel de renseignement russe en Suisse est employé par le service de renseignement extérieur SVR. Grâce à leur personnel, ce dernier, ainsi que le service de renseignement militaire GRU, exploitent des réseaux d'agents en Suisse. Ces réseaux ne sont pas uniquement utilisés pour l'espionnage : ils servent par exemple aussi à des fins d'influence politique, de propagande, de désinformation et d'acquisition de biens, tant en Suisse qu'à l'étranger.

Tandis que la plupart des services de renseignement étrangers recherchent avant tout des informations au sujet de personnes et de groupes perçus comme des menaces dans leurs propre pays, les services russes manifestent un intérêt beaucoup plus large. La Russie s'intéresse à une multitude de sujets en lien avec la politique intérieure, la politique étrangère, la politique de sécurité, la politique commerciale et l'armement.

Une proportion significative des activités russes en Suisse sont dirigées contre d'autres entités étrangères sur notre territoire. À Genève, les



services russes tentent d'obtenir des informations par l'intermédiaire du personnel des organisations internationales et des représentations diplomatiques d'autres États. Ainsi, des officiers de renseignement russes sous couverture diplomatique participent à des assemblées et à des discussions à l'ONU dans le but notamment d'identifier de potentielles cibles en vue d'un recrutement.

Les antennes des services de renseignement implantées dans les représentations diplomatiques et consulaires conservent une importance primordiale pour la Russie. Les services de renseignement russes continuent de miser fortement sur l'espionnage au moyen de sources humaines et sur la présence sur place d'officiers traitants dûment formés. Ils reconstituent donc à nouveau leurs structures en Europe, voire les étendent, là où ils ne subissent pas d'entrave. Les postes au sein de représentations diplomatiques et consulaires offrent en effet une multitude d'avantages. Les événements officiels dans ces locaux servent non seulement à entretenir les relations diplomatiques et économiques, mais aussi, dans le contexte du renseignement, à établir des contacts et à recruter dans un cadre protégé. La couverture diplomatique permet en outre aux officiers de renseignement d'accéder facilement à des personnes, organisations et infrastructures dans les domaines de la politique, de l'économie et de la science. Cette couverture offre par ailleurs une protection élevée contre les poursuites pénales dans le pays hôte.

En parallèle, les services continueront de recruter des agents depuis la Russie via des canaux numériques. Cette approche ne remplacera pourtant pas le travail des officiers traitants sur place, même à long terme. Une relation entre un officier traitant et un agent, qui repose notamment sur de véritables rencontres, est en effet plus intensive et plus fiable qu'une relation purement virtuelle lors de laquelle les officiers traitants ne montrent généralement même pas leur visage.

Une proportion significative des activités russes en Suisse sont dirigées contre d'autres entités étrangères sur notre territoire.

Échelle de probabilité



MENACE LIÉE À L'ESPIONNAGE PAR LA CHINE



Outre la Russie, la principale menace liée à l'espionnage émane de la Chine. Elle recourt à des dispositifs de renseignement de grande ampleur, qui ciblent aussi la Suisse et des entités en rapport avec la Suisse. En revanche, les antennes de renseignement implantées dans les représentations diplomatiques et consulaires chinoises en Suisse sont vraisemblablement plus petites que celles de la Russie. La Chine mise davantage sur des membres des services de renseignement voyageant et se présentant sous différentes légendes sans nécessairement recourir à la couverture diplomatique.

Sur le plan thématique, la Chine manifeste un intérêt constant pour les activités et réseaux des groupes qu'elle nomme les « cinq poisons » : les Taïwanais, les Tibétains, les Ouïgours, les adeptes du Falun Gong et les militants de la cause démocratique. Les personnes et organisations en Suisse qui leur apportent un soutien se retrouvent également dans son viseur. Les services chinois suivent également des cibles dans les domaines de la politique étrangère, de la politique commerciale, de la politique de sécurité, de l'économie et de la science. À celles-ci s'ajoutent diverses entités étrangères basées en Suisse, dont les représentations diplomatiques et consulaires d'autres États.

D'une manière générale, la Chine adopte une approche globale en matière de recherche d'informations, au sens qu'elle collecte des données relevant d'un spectre thématique très

D'une manière générale, la Chine adopte une approche globale en matière de recherche d'informations, au sens qu'elle collecte des données relevant d'un spectre thématique très large.

large. Il est très probable qu'elle n'est pas le seul État au monde à agir de la sorte, mais elle se distingue par l'immensité de son terri-

toire ainsi que par les interdépendances qu'elle a construites sur le plan politique, et surtout économique, à l'échelle mondiale. À cet égard, les organisations et ressortissants chinois sont légalement tenus de collaborer avec les autorités, et par conséquent avec les services de renseignement.



La menace émanant de la Chine dépendra fortement du degré d'interdépendance économique qui existera à l'avenir entre la Suisse et la Chine. Contrairement à la situation prévalant à l'égard de la Russie, il est très probable que les échanges commerciaux augmenteront encore au cours des prochaines années, pour autant que les conditions ne changent pas. Or, ces échanges génèrent des données, et il est extrêmement probable que la Chine traite ces données également à des fins de renseignement. Aujourd'hui déjà, les services chinois disposent de moyens techniques et humains leur permettant de traiter de grandes quantités de données et de les rendre exploitables pour leurs propres besoins, mais aussi pour ceux du Parti communiste, de l'armée, du reste de l'appareil étatique et des entreprises d'État. Il est très probable qu'ils continuent de développer ces compétences à grande échelle. Il est par exemple réaliste de supposer que les données générées par les voitures chinoises modernes sont transmises aux services chinois via les constructeurs, ou que les services de renseignement disposent, ou disposeront, d'un accès à ces données via des interfaces. Lors de l'achat de véhicules chinois, les particuliers et organisations en Suisse doivent tenir compte de cet aspect, en particulier s'ils appartiennent aux catégories qui sont principalement ciblées par l'espionnage.



MENACE CONTRE LES INFRASTRUCTURES CRITIQUES



LA MENACE EN GÉNÉRAL

Divers acteurs menacent les infrastructures critiques en Suisse, tant par le biais d'attaques physiques que par des moyens cyber. Les attaques lancées par des cyberacteurs étatiques russes, chinois, iraniens et nord-coréens représentent la cybermenace la plus concrète dans notre pays pour l'existence et le fonctionnement de l'État suisse. La plupart du temps, ces cyber-acteurs sont employés par des autorités de sécurité; ils disposent de moyens techniques sophistiqués, agissent de manière ciblée et font preuve d'une grande ténacité. Toutefois, ce genre de cyberattaques sont aussi perpétrées par des acteurs externes sous mandat étatique, soit des «proxys».

Les États pratiquent le cyberespionnage en fonction de leurs intérêts stratégiques. La guerre contre l'Ukraine, la guerre en Iran ainsi que le conflit commercial et la rivalité technologique entre les États-Unis et la Chine sont autant de facteurs qui motivent ce type d'activités. Les attaquants espionnent des cibles militaires à l'aide de moyens cyber et mettent la main sur des informations politiques confidentielles relevant d'autorités gouvernementales. Ils s'intéressent également aux travaux de recherche et de développement pertinents sur le plan économique ou militaire, particulièrement dans les domaines de l'armement et des technologies de pointe. La Corée du Nord se sert également de ses cyberacteurs pour se procurer des devises étrangères en volant de l'argent sous forme de cryptomonnaies.

Les groupes de rançongiciel chiffrent des données afin de réclamer une rançon. En Suisse, on dénombre une à deux attaques de ce type contre des infrastructures critiques chaque mois. Elles touchent en majorité des entreprises et non des autorités. Les attaques par rançongiciel ont le potentiel de perturber l'exploitation des infra-

structures critiques, voire de l'interrompre pendant une longue période. La publication des données volées par les attaquants constitue un autre risque, car l'entité concernée peut se voir atteinte dans sa réputation ou mise dans une position concurrentielle désavantageuse. Les prestataires de service qui travaillent avec les autorités sont eux aussi ciblés par des attaques par rançongiciel, faisant courir un risque de fuite d'informations politiques confidentielles. En Suisse et dans d'autres États occidentaux, la grande majorité de ce genre d'attaques sont le fait de groupes de hackers russes.

Les groupes hacktivistes - qui cherchent à atteindre leurs objectifs de nature idéologique notamment au moyen du piratage informatique - sont connus pour mener des attaques par surcharge. Des groupes de hacktivistes pro-russes en particulier ont en outre commencé à perturber des systèmes de contrôle industriels raccordés à Internet à l'étranger. Ces systèmes étaient souvent mal protégés et pouvaient donc être attaqués sans compétences particulières. Il faut toutefois s'attendre à ce que les attaquants perfectionnent leurs compétences dans les prochains mois. Bien que les infrastructures critiques concernées n'aient pour la plupart pas subi de perturbations notables, ces attaques ont retenu l'attention. Elles ont par ailleurs montré que les systèmes de contrôle industriels sont parfois uniquement protégés par le mot de passe par défaut, et sont à ce titre vulnérables. En Suisse, de telles attaques contre les systèmes de contrôle industriels sont moins probables que dans les pays de l'UE et de l'OTAN qui apportent un soutien militaire à l'Ukraine et se retrouvent de ce fait prioritairement dans le viseur de groupes hacktivistes pro-russes. En revanche, les attaques par surcharge contre des cibles en Suisse sont très probables, notamment en lien avec des

conférences internationales et des événements de grande ampleur comme le WEF. Ces tentatives n'interrompent l'exploitation d'infrastructures critiques que de manière marginale, mais elles sont parfois très médiatisées. Les groupes pro-russes et pro-palestiniens sont particulièrement actifs. Certains États mandatent ponctuellement de tels groupes de hackers afin de dissimuler leur responsabilité dans des actions.

Les actions de sabotage ont le potentiel d'infliger des dégâts bien plus importants, qu'elles soient physiques ou qu'elles passent par des moyens cyber. Elles sont par exemple menées dans le cadre du conflit hybride de la Russie contre l'Europe; d'une manière générale, elles s'inscrivent surtout dans le cadre de guerres ou de conflits directs. La probabilité que des infrastructures critiques de la Suisse soient touchées par des actes de sabotage étatique ciblés augmenterait donc aussi rapidement en cas de conflit avec un autre État. Bien qu'il n'existe pour l'heure aucune indication portant sur une attaque par sabotage contre les infrastructures critiques en Suisse, un tel scénario pourrait néanmoins se produire: dans le cadre d'un calcul politique visant à toucher des États ou

des alliances qui

Le sabotage est également pratiqué par des acteurs dont les motivations sont de nature idéologique. Les milieux d'extrême gauche violents considèrent la violence comme un moyen éprouvé dans le cadre de la lutte contre le capitalisme. Des entreprises, des infrastructures comme les autoroutes et les équipements techniques des chemins de fer, ou encore des fournisseurs de télécommunications en Suisse et à l'étranger ont déjà été les cibles d'actes de sabotage physique répétés. Il est plutôt probable que d'autres actes de ce type soient commis en Suisse.

Dans le cadre d'un calcul politique visant à toucher des États ou des alliances qui dépendent d'infrastructures critiques en Suisse, ces dernières pourraient être sabotées en usant de moyens physiques ou cyber.

des alliances qui dépendent d'infrastructures critiques en Suisse, ces dernières pourraient être sabotées en usant de moyens physiques ou cyber. L'attrait de

telles cibles augmente à mesure que les États de l'OTAN et de l'UE renforcent la protection de leurs infrastructures critiques sans que la Suisse ne fasse de même. Des actes de cybersabotage contre des cibles à l'étranger sont en revanche susceptibles d'entraîner des domma-

MENACE PERSISTANTE LIÉE AU CYBERESPIONNAGE



Les cyberacteurs étatiques russes, chinois, iraniens et nord-coréens disposent de capacités techniques avancées. L'un de leurs objectifs principaux est de se procurer des informations politiques auprès d'autorités suisses, leur priorité allant tout particulièrement à la politique de sécurité et à la politique étrangère.

Les cyberacteurs étatiques espionnent par ailleurs des hautes écoles et des institutions scientifiques suisses. Les travaux de recherche dans les domaines de l'armement et des technologies de pointe, mais aussi les programmes de recherche et de développement de l'économie privée sont particulièrement exposés. Une partie de ces connaissances peuvent en effet être utilisées à des fins militaires. Les technologies de pointe jouent en outre un rôle clé dans la course internationale à la suprématie économique. Lorsque des États sont soumis à des sanctions et qu'ils ne peuvent donc pas acquérir du savoir-faire par les voies légales, la recherche d'informations au moyen de l'espionnage gagne en importance.

Ce sont avant tout des cyberacteurs étatiques chinois qui compromettent les opérateurs de télécommunications aux États-Unis, en


Ce sont avant tout des cyberacteurs étatiques chinois qui compromettent les opérateurs de télécommunications aux États-Unis, en Europe et en Asie du Sud-Est. Cette menace reste aussi d'actualité pour la Suisse.

Europe et en Asie du Sud-Est. Cette menace reste aussi d'actualité pour la Suisse. Les fournisseurs de télécommunications représentent non seulement une cible pour l'espionnage, mais aussi un vecteur permettant de s'immiscer dans les systèmes informatiques de leurs clients. La chaîne d'approvisionnement, et en particulier

les prestataires informatiques, demeure une porte d'entrée importante pour les cyberattaques.

Les cyberacteurs étatiques exploitent souvent des failles logicielles dans le cadre de l'intrusion initiale. Il s'agit parfois de vulnérabilités *zero-day*: jusqu'au moment de l'attaque, celles-ci ne sont connues que par son auteur, aucune mise à jour de sécurité n'ayant encore été rendue disponible. Les cyberacteurs étatiques s'attaquent toutefois bien plus fréquemment à des appareils équipés de logiciels obsolètes dont les failles sont connues depuis des semaines, voire des années. Les attaques exploitant des vulnérabilités dans des équipements réseau exposés à Internet, comme les routeurs et les pare-feu, sont particulièrement courantes. Les acteurs étatiques se servent aussi de vulnérabilités dans les appareils mobiles à des fins de cyberespionnage.

Le facteur humain joue un rôle important en matière de cyberespionnage. Dans la majorité des cas, les acteurs étatiques ciblent leurs victimes au moyen de courriels personnalisés (*spearphishing*), par exemple en les invitant à une conférence dans leur domaine d'activité. Cette technique d'ingénierie sociale vise à instaurer un climat de confiance afin d'amener la personne cible à télécharger et à installer un programme sans qu'elle ne s'en rende compte ou à divulguer ses identifiants. Des employés de l'administration sont aussi destinataires de courriels de ce type. Il arrive toujours plus fréquemment que des cyberacteurs étatiques prennent contact avec leurs cibles via des applications de messagerie afin d'accéder aux conversations, aux contacts et à d'autres informations enregistrées sur leur téléphone mobile.

 Ces prochaines années, il est probable que les attaques de cyberespionnage contre des cibles suisses deviennent plus fréquentes. Demeurant un instrument important pour obtenir des informations, elles complètent l'espionnage humain, avec lequel elles interagissent parfois (voir le «*Court métrage sur l'espionnage économique en Suisse*», p.61).

L'environnement politico-sécuritaire de la Suisse s'est détérioré de manière durable; en temps de guerre et de conflit, le besoin d'obtenir des informations relatives à l'adversaire augmente. La Suisse coopère avec l'OTAN et l'UE en matière de politique de sécurité; elle acquiert des technologies d'armement occidentales de pointe qui susciteront particulièrement l'intérêt de cyberacteurs étatiques russes et chinois. Ces cyberacteurs s'en prendront également à des politiciens ainsi qu'à l'administration fédérale pour tenter d'accéder à des informations relatives aux États et alliances avec lesquels la Suisse collabore. L'aggravation du conflit commercial entre les États-Unis et la Chine et leur rivalité systémique, de même que les interdépendances économiques entre la Suisse et des partenaires internationaux, y compris la Chine, augmentent le risque d'activités d'espionnage à motivation politique et économique en Suisse. Cette tendance sera encore plus marquée si les États-Unis continuent à durcir les barrières à l'exportation de technologies vers la Chine. L'espionnage restera alors un moyen d'accéder à de telles technologies, y compris en Suisse.

Les cyberacteurs étatiques collaborent avec des entreprises spécialisées et des hautes écoles dans leur pays, ce qui leur permet de développer rapidement leurs capacités d'attaque. Le cyberécosystème chinois implique par exemple l'obligation générale de signaler rapidement à l'État les vulnérabilités identifiées, ce dont

les cyberacteurs étatiques peuvent tirer parti. Dans plusieurs pays, les cyberacteurs étatiques profitent également du progrès technologique. Ils utilisent par exemple l'intelligence artificielle pour conduire leurs attaques de manière encore plus efficace.

Il est probable que le nombre de vulnérabilités identifiées continuera à croître fortement, étant donné que la numérisation progresse et implique que toujours plus d'appareils potentiellement vulnérables sont mis en réseau. Alors qu'il est souvent possible pour les attaquants de détecter et d'exploiter les vulnérabilités assez rapidement, le développement de logiciels sécurisés nécessite beaucoup de travail. De surcroît, les éditeurs n'ont aucune obligation légale de concevoir des logiciels aussi résistants que possible aux attaques.



ÉVALUATION DES PROPRES MESURES DE SÉCURITÉ INFORMATIQUE

Office fédéral de la cybersécurité OFCS
www.ofcs.admin.ch

Normes minimales pour les TIC

Norme minimale pour les TIC afin d'améliorer la résilience informatique des exploitants d'infrastructures, d'entreprises et d'organisations critiques (y compris outil d'évaluation)
<https://www.ofcs.admin.ch>

Informations pour > Informations pour des spécialistes IT > Thèmes actuels > Normes minimales pour les TIC

Signalement de sites de phishing et e-mails de phishing
www.antiphishing.ch

Allianz Digitale Sicherheit Schweiz

Test rapide en ligne de cybersécurité des PME
(disponible en allemand et en anglais)
www.digitalsecurityswitzerland.ch

DES CYBERACTEURS SE SERVENT D'INFRASTRUCTURES SUISSES POUR DES ATTAQUES



Les cyberacteurs étatiques ou sous mandat étatique disposent souvent de ressources considérablement plus importantes que les groupes hacktivistes ou que ceux qui sont motivés par l'appât du gain. Ils peuvent inscrire leurs cyberattaques dans la durée: il peut s'écouler des mois, voire des années, entre la reconnaissance initiale et l'exfiltration de données ou le cybersabotage.

Les cyberacteurs prennent des mesures afin d'éviter que leurs activités ne soient découvertes et que l'on puisse remonter à leur origine. Parfois, ils ne se contentent pas d'effacer leurs traces, mais ils dessinent aussi délibérément de fausses pistes menant à un autre État. Il est dès lors plus difficile de mettre une cyberattaque sur le compte d'un État ou d'une autorité en particulier. À cette fin, les cyberactivités passent par des réseaux d'anonymisation: les acteurs impliqués n'attaquent pas directement un système depuis leur propre infrastructure, mais par l'intermédiaire de multiples appareils. L'attribution de cyberincidents pertinents au regard

L'attribution de cyberincidents pertinents au regard de la politique de sécurité à un acteur donné est d'autant plus difficile que plusieurs cyberacteurs d'un même État peuvent utiliser les mêmes réseaux.

de la politique de sécurité à un acteur donné est d'autant plus difficile que plusieurs cyberacteurs d'un même État peuvent utiliser les mêmes réseaux. Les acteurs étatiques conçoivent parfois ces réseaux eux-mêmes, mais ils peuvent également recourir aux services d'entreprises de cybersécurité.

Les réseaux d'anonymisation comprennent principalement deux composants:

- Des appareils mal protégés et exposés à Internet, comme des routeurs. L'inconvénient pour les cyberacteurs est qu'ils n'exercent que

peu de contrôle sur ces appareils et peuvent par exemple en perdre l'accès lorsque leurs propriétaires mettent à jour le logiciel.


- Des infrastructures informatiques louées, comme des serveurs. Dans ce cas, les attaquants exercent davantage de contrôle. Les serveurs loués peuvent servir de passerelle pour passer d'un serveur à un autre, ou pour établir une liaison avec le système cible, notamment pour y installer un logiciel malveillant.

Les attaquants remplacent en permanence les composants de leurs réseaux d'anonymisation, parfois en l'espace de quelques heures, afin de brouiller davantage encore les pistes.

Pour rester anonymes, les cyberacteurs étatiques ou leurs prestataires louent généralement des serveurs auprès d'un fournisseur d'hébergement dit blindé (bulletproof hosting provider). Les fournisseurs de ce type louent en partie eux-mêmes des serveurs dans d'autres centres de données et font donc office de revendeurs, autrement dit d'intermédiaires, entre les acteurs étatiques et les fournisseurs. De tels revendeurs louent aussi les serveurs de fournisseurs basés dans des États occidentaux, y compris en Suisse, car les attaques provenant de serveurs situés dans la même région que le pays cible se remarquent moins. Les fournisseurs d'hébergement blindé disposent souvent de sociétés écrans dans des juridictions offshore. Ils ne divulguent généralement aucun renseignement sur leurs clients et leurs activités, bien qu'ils y soient tenus dans de nombreux pays occidentaux, dont la Suisse, à partir du moment où ils utilisent les infrastructures de centres de données locaux. Ils offrent par ailleurs souvent une possibilité de paiement anonyme en cryptomonnaie. Pour les cyberacteurs étatiques comme non étatiques, ces revendeurs jouent par conséquent un rôle essentiel en

matière de mise en place de l'infrastructure d'attaque et des réseaux d'anonymisation.

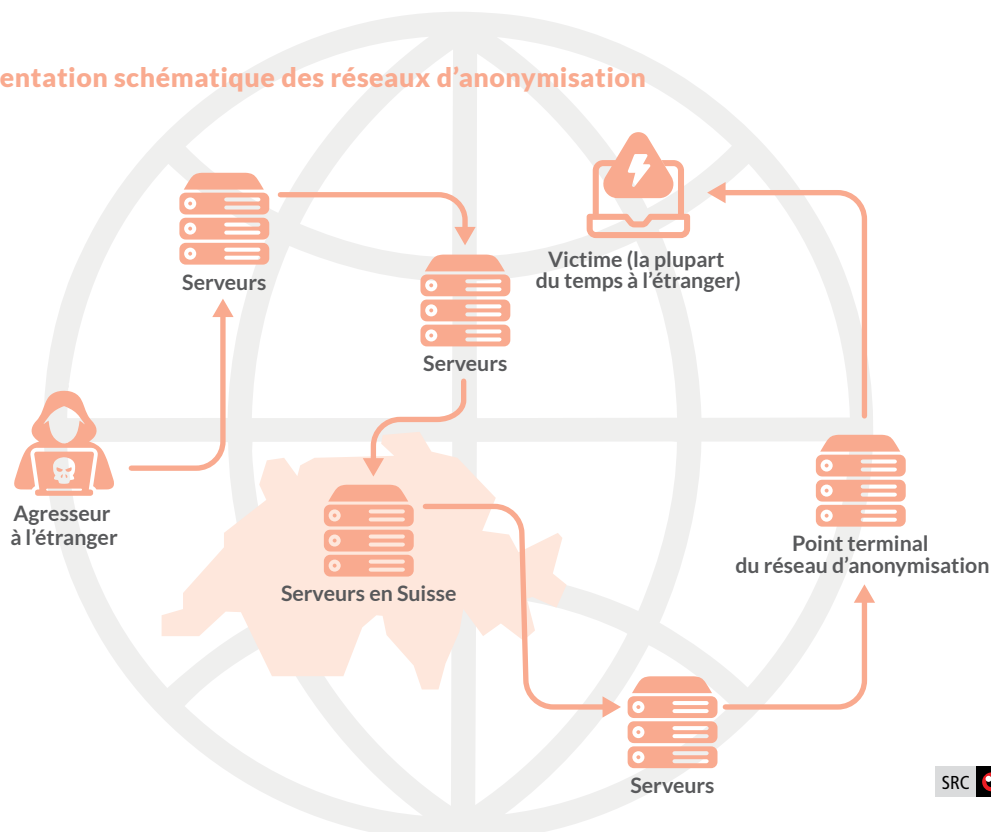
Les réseaux d'anonymisation s'étendent typiquement sur plusieurs continents. Des cyberacteurs étatiques utilisent les services de revendeurs qui sous-louent à leur tour les serveurs d'entreprises suisses. En Suisse, ce sont principalement des cyberacteurs étatiques chinois et russes qui recourent à de telles infrastructures pour espionner des cibles militaires et politiques dans d'autres États. Dans certains cas, des cyberacteurs étatiques ont aussi utilisé ces infrastructures pour mener à bien des attaques de cybersabotage à l'étranger. Pour identifier les auteurs, mais aussi les victimes, il est nécessaire de faire rapidement la lumière sur ces infrastructures d'attaque en étroite collaboration avec des partenaires internationaux.

 Les États-Unis et d'autres États occidentaux, y compris en Europe, ont adopté dernièrement des sanctions contre plusieurs fournisseurs d'hébergement blindé. Malgré cela, ces prestataires restent un maillon essentiel pour les acteurs étatiques en ce qui

concerne la mise en place d'infrastructures d'attaque. Sans compter que la procédure de location pour de tels serveurs ainsi que la création des données d'utilisateur nécessaires à cette fin, comme les adresses de messagerie électronique, est de plus en plus facile grâce à l'automatisation. Il est donc probable que les cyberacteurs étatiques élargissent et renouvellent leurs infrastructures d'attaque plus rapidement. Dès lors, il est aussi très probable que des sanctions supplémentaires soient prises contre les fournisseurs d'hébergement blindé, y compris contre ceux qui sous-louent des serveurs auprès de fournisseurs suisses.

La Suisse a ratifié les onze normes de l'ONU pour un comportement responsable des États dans le cyberspace et elle les met en œuvre. La prévention de l'utilisation abusive d'infrastructures informatiques sur son territoire national entre dans ce cadre. À cette fin, le SRC, l'Office fédéral de la cybersécurité ainsi que les autorités de poursuite pénale de la Confédération et des cantons collaborent étroitement entre eux et avec leurs partenaires internationaux respectifs.

Représentation schématique des réseaux d'anonymisation





CHIFFRES CLÉS 2025



LE RÉSEAU DE RENSEIGNEMENT DU SRC

Comment le SRC centralise les informations pertinentes relatives à la sécurité – et pourquoi cela est déterminant pour la sécurité de grands événements.

Lorsque des dirigeants politiques de haut rang se réunissent au niveau international, l'attention se porte sur les dispositifs de sécurité, la présence policière et les mesures tangibles qui ont été prises. En revanche, ce qui fonctionne depuis longtemps en arrière-plan – le réseau de renseignement du SRC – passe presque inaperçu.

Grâce à ce réseau, un grand nombre d'informations isolées sont rassemblées, coordonnées et évaluées afin de dresser une vue d'ensemble de la situation qui soit utilisable pour la prise de décisions. Ce système n'est pas une invention récente. Bien avant que le SRC ne soit doté de l'actuelle loi sur le renseignement, la Confédération et les cantons travaillaient déjà en étroite collaboration.

Ce qui a déjà fait ses preuves en 2003 dans le contexte du sommet du G8 à Évian est aujourd'hui une pratique courante : lors de grands événements internationaux – comme le Forum économique mondial à Davos ou le Sommet du G7 en France –, le réseau de renseignement garantit que les services concernés de la Confédération et des cantons disposent en temps utile d'informations pertinentes relatives à la situation. Dans le cadre de la coopération internationale, la France en profite également.

La question centrale est de savoir comment obtenir une vue d'ensemble fiable à partir d'informations fragmentées ? C'est précisément là qu'intervient le réseau de renseignement du SRC.

Grâce à son Centre fédéral de situation, le SRC veille à ce que les informations ne restent pas isolées, mais qu'elles soient rapidement rassemblées, structurées et contextualisées. Si le SRC assume un rôle de plaque tournante, il n'est pas le seul producteur d'informations relatives à la situation. Tous les acteurs impliqués fournissent des contributions portant sur leurs domaines de compétence respectifs – de la lutte contre le terrorisme au contre-espionnage en passant par les cybermenaces.

La valeur ajoutée du réseau de renseignement réside dans le traitement et la synthèse de ces informations. La qualité de la vue d'ensemble de la situation qui en résulte et sa diffusion sécurisée via la Présentation électronique de la situation à tous les partenaires du réseau de renseignement sont décisives pour l'efficacité des mesures étatiques et, en fin de compte, pour la sécurité de la Suisse.

Les structures décentralisées de la Suisse rendent cette coordination exigeante. En même temps, le réseau de renseignement profite de la proximité qui existe entre les acteurs et les événements concernés. À cela s'ajoute le réseau international du SRC : il permet d'accéder à des informations auxquelles les différents corps de police et autres partenaires n'auraient pas accès autrement.

Le réseau de renseignement du SRC est donc un élément central et indispensable de la sécurité de la Suisse.

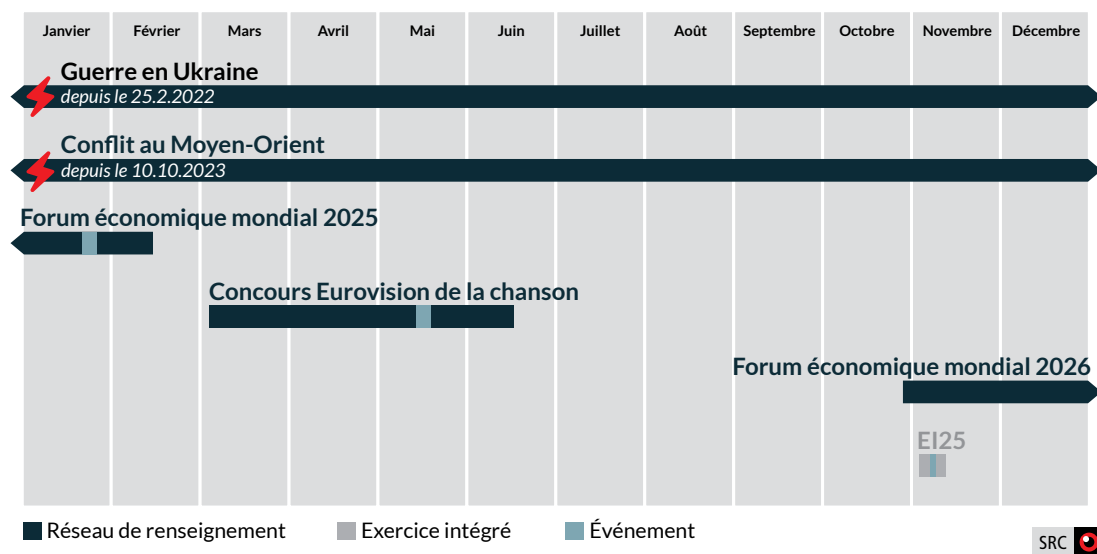
APPRÉCIATION DE LA SITUATION

**La Suisse a besoin du SRC, car ...
... le SRC identifie les menaces importantes qui pèsent sur la Suisse et en rend compte.**

Les rapports d'appréciation de la situation du SRC sont remis au Conseil fédéral, à d'autres décideurs politiques et aux services compétents au sein de la Confédération et des cantons, aux décideurs militaires ainsi qu'aux autorités de poursuite pénale. Ces destinataires, à leur demande ou à l'initiative du SRC, reçoivent périodiquement, spontanément ou dans des délais établis, des informations et des connaissances, sous forme orale ou écrite, concernant tous les domaines couverts par la loi fédérale sur le renseignement (LRens) et en application de la mission de base classifiée du SRC.

Réseau de renseignement

En 2025, le SRC a apporté son soutien aux cantons au moyen de cinq réseaux de renseignement dirigés par son Centre fédéral de situation. Le SRC a également mis en place un réseau de renseignement à l'occasion de l'exercice de crise national « EI 25 ».



RAPPORTS OFFICIELS

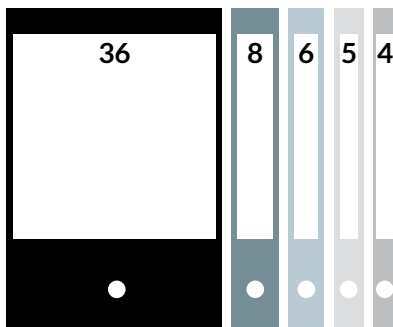
**La Suisse a besoin du SRC, car ...
... le SRC remet aux autorités compétentes des informations non classifiées pour leur utilisation dans des procédures pénales et administratives.**

En 2025, il a ainsi remis 24 rapports officiels au Ministère public de la Confédération et 35 rapports officiels à d'autres autorités fédérales telles que l'Office fédéral de la police, le Secrétariat d'État aux migrations ou le Secrétariat d'État à l'économie (sans les compléments aux rapports officiels déjà existants).

Rapports officiels remis aux autorités fédérales selon les domaines

Total 59

- Terrorisme
- Extrémisme violent
- Espionnage
- Prolifération
- Non consacrés exclusivement à l'un de ces thèmes



COOPÉRATION INTERNATIONALE

**La Suisse a besoin du SRC, car ...
... le SRC travaille avec des autorités étrangères qui accomplissent des tâches au sens de la LRens. À cet effet, le SRC représente entre autres la Suisse dans des organismes internationaux.**

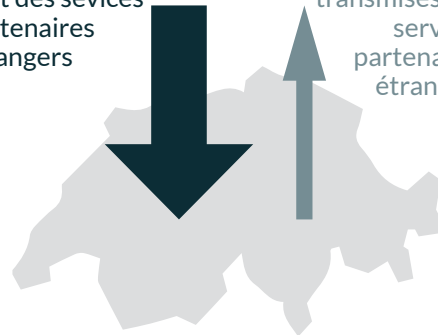
Le SRC échange des informations avec plus d'une centaine de services partenaires de divers États et avec des organisations internationales, par exemple avec les services compétents de l'ONU et les institutions et services de l'UE qui s'occupent de questions de politique de sécurité.

13'308

communications en lien avec les tâches du SRC reçues de la part des services partenaires étrangers

3887

communications en lien avec les tâches du SRC transmises aux services partenaires étrangers



SENSIBILISATION

La Suisse a besoin du SRC, car ...

... le SRC mène, en collaboration avec les cantons, des programmes destinés à la sensibilisation aux activités en matière d'espionnage et de prolifération.

Avec son programme Prophylax, le SRC sensibilise les entreprises, les organisations économiques, les universités, les hautes écoles, les instituts de recherche et les autorités. Dans ce cadre, le SRC présente des mesures de sécurité contre le transfert indésirable de connaissances ou la fuite d'informations ou de données.

En 2025, le SRC a mené 121 sensibilisations: 24 sensibilisations auprès d'entreprises et d'associations économiques, 31 sensibilisations dans les hautes écoles, etc., 66 sensibilisations auprès d'autorités fédérales et cantonales.

PRÉVENTION

La Suisse a besoin du SRC, car ...

... le SRC mène aussi, en collaboration avec les cantons et les autorités fédérales, des entretiens préventifs dans les domaines de l'espionnage et de la prolifération.

Le SRC prend aussi contact avec des entreprises et des hautes écoles pour des entretiens dont l'objectif est la prévention.

En 2025, le SRC a mené 69 entretiens préventifs.

CONTRÔLES À L'EXPORTATION

La Suisse a besoin du SRC, car ...

... le SRC lutte contre la prolifération en contribuant à empêcher que des biens à double usage, du matériel de guerre et des technologies ne soient exportés illégalement depuis la Suisse.

Avec le Département fédéral des affaires étrangères, le Département fédéral de l'environnement, des transports, de l'énergie et de la communication, ainsi qu'avec le Secrétariat d'État à la politique de sécurité et le Secrétariat d'État à l'économie, le SRC constitue le groupe de contrôle des exportations de la Confédération. Le Secrétariat d'État à l'économie consulte le SRC à propos des demandes d'exportation soumises à autorisation pour une évaluation de risque.

En 2025, le SRC a pris position sur 135 dossiers afin de déterminer s'il existait un risque d'infraction à la loi sur le contrôle des biens, la loi sur le matériel de guerre ou la loi sur les embargos. Le SRC signale par ailleurs de sa propre initiative les infractions potentielles aux autorités en charge du contrôle des exportations ou aux autorités de poursuite pénale.

MESURES DE RECHERCHE SOUMISES À AUTORISATION

**La Suisse a besoin du SRC, car ...
... le SRC peut, en cas de menace grave et imminente dans les domaines du terrorisme, de l'espionnage, de la prolifération, des attaques visant des infrastructures critiques ou pour la sauvegarde d'autres intérêts nationaux importants au sens de l'article 3 LRens, ordonner des mesures de recherche soumises à autorisation.**

Les mesures de recherche soumises à autorisation doivent être autorisées par le Tribunal administratif fédéral et avalisées par le chef du Département fédéral de la défense, de la protection de la population et des sports après consultation du chef du Département fédéral

des affaires étrangères et du chef du Département fédéral de justice et police.

Les mesures de recherche soumises à autorisation sont autorisées pour une durée maximale de trois mois. À échéance de ce délai, le SRC peut faire une demande motivée de prolongation pour trois mois supplémentaires au maximum. Les mesures sont soumises au strict contrôle de l'Autorité de surveillance indépendante des activités de renseignement et de la Délégation des Commissions de gestion.

Mesures autorisées et avalisées

Tâches	Mesures
Terrorisme	32
Espionnage	29
Prolifération NBC	36
Attaques visant des infrastructures critiques	112
Total	209

Personnes concernées par ces mesures

Catégorie	Nombre
Personnes ciblées	9
Tiers	6
Personnes inconnues (par ex. uniquement numéro de téléphone connu)	9
Total	24

Méthode de comptage

- Chaque prolongation autorisée et avalisée d'une mesure (possible plusieurs fois pour chaque fois trois mois au maximum) est comptée comme une nouvelle mesure, car toute prolongation doit être à nouveau demandée et motivée dans le cadre de la procédure ordinaire.
- Les personnes concernées ne sont par contre comptées qu'une fois par année, cela également dans le cas où des mesures sont prolongées.

EXPLORATION DU RÉSEAU CÂBLÉ

La LRens prévoit également que le SRC est habilité à procéder à l'exploration du réseau câblé pour la recherche d'informations sur des événements importants en matière de politique de sécurité se produisant à l'étranger (art. 39 ss LRens).

Comme l'exploration du réseau câblé passe par l'étranger pour la collecte d'informations, elle n'est pas considérée comme une mesure de recherche soumise à autorisation en Suisse.

L'exploration du réseau câblé ne peut être réalisée qu'avec la participation d'exploitants des réseaux filaires et d'opérateurs de télécommunications suisses qui ont l'obligation de transmettre les signaux correspondants au Service action cyber- et électromagnétique de l'armée suisse. La LRens prévoit l'obligation d'obtenir une autorisation selon une procédure d'aval analogue à celle prévue pour les mesures soumises à autorisation pour confier un mandat d'exploration à un exploitant ou à un opérateur.

4

mandats d'exploration
du réseau câblé

(en traitement à fin 2025)



EXPLORATION RADIO

L'exploration radio est elle aussi axée sur l'étranger (art. 38 LRens), ce qui signifie qu'elle ne peut porter que sur des systèmes radio qui se trouvent à l'étranger. Dans la pratique, cela concerne avant tout les satellites de télécommunications et les émetteurs à ondes courtes.

12

mandats d'exploration
radio

(en traitement à fin 2025)



EXAMENS EFFECTUÉS DANS LE DOMAINE DE LA MIGRATION ET DEMANDES D'INTERDICTION D'ENTRÉE

La Suisse a besoin du SRC, car ...

... le SRC examine les dossiers et demandes déposés depuis l'étranger sous l'angle d'une éventuelle mise en danger de la sécurité intérieure du pays.

Si le SRC estime que la personne concernée représente un risque potentiel, il peut recommander le rejet de la demande ou faire valoir des réserves auprès des autorités compétentes, c'est-à-dire, selon les demandes, le Département fédéral des affaires étrangères, le Secrétariat d'État aux migrations ou l'Office fédéral de la police.

	Nombre de demandes examinées	Recommandation de rejet
Demandes d'accréditation pour diplomates et fonctionnaires internationaux		30
Demandes de visa	4793	36
Autorisations de séjour ou de travail soumises au droit des étrangers		5
Dossiers de requérants d'asile	373	2
statut de protection S	3	0
Demandes de naturalisation	46'992	1
Fichiers examinés dans le cadre de la procédure de consultation Schengen en matière de visas Vision	1'530'508	7
Examen des informations préalables sur les passagers API (Advance Passenger Information) <small>Les données API qui ne fournissent aucun résultat lorsqu'elles sont comparées avec les données dont dispose le SRC sont effacées par ce dernier après un délai de 96 heures.</small>	4'195'024 personnes sur 24'732 vols	

DEMANDES D'INTERDICTION D'ENTRÉE

Sur les 63 interdictions d'entrée en Suisse que le SRC a demandé à l'Office fédéral de la police de prononcer pour préserver la sécurité de la Suisse, 51 l'ont été. 12 demandes étaient encore en traitement à fin 2025. Aucune demande n'a été rejetée.

CONTRÔLES DE SÉCURITÉ RELATIFS AUX PERSONNES

Les contrôles de sécurité relatifs aux personnes (CSP) constituent une mesure préventive destinée à préserver la sécurité de la Suisse et à protéger sa population. Les CSP concernent des personnes exerçant des fonctions sensibles, nécessitant l'accès à des informations, du matériel ou des installations classifiés.

Pour le compte de la Chancellerie fédérale et du Service spécialisé chargé des contrôles de sécurité relatifs aux personnes du DDPS, le SRC mène de recherches d'information à l'étranger ainsi que des examens approfondis relatifs à des personnes enregistrées dans les systèmes d'information et de stockage des données du SRC.

En 2025, le SRC a mené 1551 recherches d'informations à l'étranger et 171 examens approfondis (relatifs à des personnes enregistrées dans les systèmes d'information et de stockage des données du SRC).

TRANSPARENCE

En 2025, 204 demandes de renseignements ont été déposées sur la base de l'article 63 LRens et de l'article 25 de la loi fédérale sur la protection des données (LPD). Au total, 118 personnes requérantes ont obtenu des renseignements complets portant sur le traitement ou non de données les concernant jusqu'au moment du dépôt de leur demande et, le cas échéant, sur ces données en question.

Dans 39 cas, la réponse a été différée, restreinte ou refusée pour intérêt exigeant le maintien du secret ou intérêt prépondérant de tiers (art. 63 al. 2 LRens et art. 26 al. 2 LPD).

Dans 11 cas, les conditions formelles pour le traitement d'une demande (comme par exemple la remise d'une preuve d'identité) n'ont pas été remplies, et cela malgré un rappel après trois mois visant à obtenir les compléments nécessaires : ces demandes ont par conséquent été classées sans suite. À fin 2025, les conditions formelles pour 4 demandes pouvaient encore être remplies dans le respect du délai de trois mois. De sorte qu'à la fin de 2025, 32 demandes de renseignements étaient encore en traitement.

En 2025, le SRC a reçu 38 demandes d'accès sur la base de la loi fédérale sur le principe de la transparence dans l'administration (LTrans). Il en a traité 26 à titre d'entité compétente et 12 à titre d'entité impliquée.

PERSONNEL ET FINANCES

Le SRC promeut une diversité vécue : des collaboratrices et collaborateurs de générations et de genres différents y travaillent ; ils disposent de formations et d'expériences professionnelles diverses et ont des parcours de vie et des horizons multiples. Leur collaboration est marquée par les valeurs d'ouverture, de courage, de respect, de confiance et de vision à long terme. Le plurilinguisme qui caractérise la Suisse s'y reflète : au SRC, toutes les langues nationales sont pratiquées au quotidien. Cette diversité conjugue différentes perspectives et renforce la coopération interdisciplinaire ainsi que le traitement global et fondé des questions complexes qui se posent dans le domaine du renseignement.

Nombre de collaborateurs

Total 458
(à fin 2025)

192

collaboratrices



266

collaborateurs

Finances

En millions de francs



77,9

charges de personnel

25,9

charges de biens et services
et charges d'exploitation

18

indemnisation des cantons pour
leurs services de renseignement

Répartition linguistique

(à fin 2025)

73,4 %

allemand

24 %

français

2,6 %

italien



TABLE DES ILLUSTRATIONS

- 1 Pétrolier en flammes suite à une frappe iranienne, port de Khor Al-Zubeir, Irak, 11 mars 2026
© Keystone / AP Photo
- 2 Dégâts causés par des drones russes ayant violé l'espace aérien polonais lors d'une attaque contre l'Ukraine, Wryki près de Lublin, 11 septembre 2025.
© AP Photo/Czarek Sokolowski
- 3 Place de la gare à Winterthour après l'attaque au couteau du 28 mai 2026
© Keystone / Claudio Thoma
- 4 Restaurant «Della Casa» au lendemain de la manifestation non autorisée en faveur de Gaza, Berne, 12 octobre 2025
© Keystone / Peter Klaunzer
- 5 Panneau publicitaire anti-israélien où figurent des missiles ainsi qu'une inscription en farsi: «Israël est plus faible qu'une toile d'araignée», Téhéran, 19 août 2024
© Keystone / EPA / Abedin Taherkenareh
- 6 L'étoile de Laufenburg joue un rôle majeur pour l'approvisionnement électrique en Europe, Laufenburg AG, 13 février 2023
© Keystone / Gaetan Bally
- 7 Travaux de réparation après l'attaque contre le réseau électrique revendiquée par le groupe d'extrême gauche allemand Vulkangruppe, Berlin, 5 janvier 2026
© Keystone / EPA / Hannibal Hanschke

Rédaction

Service de renseignement de la Confédération SRC

Clôture de la rédaction

Mai / juin 2026

Contact

Service de renseignement de la Confédération SRC

Papiermühlestrasse 20

CH-3003 Berne

media@ndb.admin.ch

www.src.admin.ch

Diffusion

OFCL, Vente des publications fédérales,

CH-3003 Berne

www.publicationsfederales.admin.ch

Art.-Nr. 503.001.26f

ISSN 1664-4698

Copyright

Service de renseignement de la Confédération SRC, 2026

LA SÉCURITÉ DE LA SUISSE

Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne

www.src.admin.ch / media@ndb.admin.ch

