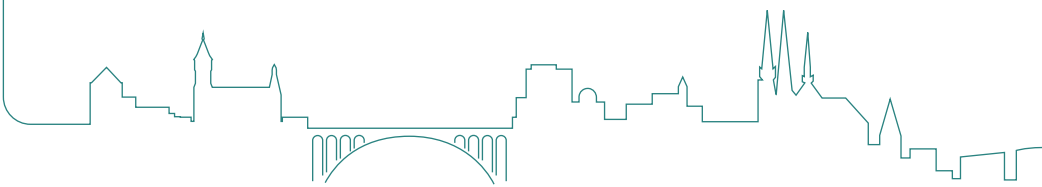
FICHE D'INFORMATION 03

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

Service de renseignement de l'État

L'ESPIONNAGE

CONNAÎTRE LES MÉTHODES ET LES RISQUES POUR MIEUX PRÉVENIR



EDITEUR : SERVICE DE RENSEIGNEMENT DE L'ÉTAT (SRE)

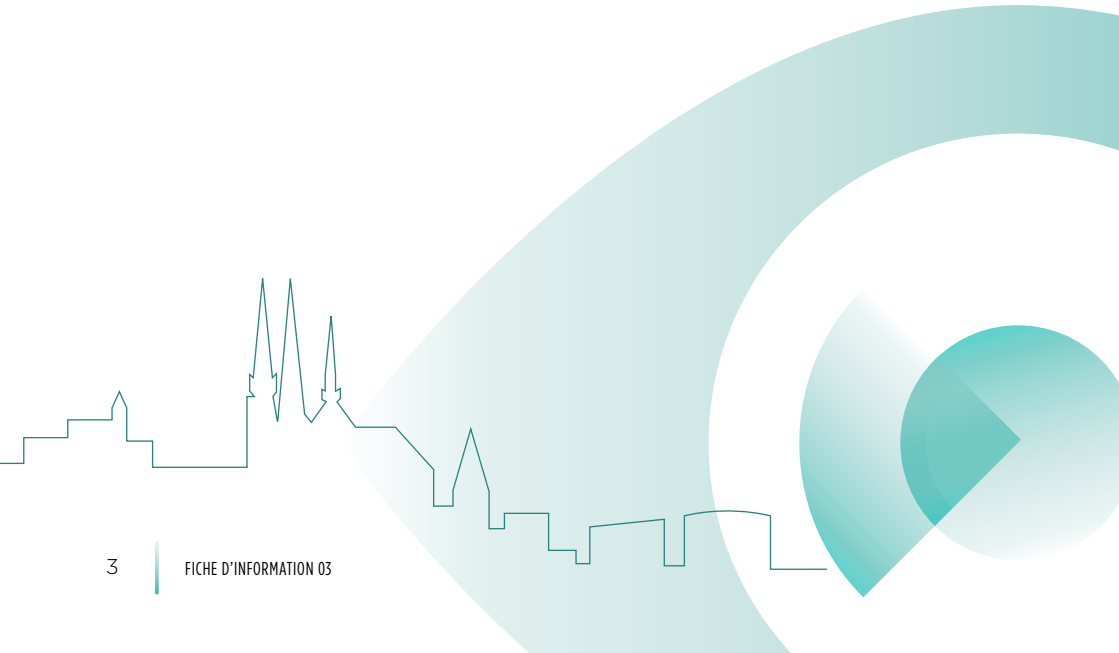
WEB : SRE.GOUVERNEMENT.LU

JUIN 2026

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

Service de renseignement de l'État

SOMMAIRE



L'espionnage constitue une menace sérieuse pour la sécurité nationale : il expose des informations sensibles à des acteurs étrangers hostiles et compromet les intérêts stratégiques, économiques et technologiques d'un État. Il peut également s'inscrire dans des stratégies hybrides plus larges ou dans des campagnes de déstabilisation combinant le recueil discret d'informations sensibles, des opérations cyber, des actions d'influence informationnelle et des actes de sabotage.

Par la présente publication, le Service de renseignement de l'État (SRE) entend, dans une perspective d'anticipation et de prévention, fournir au public des éléments d'information sur le phénomène de l'espionnage, ses modes opératoires, ses cibles potentielles ainsi que les risques qui y sont associés Cette démarche s'inscrit dans le cadre des missions confiées au SRE en matière de lutte contre l'espionnage, de protection du potentiel scientifique et technique ainsi que des intérêts économiques du Luxembourg. En complément, le SRE mène des actions de sensibilisation auprès d'acteurs nationaux susceptibles d'être exposés à des activités malveillantes.

QU'ENTEND-ON PAR ESPIONNAGE ?

L'« espionnage » désigne des activités visant à recueillir, par des moyens clandestins ou dissimulés, des informations sensibles ou stratégiques relatives à un État, à une organisation ou à une entreprise. Ces activités sont généralement menées au profit d'un acteur étatique étranger poursuivant des objectifs politiques, économiques ou technologiques. Les informations recherchées peuvent concerner des domaines variés, notamment la défense, l'économie, les relations internationales, la recherche scientifique ou encore les technologies de pointe.

Au Grand-Duché, la concentration d'entreprises innovantes et d'un environnement de recherche de pointe constitue un facteur d'attractivité susceptible de susciter l'intérêt d'acteurs engagés dans des activités d'espionnage économique ou scientifique. Ce risque est renforcé par l'implantation de plusieurs institutions européennes et d'infrastructures de l'OTAN sur le territoire.

QUELS SONT LES ACTEURS DE L'ESPIONNAGE ET QUELLES SONT LEURS MOTIVATIONS ?

Dans un contexte international marqué par des tensions géopolitiques et une concurrence stratégique croissante, l'espionnage demeure un moyen discret mais puissant utilisé par certains États pour faire prévaloir leurs propres intérêts stratégiques, politiques, militaires ou économiques, au détriment d'autres nations.
Les motivations susceptibles d'inciter un État à recourir à des activités d'espionnage sont multiples, parmi lesquelles :

- contourner d'éventuelles sanctions prises à son encontre ;
- s'approprier du savoir-faire technologique ou industriel afin de servir ses propres intérêts économiques ;

- obtenir des informations non publiques sur les intentions commerciales ou diplomatiques d'un autre État ou organisme dans le but de mieux anticiper leurs décisions ;
- connaître les capacités militaires d'un autre État ;
- collecter des données relatives à des infrastructures critiques ;
- surveiller ou instrumentaliser des communautés émigrées (diaspora) dans une optique d'influence extérieure ;
- etc.

Ces activités d'espionnage sont généralement menées par des services de renseignement étrangers, opérant pour le compte d'un État. Elles peuvent toutefois impliquer des acteurs intermédiaires (proxies), tels que des organisations criminelles ou des mercenaires, agissant pour des motifs financiers ou en soutien aux objectifs de l'État commanditaire.

L'ESPIONNAGE : QUELLES CIBLES ET QUELS RISQUES ?

Toute entité détenant ou traitant des informations sensibles à forte valeur stratégique peut potentiellement devenir la cible d'activités d'espionnage. Cela concerne notamment les entreprises, les instituts de recherche, les institutions publiques, les infrastructures critiques ou encore les structures militaires.

Les secteurs innovants dotés d'un savoir-faire stratégique ou développant des technologies avancées – en particulier lorsqu'elles sont soumises à des contrôles à l'exportation ou présentent un potentiel à double usage – sont particulièrement visés.

L'espionnage ne se limite pas aux informations classifiées. Certaines données sensibles, bien qu'elles ne soient pas formellement classifiées, peuvent présenter une valeur stratégique élevée. Leur exploitation permettrait à un acteur hostile d'anticiper des décisions ou d'influencer des rapports de force. Par exemple, le vol d'un organigramme d'entreprise peut servir à identifier les responsables impliqués dans des projets sensibles et, par la suite, à cibler leurs communications afin d'obtenir des informations confidentielles.

L'espionnage constitue une menace multiforme pour la sécurité nationale des États visés. Il peut compromettre les capacités militaires d'un pays en exposant des éléments relatifs à sa stratégie de défense. Il peut également viser des infrastructures critiques — telles que les réseaux énergétiques, les systèmes de communication ou les réseaux de transport — susceptibles d'être infiltrées ou perturbées. Sur le plan économique, le vol de données industrielles ou technologiques peut nuire à la compétitivité des entreprises nationales. Enfin, certaines institutions démocratiques peuvent être ciblées dans le but d'obtenir des informations sur les intentions économiques,

politiques ou diplomatiques d'un État, permettant ainsi à des acteurs étrangers d'anticiper certaines décisions ou de renforcer leur position dans des négociations internationales.

SOUS QUELLES FORMES L'ESPIONNAGE PEUT-IL SE MANIFESTER ?

L'espionnage peut se manifester sous des formes diverses. Il englobe à la fois des méthodes traditionnelles, reposant sur des interactions humaines directes, et des techniques numériques, recourant à des outils de cyber-espionnage pour collecter des données sensibles. À cet égard, les modes opératoires dits « hybrides » synchronisent ou séquencent fréquemment plusieurs actions coordonnées : l'espionnage humain, des opérations cyber, des activités d'influence informationnelle et, dans certains cas, des actes de sabotage physique.

De manière générale, les modes opératoires employés par les acteurs de l'espionnage varient en fonction de la nature des cibles, du degré de sensibilité des informations recherchées et de la finalité stratégique de l'opération.

Exemples non exhaustifs de modes opératoires pouvant être utilisés dans le cadre de pratiques d'espionnage :

- **Les méthodes d'espionnage traditionnelles**

  Les méthodes traditionnelles et physiques d'espionnage reposent principalement sur des techniques d'infiltration humaine. Elles comprennent notamment le recrutement d'agents sur le terrain, le recours à des sources internes (informateurs), l'interception de communications ou de courriers, ainsi que la surveillance physique de personnes ou de lieux stratégiques. Les agents opèrent souvent sous couverture – diplomatique, commerciale ou académique – afin d'établir des relations de confiance avec leurs cibles et de les amener à divulguer des renseignements.

Ces opérations reposent également sur l'exploitation d'événements professionnels, tels que des conférences, salons professionnels ou séminaires, qui offrent des occasions de nouer des contacts avec des cibles intéressantes. Par ailleurs, les acteurs hostiles recourent aux médias sociaux pour collecter des informations sur leurs cibles, identifier des vulnérabilités potentielles et préparer des approches de manipulation ou d'ingénierie sociale.

Consultez également la publication « Voyager en sécurité »
Les voyages d'affaires à l'étranger constituent des situations de vulnérabilité supplémentaires, susceptibles d'être exploitées par des acteurs étatiques étrangers à des fins de collecte d'informations sensibles. Prendre des précautions adéquates avant, pendant et après le déplacement permet de réduire considérablement les risques encourus. Pour des conseils pratiques sur la manière de vous protéger contre l'espionnage lors de déplacements professionnels en dehors du Luxembourg, consultez notre publication « Voyager en sécurité ».

Le cyber-espionnage

Avec la numérisation croissante des activités et des données, le cyber-espionnage s'est imposé comme l'un des modes opératoires les plus répandus. Il consiste à infiltrer les systèmes informatiques d'organisations ciblées pour en extraire des informations sensibles, telles que des données économiques, scientifiques, diplomatiques ou militaires.

Les techniques employées incluent notamment l'utilisation de logiciels malveillants, le phishing, les attaques par ransomware ou encore l'exploitation de vulnérabilités de sécurité. Les infrastructures critiques – en particulier celles liées à l'énergie, au transport et aux télécommunications – ainsi que les administrations publiques, le secteur financier et l'industrie manufacturière figurent parmi les secteurs les plus ciblés à l'échelle européenne. Les attaques peuvent viser à perturber leur fonctionnement ou à accéder à des informations relatives à leurs systèmes de sécurisation.

Ces méthodes d'espionnage numérique permettent d'obtenir rapidement d'importants volumes d'informations, tout en rendant la détection et l'attribution particulièrement difficiles.

Les menaces hybrides

L'espionnage joue un rôle important dans les stratégies hybrides modernes, auxquelles l'Europe est de plus en plus exposée. Il permet à des acteurs malveillants de recueillir discrètement des informations sensibles concernant un pays, ses infrastructures critiques, ses institutions ou ses entreprises. Ces données sont ensuite exploitées pour mener d'autres actions coordonnées, telles que des attaques cyber, des activités de manipulation de l'information et d'ingérence ou des actes de sabotage. Considérées isolément, les intentions derrière ces actions hybrides peuvent être difficiles à discerner. Analysées dans leur ensemble, elles s'inscrivent toutefois dans une stratégie plus large visant à déstabiliser les démocraties européennes, à affaiblir la confiance du public dans les institutions, ou encore à semer la discorde entre des États partenaires. L'attribution de ces actions hybrides s'avère souvent complexe, notamment en raison de l'utilisation de méthodes sophistiquées visant à masquer l'origine des opérations.

COMMENT SIGNALER UNE SUSPICION D'ESPIONNAGE ?

Vous pensez que vous ou votre organisation avez été la cible d'activités d'espionnage ?
Vous détenez des informations pouvant avoir trait à des activités d'espionnage étranger ou vous avez besoin de conseils sur la manière de réagir face à une potentielle approche par un service de renseignement étranger ?

Dans ce cas, vous pouvez remplir notre formulaire de contact en ligne ou nous écrire à l'adresse info@me.etat.lu.

Veuillez indiquer dans votre message :

- vos nom(s) et prénom(s) ;
- votre employeur ou l'organisation que vous représentez ;
- votre message (veuillez préciser la situation que vous voulez signaler ou les renseignements que vous souhaitez obtenir) ;
- un numéro de téléphone pour permettre au SRE de vous contacter, si vous le souhaitez.

Toute information fournie est traitée de manière discrète et strictement confidentielle.

Pensez également à signaler toute rencontre ou tout événement suspect au service de sécurité de votre entreprise ou organisation.