ADIV • SGRS
QUAERO ET TEGO

ESPIONNAGE
SUIS-JE EN DANGER ?

LA DÉFENSE

.be

Contenu

3 ESPIONNAGE ? INGÉRENCE ?

4 INFORMATION SENSIBLE ET CLASSIFIÉE

7 QUE PUIS-JE FAIRE ?

8 DISCRÉTION

10 INTÉGRITÉ

12 ET MAINTENANT ?

Espionnage ? Ingérence ?

Pourquoi des espions s'intéresseraient-ils à moi ? C'est une remarque que l'on entend souvent. Or, l'espionnage et l'ingérence ne relèvent pas de la fiction. Ce sont des méthodes qui sont bel et bien mises en œuvre par des puissances étrangères, soit pour tenter d'obtenir des informations qui ne sont pas accessibles publiquement (il ne s'agit donc pas nécessairement d'informations classifiées ou secrètes), soit pour influencer les processus de prise de décision de manière illicite.

Leur but final ? Obtenir un avantage stratégique sur le plan politique, économique, technologique, scientifique ou militaire. Ce sont surtout les services de renseignement de puissances étrangères qui utilisent de tels moyens. Bien que certains pays soient souvent associés à l'espionnage et à l'ingérence, leurs alliés emploient également des méthodes similaires.

Cette menace implique que vous devez toujours être sur vos gardes dans le monde professionnel. Il y a par ailleurs des acteurs non étatiques, comme des groupes terroristes et des bandes criminelles, qui cherchent également à obtenir des informations qui peuvent leur être utiles dans le cadre de leurs activités et qui utilisent à cet effet des techniques d'espionnage.

Comment s'y prennent-ils ? Cela peut passer par des amitiés en apparence innocentes et le développement de réseaux, et aller jusqu'à la compromission et au chantage purs et durs. Les évolutions technologiques du 21e siècle ont par ailleurs élargi le champ des possibilités en matière d'espionnage technique et d'influence. Citons par exemple le cyberespionnage et la propagation de fake news.

Information sensible et classifiée

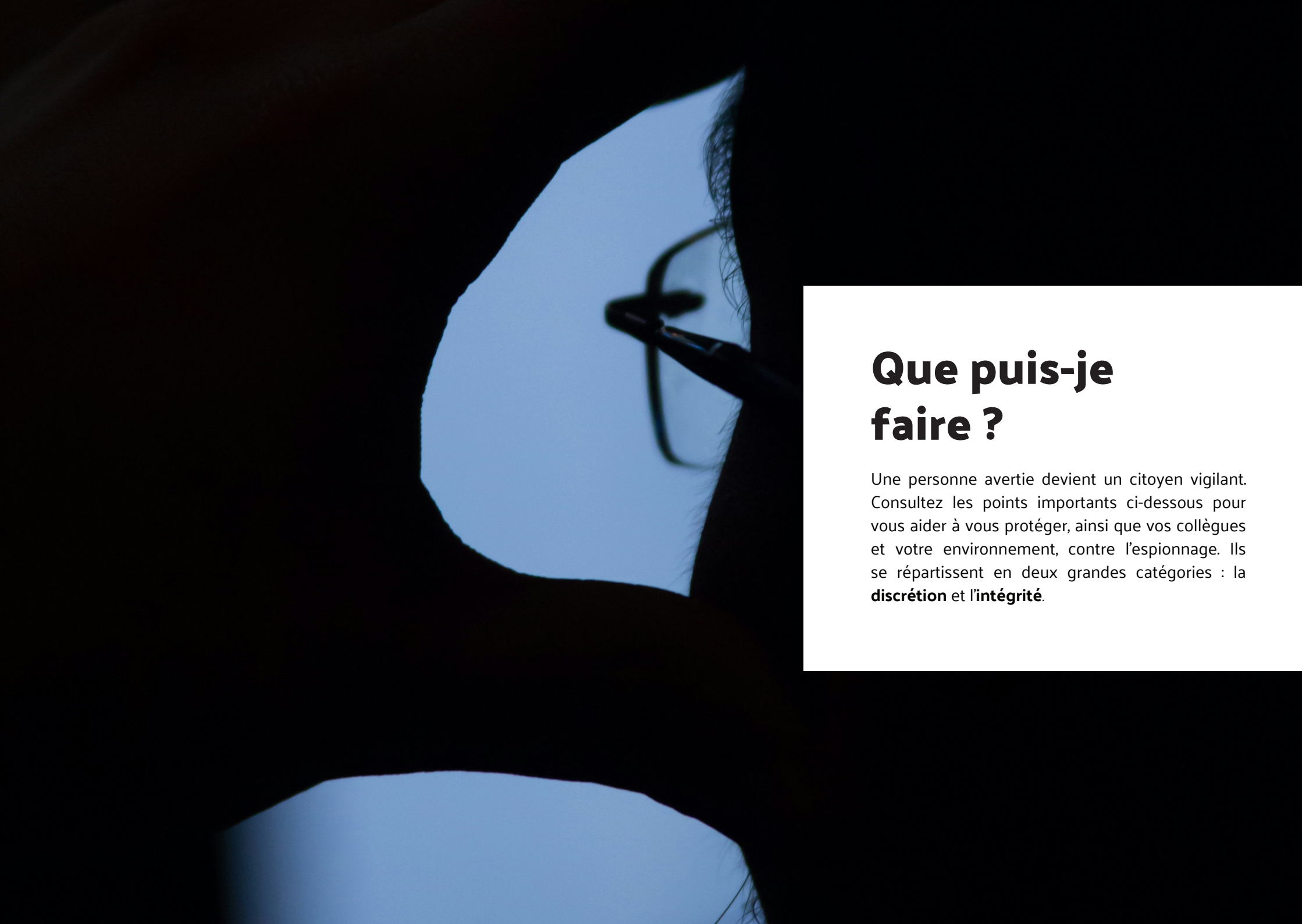
Êtes-vous fonctionnaire ? Employé dans une grande entreprise ? Peut-être scientifique ou chercheur ? Chacun a, par son travail, accès à des informations qui ne sont pas accessibles aux personnes extérieures. Et cela fait peut-être de vous une cible intéressante pour l'espionnage ! En effet, ces informations sont sensibles et peuvent être utilisées à mauvais escient quand elles tombent dans de mauvaises mains. Les espions ne sont donc pas seulement intéressés par les informations classifiées, mais aussi par des informations qui pourraient à première vue vous sembler banales.

CAS I

J.L. est un civil qui occupe un poste de secrétaire à la DGMR. Un jour, il rencontre un certain Pierre, un délégué médical, dans la salle de sport où il se rend de manière régulière. Ils prennent l'habitude de boire un verre au bar après leur sport et, un jour, Pierre demande à J.L. s'il connaît la personne responsable des acquisitions de matériel médical à la Défense .

Au début, J.L. répond à ses questions, mais il remarque après un certain temps que Pierre pose de plus en plus de questions sur les missions qui sont planifiées, sur les intervenants dans les dossiers d'acquisition de matériel IT et sur le projet F-35.

Ce que J.L. ignore, c'est que l'épouse étrangère de Pierre transmet les informations à un service de renseignement offensif .



Que puis-je faire ?

Une personne avertie devient un citoyen vigilant. Consultez les points importants ci-dessous pour vous aider à vous protéger, ainsi que vos collègues et votre environnement, contre l'espionnage. Ils se répartissent en deux grandes catégories : la **discrétion** et l'**intégrité**.

DISCRÉTION

Une remarque souvent entendue est « Je n'ai rien à cacher, ils peuvent tout savoir sur moi ». Mais peut-être avez-vous accès à des informations intéressantes en raison de votre vie privée ou professionnelle. C'est pourquoi, pour vous protéger et protéger vos proches, vous avez tout intérêt à faire preuve de discrétion.

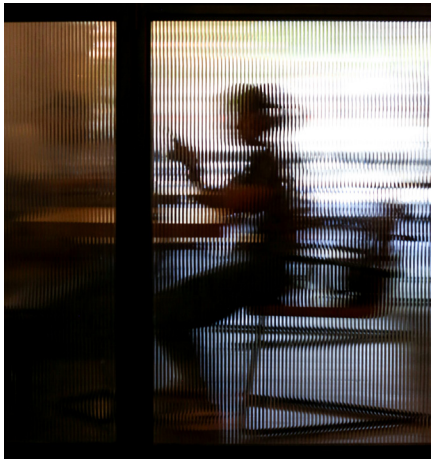
Réseaux sociaux et contacts sociaux

Les services de renseignement offensifs lancent encore souvent leur approche de manière classique, à savoir par le biais de contacts personnels. Plus les espions en savent sur vous et votre vie privée, plus il devient facile pour eux d'engager la conversation avec vous, de vous donner l'impression que vous pourriez bien vous entendre et de créer un lien grâce à vos centres d'intérêt 'communs'.

De cette façon, il est plus facile pour eux d'identifier vos points faibles, votre éventuelle vulnérabilité face à la manipulation ainsi que les moyens de vous compromettre et de faire pression sur vous.

Télétravail

Le télétravail brouille la frontière entre travail et vie privée. Vous travaillez parfois avec des informations sensibles ? Veillez alors à ce que votre environnement de travail soit suffisamment discret. Si vous passez des appels professionnels ou participez à des réunions en ligne depuis votre domicile, demandez-vous qui peut vous entendre. Il est ainsi préférable d'éviter de le faire dans votre jardin, sur votre terrasse, près d'une fenêtre ouverte ou en présence d'autres personnes dans la pièce. De même, demandez-vous par exemple si l'écran de votre ordinateur est visible depuis une fenêtre. Ne laissez pas non plus traîner de documents professionnels chez vous. Si vous travaillez avec des systèmes classifiés quand vous êtes au bureau, assurez-vous de bien faire attention à la frontière entre ce que vous partagez ou non via les réseaux ordinaires. La tentation peut en effet être grande de tout de même communiquer sur des sujets sensibles voire classifiés par téléphone ou par mail lorsque l'on est en télétravail. Utilisez également toujours un VPN quand vous travaillez à domicile.



Voyages à l'étranger

Vous voyagez pour des raisons professionnelles ou privées dans un pays non membre de l'OTAN ? Sachez alors que certains pays n'hésitent pas à installer des appareils d'écoute dans les chambres d'hôtel, à écouter vos conversations téléphoniques ou lire vos e-mails, à demander aux chauffeurs de taxi d'écouter vos conversations ou à vous envoyer des interlocuteurs sympathiques, intéressants et séduisants (mais peu fiables). Si votre organisation dispose d'un responsable de la sécurité, contactez-le et demandez-lui si vous devez prendre des mesures particulières afin de partir l'esprit tranquille.

CAS II

A.V. a effectué des études de traduction et d'interprétation et a effectué un stage dans une entreprise en Asie pendant ses études. Une fois diplômée, elle se met à la recherche d'un emploi et publie son CV en ligne sur son profil LinkedIn. Elle y annonce fièrement qu'elle va travailler pour le ministère de la Défense.

Quelques mois après avoir commencé son travail au ministère de la Défense, elle estvcontactée par Fay, qu'elle avait rencontrée lors de son stage à l'étranger. Fay invite A.V. dans son pays natal pour une conférence et lui demande de venir parler de son expérience en tant qu'étudiante étrangère.

Fay accueille A.V. à bras ouverts, l'invite à des réceptions où elle est présentée à des personnalités locales et montre un intérêt particulier pour le travail d'A.V. au ministère de la Défense. Fay reste quant à elle vague sur son travail et le contexte de toute cette affaire. De retour en Belgique, Fay reste en contact avec A.V. et lui pose de plus en plus de questions sur son travail.

Fay est en contact avec les services de renseignement de son pays et a pour mission de renforcer ses liens d'amitié avec A.V. afin d'évaluer à quelles informations A.V. a accès et comment elle pourrait être convaincue de transmettre ces informations à Fay.

INTÉGRITÉ

Dans le domaine professionnel

Aujourd'hui, **les contacts internationaux** sont monnaie courante pour beaucoup d'entre nous, dans la sphère tant privée que professionnelle. Dans ce dernier cas, ils s'accompagnent souvent d'événements sociaux, tels que des dîners et des réceptions. Il arrive également que des cadeaux d'affaires soient offerts. Il est alors important de veiller à ce que la relation reste professionnelle et équilibrée. Les cadeaux d'affaires ne sont pas toujours inoffensifs. Les clés USB ou autres outils numériques peuvent contenir des logiciels malveillants et ne doivent donc pas être utilisés sans précaution. Assurez-vous de connaître et de respecter la politique de votre organisation en la matière.

Les frustrations entraînent souvent une perte de loyauté envers l'employeur. Un employé frustré est donc une cible facile à manipuler. Les espions sont formés pour exploiter cela.

Les règles et conventions ont pour objectif de permettre à l'organisation de fonctionner correctement. Quelqu'un qui contourne les règles se rend vulnérable au chantage et à la manipulation.

CAS III

Après sa mission au Mali, le capitaine R.S. reste en contact avec Jeremy, qui a également participé à la mission de l'ONU au Mali pour son pays d'origine. Jeremy lui envoie un message pour lui annoncer qu'il est affecté à Bruxelles auprès de son ambassade et lui demande de le rencontrer.

Lors de leurs joyeuses retrouvailles, Jeremy lui demande des conseils sur la vie en Belgique. Au fil des rencontres suivantes, l'ambiance devient de plus en plus amicale. Jeremy invite R.S. à des dîners luxueux et à des événements à l'ambassade. Peu à peu, R.S. remarque que Jeremy lui pose des questions subtiles sur les procédures de la Défense, la préparation des missions, la structure et la planification.

Jeremy s'avère être un officier de renseignement du service de renseignement militaire de son pays et est formé pour transformer des relations professionnelles en relations amicales qu'il peut utiliser, si nécessaire. Le fait que R.S. n'ait jamais signalé au ministère de la Défense ses contacts avec Jeremy peut désormais être utilisé par ce dernier pour faire pression sur lui.

Dans le domaine privé

De par la mondialisation, il n'est pas rare non plus d'avoir **des contacts internationaux** dans la sphère privée. Si vos amis étrangers se montrent particulièrement intéressés par votre travail ou si vous avez l'impression qu'ils se montrent extrêmement serviables, au point que la relation n'est plus équilibrée, cela peut être le signe qu'ils ont des arrière-pensées.

La vie n'est pas toujours un long fleuve tranquille. Nous nous retrouvons parfois indépendamment de notre volonté dans des situations difficiles, même si nous aurions parfois pu les éviter.

Les exemples de situations qui nous rendent particulièrement vulnérables – et par conséquent plus susceptibles d'être victimes de manipulation ou de chantage – sont nombreux. Ils incluent les difficultés financières, les problèmes de santé, les infidélités, les infractions pénales, l'abus d'alcool ou encore les visites à des prostituées (qui sont souvent des personnes d'origine étrangère et qui peuvent elles-mêmes être manipulées par ou soumises aux pressions des services de renseignement de leur pays d'origine).

CAS IV

Sergent G.J. est engagé dans une procédure de divorce conflictuelle. Il vient par ailleurs d'apprendre qu'il n'a pas été promu et se sent frustré car il ne dispose pas des moyens nécessaires pour soulager le mécontentement de ses collaborateurs vis-à-vis des infrastructures.

Lors d'une soirée arrosée, G.J. entame la conversation avec une charmante personne dont il fait la connaissance, une certaine Elisa. Celle-ci lui offre une oreille attentive et il se confie à elle.

Elisa se révèle être une amie proche d'une employée d'une ambassade étrangère, à qui elle transmet régulièrement des informations qu'elle a collectées lors de ses sorties en soirée.

Et maintenant ?

N'importe qui est donc susceptible d'être la cible de techniques d'espionnage. Le bon sens, une attitude loyale et intègre ainsi qu'une bonne prise de conscience de la menace vous aideront déjà à vous protéger vous-même et à protéger vos collègues et votre organisation.

Dans cette brochure, nous accordons beaucoup d'attention aux techniques dites 'HUMINT'. Celles-ci consistent à chercher à obtenir des informations en utilisant les relations interpersonnelles. Ces relations sont souvent très subtiles et la victime tarde donc souvent à se rendre compte que l'interlocuteur a des intentions cachées.

Il ne faut pas pour autant négliger les autres méthodes d'espionnage, souvent techniques. Dans de nombreux cas, le respect des règles de sécurité offrira une bonne protection contre les techniques d'écoute ou de cyber-espionnage.

QUE FAIRE EN CAS DE SOUPÇON D'ESPIONNAGE ?

Signalez toute approche suspecte ou tout soupçon d'espionnage via le formulaire de contact disponible sur notre site web **www.sgrs.be.**

ADIV • SGRS

QUAERO ET TEGO

Éditeur responsable

ADIV - SGRS