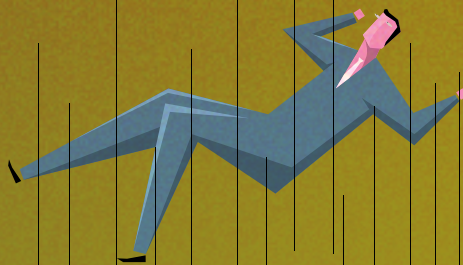




VSSE

veiligheid van de staat
sûreté de l'état



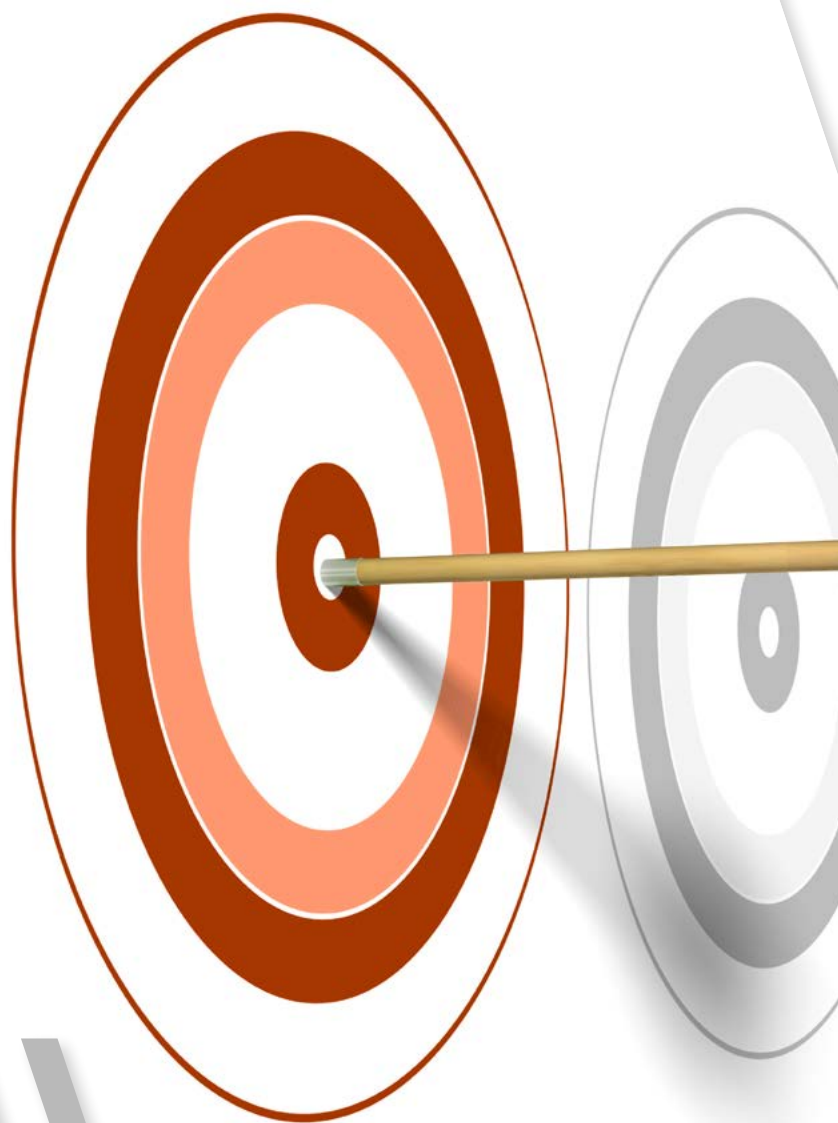
Espionage and interference
Public Services - Diplomacy

DOES THIS
AFFECT YOU?

Espionage and interference are serious threats. Foreign powers are deploying ever greater and more inventive resources to obtain information that is not in the public domain, including through espionage. They also interfere in an attempt to influence decision-making processes.

Employees and representatives of a public service are potential targets of such activity. This makes you a critical link in the security of our institutions and our democratic processes.

How can I protect myself against espionage and interference? The first step is to understand and identify these threats. With this brochure, State Security hopes to help you in this process, and to strengthen your resilience and that of your organisation.



WHAT'S IT ABOUT?



Espionage and interference are inherently low-profile threats. They rely on deceptive or clandestine methods of information-gathering and influence, such as manipulation of people or interception of communications.

The unlawful advantage thus obtained can then be exploited in diplomatic or trade negotiations. It can be used to support domestic companies from these countries, or to destabilise an adversary or a geostrategic competitor.

Some states also use espionage and interference as a tool to control and retain a hold over their communities (diasporas) in our country.

Such methods are most often used by foreign intelligence services, their agents or their allies. And it's not just Russia or China: many foreign powers are involved.

HOW

DOES IT WORK?



Foreign intelligence services work discreetly using covers. Spies may operate in the guise of diplomats, journalists, civil servants, lobbyists, researchers, teachers, or any other position that gives them the legitimacy and credibility to enter into a relationship with you. The number of foreign intelligence professionals deployed undercover in Belgium is in the hundreds, not counting their network of contacts and agents.

They mainly exploit our personal vulnerabilities and the weaknesses in the electronic devices we use each day.

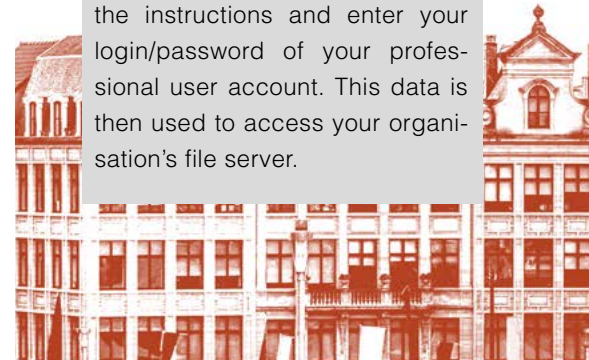
Human manipulations can take extremely varied forms. It could, for example, take the form of a professional or friendly relationship with a hidden agenda concealed by a façade of courtesy, shared ideological or cultural references, or flattery. This type of relationship is generally asymmetrical: the individual will most often initiate contacts and will always be generous and helpful. These seemingly pleasant and harmless manoeuvres serve to build trust, which creates a close, friendly relationship that is conducive to confidences and mutual support. This deceitful behaviour is the breeding ground for manipulation.

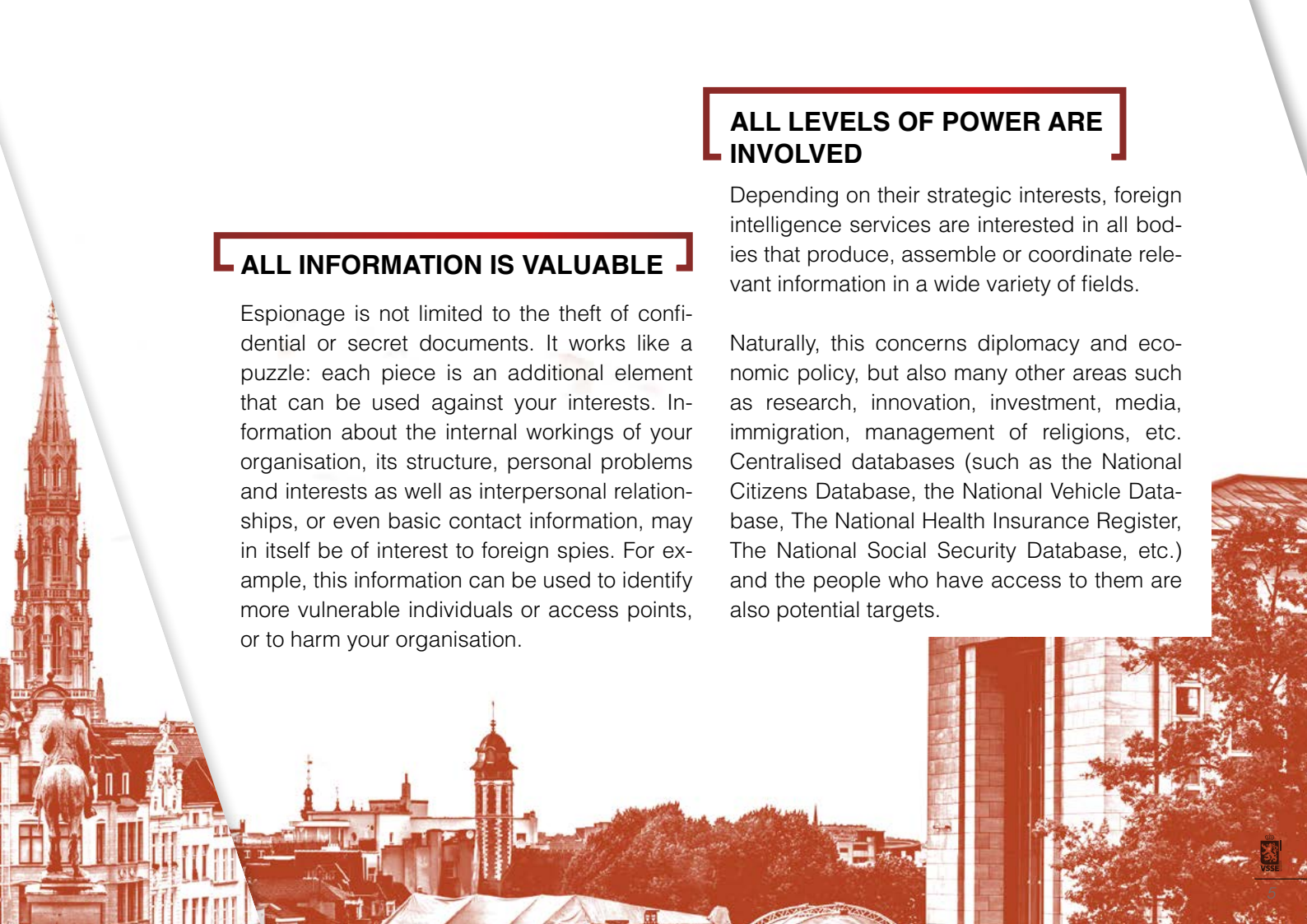
Some examples

1 : Someone you met at a group event invites you to a restaurant. You get on well and meet several times afterwards. With this budding friendship, you let your guard down and share your impressions and all the gossip about the members of the management committee.

Apart from human manipulation, technical manipulation is also on the rise, facilitated by our increasing dependence on digital technologies and mobile devices.

2 : After clicking on a seemingly legitimate hyperlink, you follow the instructions and enter your login/password of your professional user account. This data is then used to access your organisation's file server.





ALL INFORMATION IS VALUABLE

Espionage is not limited to the theft of confidential or secret documents. It works like a puzzle: each piece is an additional element that can be used against your interests. Information about the internal workings of your organisation, its structure, personal problems and interests as well as interpersonal relationships, or even basic contact information, may in itself be of interest to foreign spies. For example, this information can be used to identify more vulnerable individuals or access points, or to harm your organisation.

ALL LEVELS OF POWER ARE INVOLVED

Depending on their strategic interests, foreign intelligence services are interested in all bodies that produce, assemble or coordinate relevant information in a wide variety of fields.

Naturally, this concerns diplomacy and economic policy, but also many other areas such as research, innovation, investment, media, immigration, management of religions, etc. Centralised databases (such as the National Citizens Database, the National Vehicle Database, The National Health Insurance Register, The National Social Security Database, etc.) and the people who have access to them are also potential targets.

HOW

DO I PROTECT MYSELF?

To defend yourself, it is essential to be aware of your vulnerabilities and to protect yourself as much as possible, both individually and collectively.

RAISING AWARENESS AMONG YOUR EMPLOYEES AND COLLEAGUES IS AN ESSENTIAL FIRST STEP.

It is important to understand that the risks are real, even if the consequences are not always obvious. Please feel free to circulate this brochure within your organisation and to contact State Security for additional information.

(Preventive) security measures should then be taken. In other words, risks must be reduced by implementing a security policy that is as comprehensive and proactive as possible. The measures should be aimed at limiting exposure to threats but also at limiting their potential impact. Be resilient!



POINTS FOR ATTENTION

Frustration leads to manipulation

Offensive intelligence services specialise in manipulating people. They take advantage of individuals' weaknesses and frustrations. A lack of recognition, built-up resentments or unresolved issues constitute the ideal basis for such manipulation work. Sound and caring human resource management is crucial to prevention.

Need-to-know

Make sure that only those staff members who need it for their daily work have access to the most sensitive data. By applying the «need-to-know» principle you can limit the risk of this information falling into the wrong hands. Similarly, a suitable destruction procedure for documents containing sensitive information ensures better protection of confidentiality.



Be discreet

Do not view or discuss sensitive information in public places. Someone may take advantage of this to gain knowledge of it without you knowing. The malicious or simply inappropriate use of information obtained in this way can damage your organisation.



Always reachable = always traceable

Smartphones make life easier for you and for intelligence services. High-tech malware can intercept your data or attack your device. Keep your operating system and applications up to date and use robust authentication methods. When storing or accessing sensitive data from your smartphone, use encryption software and a VPN. It is strongly recommended to have a separate device for use exclusively when travelling abroad.



Foreign travel

Outside our borders, we are more vulnerable, and offensive intelligence services have greater power. Travel is an excellent opportunity for espionage. It is therefore essential to take extra precautions. The watchwords are: caution and discretion. Reduce exposure by keeping your documents to a minimum and securing your media. You can find additional recommendations in our «Travel Security» brochure (www.vsse.be).






Social media

Offensive services are also exploiting new social media opportunities. These platforms greatly facilitate the profiling of potential targets and provide further methods of making contact. Make sure you know any person who wants to become your «friend» or online contact. Be aware that accepting a new contact allows him/her to access your circle of online friends, while providing a significant legitimacy boost that could facilitate future attempts at manipulation.

Control, verification and approval

Without being naïve or paranoid, make sure you have a comprehensive access control and management policy in place. Visitors must be identified in advance and should not be allowed to move unaccompanied through your building or access your organisation's internal computer network. Similarly, certain premises must be reserved for certain categories of function, or even be restricted to authorised persons only or persons who have undergone a security check (based on the law of 11 December 1998 on Classification, security clearances, certificates and advice).



Foreign delegation

A visit by a foreign delegation is an opportunity to forge very useful relationships or collaborations. For foreign intelligence services, it is also an opportunity to obtain information that is not in the public domain or to develop relationships that can be exploited for espionage or interference. Socio-cultural activities are particularly conducive to informal and sometimes inappropriate exchanges. Be vigilant and make sure that the employees involved have all the necessary information to evaluate the situation and understand what constitutes harmless exchanges.

I HAVE BEEN THE VICTIM OF ESPIONAGE OR INTERFERENCE. WHAT CAN I DO ?

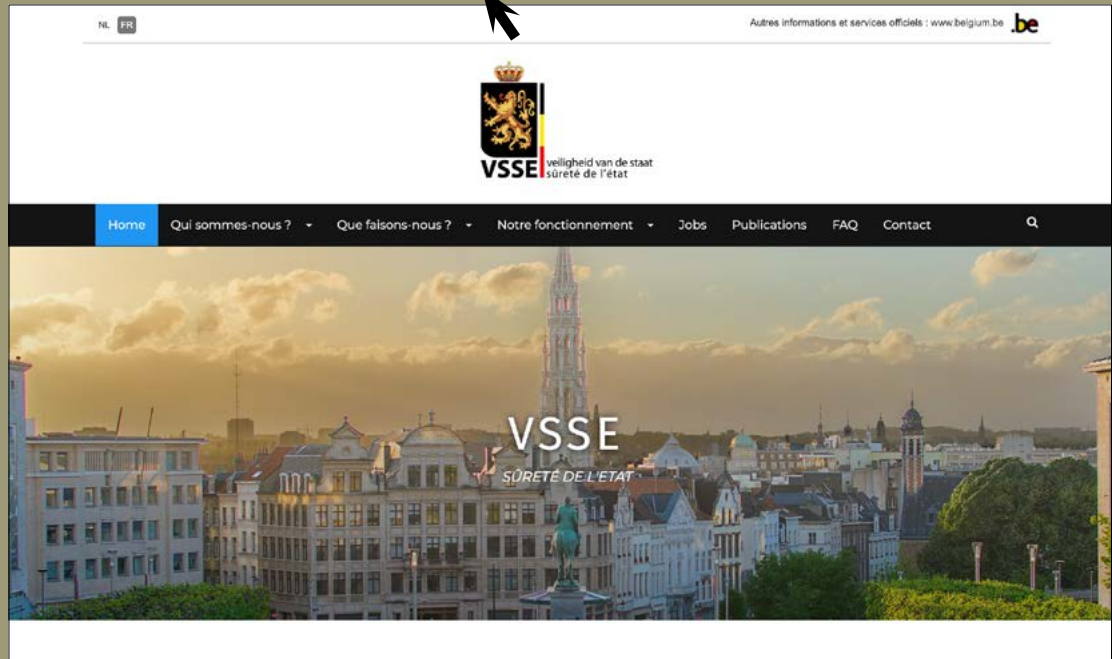
If you believe that you or your organisation has been a victim of espionage or interference, contact your organisation's security officer or State Security (VSSE). It's never too late to report it, but don't investigate on your own.

Informing State Security is in everyone's interest. By doing so you can obtain our support with total discretion. With your cooperation we will be able to protect the country's fundamental interests even more effectively.



NEED MORE INFORMATION?

Visit our website: www.vsse.be



State Security (VSSE)
Boulevard du Roi Albert II, 6 - 1000 Brussels

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

