



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Rapport d'activité 2024

Extrait :
« Chapitre B.5 Le service de renseignement
de l'État (SRE) »

Juillet 2025

B.5 Le Service de renseignement de l'État (SRE)

B.5.1 Introduction

La loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (SRE) définit clairement les missions et délimite les champs d'intervention de celui-ci.

Le SRE exerce ses missions dans une optique d'anticipation et de prévention et vise à contrer toute menace ou risque de menace pour la sécurité nationale, la sécurité et le fonctionnement des institutions, les droits fondamentaux et les libertés publiques, la sécurité des personnes et des biens, le potentiel scientifique et technique ou les intérêts économiques du Luxembourg.

Le champ d'activité concerne toute menace qui peut avoir un rapport avec :

- l'espionnage et l'ingérence ;
- le terrorisme et l'extrémisme à propension violente ;
- la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies afférentes ; et
- la cyber-menace et le crime organisé, dans la mesure où ils se trouvent liés à l'une des menaces précédentes.

B.5.2 Principales menaces en 2024

En 2024, l'éventail des menaces pesant sur la sécurité nationale s'est diversifié. L'instabilité internationale, alimentée par des tensions entre grandes puissances et des conflits géopolitiques comme la guerre en Ukraine et les affrontements au Moyen-Orient, impacte directement sur les risques d'espionnage et d'ingérences étrangères. La multiplication des cyberattaques et des campagnes de désinformation visant les États européens menace de fragiliser leurs institutions démocratiques. En même temps, la persistance et la diversification des mouvances extrémistes, quelles que soient les idéologies, ajoutent au défi de l'anticipation et de la prévention des menaces endogènes.

Lutte contre le terrorisme et l'extrémisme à propension violente

En 2024, la détection précoce d'individus radicalisés par la propagande djihadiste reste une priorité pour le SRE. Depuis quelques années, les services de renseignement occidentaux constatent une évolution significative des modes opératoires des groupements terroristes d'inspiration djihadiste, qui se sont réorientés vers des acteurs solitaires, plus jeunes, aux modes opératoires rudimentaires.

De même, les dynamiques de radicalisation, de recrutement et d'incitation des mouvances extrémistes ont profondément évolué, s'appuyant largement sur les espaces numériques. Détecter des personnes de plus en plus jeunes, radicalisés par le biais d'internet et des réseaux sociaux, susceptibles de basculer dans l'action violente, demeure un enjeu majeur pour le SRE.

Le phénomène d'auto-radicalisation chez des jeunes, parfois mineurs, lié à la consommation de propagande extrémiste sur les réseaux sociaux est une réalité en Europe.

Par ailleurs, les pays occidentaux sont confrontés à une diversification d'idéologies à caractère violent. Ces idéologies peuvent être axées entre autres sur l'opposition à l'autorité et aux institutions étatiques, des théories conspirationnistes ou encore la xénophobie. Souvent, les auteurs d'actes violents adhèrent à plusieurs idéologies simultanément ou basculent de l'une à l'autre. La décentralisation des structures terroristes a davantage compliqué la détection précoce de personnes susceptibles à commettre des actes violents.

En 2024, le SRE a intensifié ses efforts de prévention dans les domaines du terrorisme et des extrémismes à propension violente. A cette fin, le service a collaboré étroitement avec ses partenaires nationaux et internationaux. Les renseignements recueillis par le Service de renseignement dans la cadre de sa mission visant à contrer la menace terroriste ont conduit à des dénonciations au Parquet du Tribunal d'Arrondissement de Luxembourg.

Anticipation et prévention des activités d'espionnage ou d'ingérence

En 2024, la menace liée à des activités d'espionnage et d'ingérence reste à un niveau élevé. Des opérations d'influence et des campagnes de désinformation à grande échelle, sont devenus des phénomènes de plus en plus fréquents.

La recrudescence des menaces hybrides, pouvant regrouper l'espionnage, la menace *cyber*, le sabotage, la désinformation et l'ingérence politique, ajoute au déficit sécuritaire en Europe. Ces menaces, émanant d'États hostiles, visent à déstabiliser les démocraties des États européens et à affaiblir leurs institutions. Les infrastructures critiques, comme l'énergie, le transport et les télécommunications, restent des cibles privilégiées.

Depuis l'invasion de l'Ukraine, la Russie recourt de manière croissante à des campagnes d'influence et de désinformation en Europe visant à affaiblir ses institutions démocratiques et de provoquer la discorde entre les États membres de l'UE. Un autre moyen reste l'ingérence dans les processus électoraux par le soutien à des partis extrémistes et des mouvements populistes dans le but d'amplifier des tensions sociales et politiques existantes. Le cyber-espionnage et les cyberattaques visent à perturber les infrastructures critiques ou à récupérer des informations sensibles relatives à leurs systèmes de sécurisation.

Le recours croissant à des « proxies », des acteurs intermédiaires motivés par des intérêts financiers rend l'attribution d'actes hostiles plus complexe.

L'utilisation de *proxies* dans le cadre des menaces hybrides constitue un défi majeur pour les services de renseignement. Un *proxy* est un acteur intermédiaire, tel qu'une organisation criminelle ou un *hacker* mercenaire, engagé par un État ou une entité pour exercer une influence ou mener

des actions hostiles, tout en dissimulant leur implication directe. Contrairement aux militants idéologiquement motivés, ces acteurs agissent principalement par intérêt financier, ce qui rend l'identification des responsables et l'attribution des attaques plus complexes.

Pour contrer ces menaces multidimensionnelles et en constante mutation, la coopération au niveau international est plus que jamais essentielle. Au niveau national, le SRE a poursuivi son étroite coopération avec ses partenaires et a fourni plusieurs briefings de sensibilisation en la matière.

Protection du patrimoine économique et scientifique

Sa présence d'entreprises innovantes dans les domaines des technologies et de la recherche, fait du Grand-Duché une cible attrayante pour des activités d'espionnage. Dans le cadre de sa mission de protection du patrimoine économique et scientifique, le SRE porte une attention particulière à l'anticipation et la prévention de menaces pesant sur des secteurs d'importance stratégique pour l'économie nationale. De manière générale, les secteurs des industries et de la recherche de pointe sont susceptibles d'intéresser des États ou groupes étrangers. Dans cette optique, le SRE procède à la sensibilisation de divers acteurs nationaux, en mettant l'accent sur la prévention des risques.

Lutte contre la prolifération

La communauté internationale travaille activement pour contrer le trafic de biens à double usage à destination de pays visés par des sanctions européennes ou onusiennes. En tant que pôle logistique européen, le Luxembourg est directement touché par ce phénomène et coopère de manière étroite avec des partenaires internationaux.

En application de la loi du 27 juin 2018 relative au contrôle des exportations, le SRE transmet régulièrement des analyses de risque portant sur des exportations de biens à double usage ainsi que de biens liés à la défense au Ministère de l'Economie et à l'Administration des douanes et accises.

En 2024, une partie substantielle des demandes adressées au SRE dans le cadre de la contre-prolifération concernait le suivi des sanctions de l'UE adoptées à l'encontre de la Russie

En 2024, l'Office du Contrôle à l'Exportation, Importations et Transits a adressé 28 demandes d'informations au SRE. Dans le cadre de l'évaluation des risques de ces demandes, le SRE sollicite de manière régulière l'appui des services partenaires.

Dans le cadre de l'article 9 de la loi modifiée du 5 juillet 2016, le SRE communique des renseignements à l'Administration des douanes et accises dans la mesure où ceux-ci puissent être utiles à l'accomplissement de ses missions. En 2024, le SRE a ainsi procédé à 59 analyses de risque.

B.5.3 Coopération nationale et internationale

En 2024, le SRE a renforcé sa coopération, tant au niveau national qu'international, avec les administrations de l'État, divers acteurs stratégiques et les services de renseignement étrangers.

Dans le cadre de sa mission, le SRE a fourni des évaluations de risque et des briefings de sensibilisation sur des sujets tels que le terrorisme, la *cyber*-menace, l'espionnage et la prolifération. Dans le cadre du contre-espionnage et de la lutte contre l'ingérence, il a poursuivi sa collaboration avec les institutions européennes et internationales basées au Luxembourg.

B.5.4 Autorité nationale de sécurité

Enquêtes de sécurité effectuées en 2024 :

Nouveaux dossiers d'enquête depuis le 1 ^{er} janvier 2024	1.179 (LUX)
<i>dont :</i>	
- Demandes initiales (707) et renouvellements (436)	1.143
- Demandes de changement du niveau d'habilitation	36
Nouveaux dossiers d'enquête « ressortissants étrangers »	352
Nombre de décisions de refus	5
Dossiers caducs (pas de statut / annulé dans le système)	15

Dans le cadre de sa mission de protection des informations classifiées au sein des entités civiles et militaires, l'Autorité nationale de sécurité (ANS) a formulé des recommandations et mené des inspections de lieux et de systèmes informatiques. Ces contrôles, portant sur les espaces où les données sensibles sont reçues, élaborées, traitées ou stockées, visaient à garantir leur conformité en vue d'une homologation nationale.