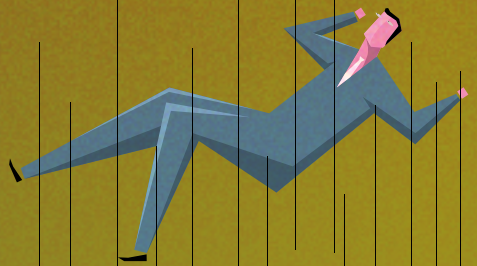
VSSE
veiligheid van de staat
sûreté de l'état



ÊTES-VOUS CONCERNÉS ?

Espionnage et ingérence
Services publics - Diplomatie

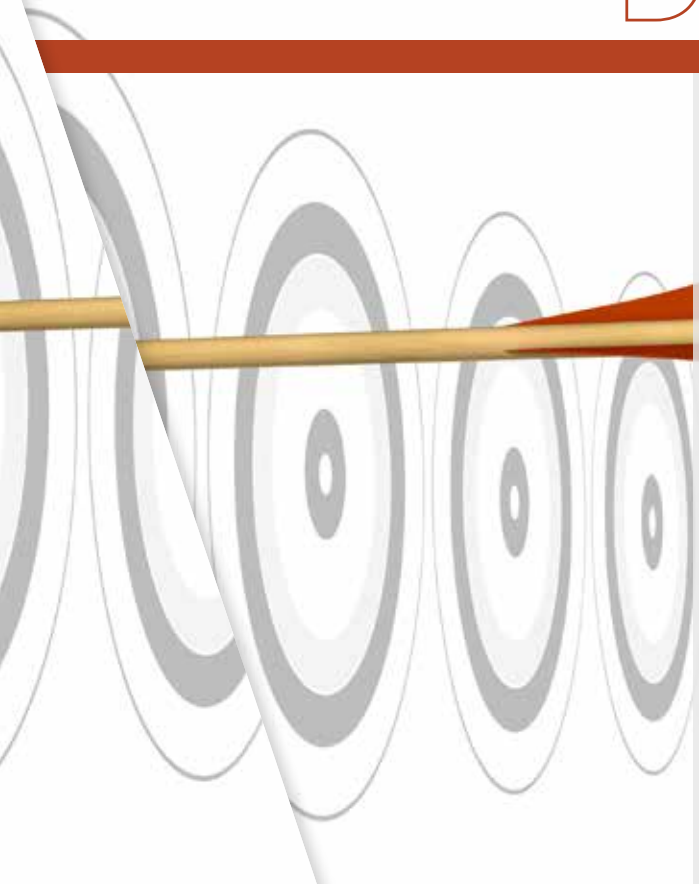
.be

L'espionnage et l'ingérence sont des menaces sérieuses. Des puissances étrangères déploient des ressources toujours plus importantes et plus variées pour obtenir des informations qui ne sont pas accessibles au public, en recourant entre autres à l'espionnage. Elles tentent également d'influencer les processus de prise de décision via l'ingérence.

Les collaborateurs et représentants d'un service public sont des cibles potentielles de ces activités. Vous êtes donc un maillon essentiel de la sécurité de nos institutions et de nos processus démocratiques.

Comment se protéger contre l'espionnage et l'ingérence? La première étape consiste à comprendre et à identifier ces menaces. Avec cette brochure, la Sûreté de l'État souhaite vous aider dans cette démarche, et renforcer votre résilience et celle de votre organisation.

DE QUOI S'AGIT-IL ?



L'espionnage et l'ingérence sont des menaces par nature peu visibles. Elles s'appuient sur des méthodes de récolte d'informations et d'influence trompeuses ou clandestines comme la manipulation de personnes ou l'interception de communications.

L'avantage illicite ainsi obtenu peut ensuite être exploité dans des négociations diplomatiques ou commerciales. Il peut ainsi servir à soutenir les entreprises nationales de ces pays, ou au contraire à déstabiliser un adversaire ou un concurrent géostratégique.

Certains états utilisent également l'espionnage et l'ingérence comme outil de contrôle et d'emprise sur leurs communautés (diasporas) dans notre pays.

De telles méthodes sont le plus souvent utilisées par des services de renseignement étrangers, leurs agents ou leurs alliés. Cela ne concerne pas uniquement la Russie ou la Chine : de nombreuses puissances étrangères, sont concernées.

COMMENT

CELA FONCTIONNE-T-IL ?

Les services de renseignement étrangers travaillent en toute discrétion en utilisant des couvertures. Les espions se présentent comme diplomate, journaliste, fonctionnaire, lobbyiste, chercheur, enseignant ou toute autre fonction qui leur offre la légitimité et la crédibilité nécessaire pour entrer en relation avec vous. Les professionnels du renseignement étranger, déployés en Belgique sous couverture se comptent par centaines, sans compter leur réseau de contacts et d'agents.

Ils exploitent principalement nos vulnérabilités personnelles et les imperfections des appareils électroniques que nous utilisons quotidiennement.

Les manipulations humaines peuvent prendre des formes extrêmement variées. Il pourrait s'agir par exemple d'une relation professionnelle ou amicale qui aurait un agenda caché derrière une façade de courtoisie, de références idéologiques ou culturelles communes, et de flatteries. Ce type de relation est généralement asymétrique : votre interlocuteur sera le plus souvent à l'initiative des contacts et se montrera toujours généreux et serviable. Ces manœuvres d'apparence agréable et inoffensive servent à installer un climat de confiance, ce qui instaure une relation amicale étroite propice aux confidences et à l'entraide. Cette construction fallacieuse est le terreau de la manipulation.

Quelques exemples

1 : Une personne rencontrée lors d'un événement collectif vous invite dans un restaurant. Vous sympathisez et le rencontrez à plusieurs reprises. L'amitié naissante vous fait baisser votre garde et vous lui partagez vos impressions et tous les ragots sur les membres du comité de direction.
En dehors des manipulations humaines, les manipulations techniques se multiplient également, facilitées par notre dépendance de plus en plus grande aux technologies numériques et aux appareils mobiles.

2 : Après avoir cliqué sur un lien qui vous semblait légitime, vous suivez les instructions et introduisez le login - mot de passe de votre compte utilisateur professionnel. Ces données sont ensuite utilisées pour pénétrer dans le serveur de fichier de votre organisation.

TOUTES LES INFORMATIONS SONT PRÉCIEUSES

L'espionnage ne se limite pas au vol de documents confidentiels ou secrets. Le mécanisme est similaire à un puzzle : chaque pièce est un élément supplémentaire qui peut être utilisé contre vos intérêts. Des informations sur le fonctionnement interne de votre organisation, sa structure, les problèmes et intérêts personnels ainsi que les relations interpersonnelles, voire de simples coordonnées de contact peuvent déjà intéresser les espions étrangers. Ces informations peuvent par exemple servir à identifier des personnes ou des accès plus vulnérables ou à nuire à votre organisation.

TOUS LES NIVEAUX DE POUVOIR SONT CONCERNÉS

Les services de renseignement étrangers s'intéressent à toutes les instances qui produisent, assemblent ou coordonnent des informations pertinentes dans des domaines extrêmement variés, en fonction de leurs intérêts stratégiques.

Cela concerne évidemment la diplomatie et la politique économique mais aussi de nombreux autres domaines tels que la recherche, l'innovation, l'investissement, les médias, l'immigration, la gestion des cultes, etc. Les bases de données centralisées (registre national, DIV, INAMI, BCSS, etc.) et les personnes qui y ont accès sont également des cibles potentielles.

COMMENT
SE PROTÉGER ?

Pour vous prémunir, il est indispensable de **prendre conscience de vos vulnérabilités** et de vous protéger autant que possible, tant individuellement que collectivement.

CONSCIENTISER VOS COLLABORATEURS ET VOS COLLÈGUES EST UNE PREMIÈRE DÉMARCHE ESSENTIELLE.
Il importe de comprendre que les risques sont réels, même si les conséquences ne sont pas toujours visibles. N'hésitez pas à faire circuler cette brochure au sein de votre organisation et à contacter la Sûreté de l'État pour obtenir des informations complémentaires.

Il convient ensuite de prendre des mesures de sécurité (préventives). En d'autres termes, il faut réduire les risques par la mise en œuvre d'une politique de sécurité aussi globale et volontariste que possible. Les mesures viseront à limiter l'exposition aux menaces mais aussi à limiter leur impact potentiel. Soyez résilient !

POINTS D'ATTENTION

La frustration mène à la manipulation

Les services de renseignement offensifs sont spécialisés dans la manipulation des personnes. Ils tirent profit des faiblesses et frustrations des individus. Le manque de reconnaissance, des rancœurs accumulées ou des dysfonctionnements non résolus constituent le terreau idéal sur lequel pourra s'appuyer le travail de manipulation. Une saine et bienveillante gestion des ressources humaines est un élément de prévention essentiel.

Besoin d'en connaître / Need-to-know

Assurez-vous que seuls les membres du personnel qui en ont besoin dans leur travail quotidien aient accès aux données les plus sensibles. En appliquant le principe du « need-to-know », vous limiterez le risque d'exploitation abusive de ces informations. De même, une procédure de destruction adéquate des documents contenant des informations sensibles garantit une meilleure protection de la confidentialité.

Soyez discret

Ne consultez et ne discutez pas d'informations sensibles dans des lieux publics. Quelqu'un peut en profiter pour en prendre connaissance à votre insu. L'exploitation malveillante ou simplement non appropriée des informations ainsi obtenues peut porter préjudice à votre organisation.

Toujours joignable = toujours traçable

Les smartphones facilitent la vie, y compris pour les services de renseignement. Des logiciels malveillants de haute technologie peuvent intercepter vos données ou attaquer votre appareil. Maintenez à jour votre système d'exploitation et vos applications et utilisez des modes d'authentification robustes. Lorsque vous stockez ou accédez à des données sensibles depuis votre smartphone, utilisez des logiciels de chiffrement et un VPN. L'utilisation d'un appareil exclusivement réservé aux voyages à l'étranger est fortement recommandée.

Voyages à l'étranger

En dehors de nos frontières, nous sommes plus vulnérables et les capacités des services offensifs augmentent. Les voyages constituent d'excellentes opportunités pour l'espionnage. Il est donc indispensable de prendre des précautions supplémentaires. Les mots d'ordre sont : prudence et discrétion. Réduisez l'exposition en limitant vos documents au strict minimum et sécurisez vos supports. Vous trouverez des recommandations supplémentaires dans notre brochure « Travel Security ». (www.vsse.be)

Médias sociaux

Les services offensifs exploitent aussi les nouvelles opportunités des médias sociaux. Ces plateformes facilitent grandement le profilage des cibles potentielles et multiplient les moyens d'entrer en relation. Assurez-vous que vous connaissez la personne qui souhaite devenir votre « ami » ou contact virtuel. Pensez également qu'accepter un nouveau contact lui permet d'accéder à votre cercle de relations virtuelles tout en procurant un gain de légitimité non négligeable qui pourrait faciliter des tentatives de manipulations ultérieures.

Contrôle, vérification et habilitation

Sans naïveté ni paranoïa, assurez-vous de disposer d'une politique complète de contrôle et de gestion des accès. Les visiteurs doivent être identifiés à l'avance en ne devraient pas pouvoir se déplacer de façon non accompagnée dans votre bâtiment, ni accéder au réseau informatique interne de l'organisation. De même, certains locaux doivent être réservés à certaines catégories de fonction, voire être limités à des personnes habilitées ou ayant fait l'objet de vérification de sécurité (sur base de la loi du 11 décembre 1998 sur la classification, les habilitations et vérifications de sécurité).

Délégation étrangère

La visite d'une délégation étrangère est l'occasion de développer des relations ou des collaborations très utiles. Pour les services de renseignement étrangers, ce contexte constitue aussi une opportunité pour obtenir des informations non accessibles au public ou pour développer des relations exploitables à des fins d'espionnage ou d'ingérence. Les activités socio-culturelles sont particulièrement propices aux échanges informels, parfois inopportuns. Soyez vigilant et assurez-vous que les collaborateurs impliqués disposent de toutes les informations nécessaires pour apprécier le contexte et les limites des échanges souhaités.

VICTIME D'ESPIONNAGE OU D'INGÉRENCE ?

QUE FAIRE ?

Si vous pensez que vous ou votre organisation êtes victime d'activités d'espionnage ou d'ingérence, contactez le responsable de la sécurité de votre organisation ou la Sûreté de l'État (VSSE). Il n'est jamais trop tard pour le signaler mais évitez de mener l'enquête seul.

Informer la Sûreté de l'État est dans l'intérêt de tous. Cela vous permettra de compter sur notre appui en toute discrétion. Grâce à votre collaboration nous pourrons encore mieux protéger plus efficacement les intérêts fondamentaux du pays.

PLUS
D'INFORMATIONS ?

Consultez notre site web : www.vsse.be

Sûreté de l'État (VSSE)
Bd du Roi Albert II, 6 - 1000 Bruxelles

+32 (0) 2 205 62 11
info@vsse.be

VSSE
veiligheid van de staat
sûreté de l'état

D/2021/7951/FR/1244
Éditeur responsable : Jaak Raes - Boulevard du Roi Albert II, 6 - 1000 Brussel