TECHNOPOL
Un module du programme
de sensibilisation Prophylax

LE MONDE ACADÉMIQUE EN LIGNE DE MIRE

Espionnage et prolifération dans les milieux académiques

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Service de renseignement de la Confédération SRC

TECHNOPOL
Un module du programme de sensibilisation Prophylax

LE MONDE ACADÉMIQUE EN LIGNE DE MIRE

Espionnage et prolifération dans les milieux académiques

TABLE DES MATIÈRES

INTRODUCTION

Le Service de renseignement de la Confédération (SRC) réalise depuis 2004 le programme Prophylax, dont l'objectif est de sensibiliser les entreprises, les organisations économiques et les instituts de recherche aux menaces de prolifération et d'espionnage. Prophylax répond au mandat légal du SRC, qui consiste à mettre en œuvre des programmes d'information et de sensibilisation aux menaces pour la sûreté intérieure et extérieure de la Suisse (Art. 6, al. 6 Loi sur le renseignement, LRens). Faisant partie intégrante du programme Prophylax, Technopol vise à sensibiliser les universités, les hautes écoles et les instituts de recherche en Suisse et au Liechtenstein.

Technopol s'adresse aux membres d'universités, de hautes écoles et d'instituts de recherche et montre pourquoi de telles institutions peuvent constituer une cible intéressante pour des services de renseignement étrangers. Ce programme vise également à accroître la prise de conscience de la menace de l'espionnage et du potentiel d'utilisation abusive des connaissances ainsi que du savoir-faire dispensés dans l'enseignement, la recherche et l'administration des institutions susmentionnées. Outre la sensibilisation, Technopol fournit à son public cible des mesures de sécurité concrètes pour mieux prévenir le transfert illégal de connaissances et de technologies ainsi que la fuite d'informations et de données.

Les hautes écoles et les instituts de recherche dépendent des échanges internationaux d'informations scientifiques et de résultats de recherche. Ces échanges sont grandement favorisés par l'Union européenne (UE). La libre circulation des chercheurs ainsi que le libre accès aux résultats de recherche et aux technologies sont en effet encouragées au sein de l'Espace européen de la recherche (EER). La Suisse est associée à la gouvernance de ce dernier au cas par cas, en tant que l'un des principaux pays tiers. Les programmes-cadres pluriannuels de l'UE pour la recherche et l'innovation constituent des outils importants dans la mise en œuvre de l'EER. Les universités européennes, respectivement les partenaires des projets, sont tenus de participer activement au transfert de connaissances en partageant leurs propres données de recherche pour bénéficier du réseau de l'EER et prendre part aux programmes-cadres.

Bien que leurs résultats de recherche soient accessibles au public, les universités et les instituts de recherche restent menacés par des activités d'espionnage et de prolifération, comme le montrent les explications suivantes.

LES HAUTES ÉCOLES ET LES INSTITUTS DE RECHERCHE EN LIGNE DE MIRE

RENFORCER LA PRISE DE CONSCIENCE

La collaboration internationale, la mobilité des étudiants et des scientifiques ainsi que l'échange de connaissances sont essentiels pour le domaine de la recherche et ne doivent pas être entravés. Il est toutefois primordial que les hautes écoles et les instituts de recherche prennent conscience de la menace de l'espionnage et de la prolifération et qu'ils fassent preuve de prudence lorsqu'ils possèdent un savoir-faire critique. Il s'agit de sensibiliser et de former tous les membres de hautes écoles et d'instituts de recherche (scientifiques, professeurs, collaborateurs, etc.) et de bien connaître les technologies qui font l'objet d'un contrôle des exportations ainsi que la demande d'autorisations d'exportation auprès du Secrétariat d'État à l'économie (SECO), si ces technologies devaient être transférées à l'étranger.

Il incombe à la Suisse et aux hautes écoles et instituts de recherche établis sur son territoire de s'assurer que les connaissances produites ou acquises en Suisse par des étudiants et des scientifiques ne soient pas utilisées à des fins illégales. Ignorer les menaces qui en découlent peut avoir de graves conséquences pour une institution si elle est effectivement la cible d'activités d'espionnage ou de prolifération. Ces organismes risquent en outre de perdre des contrats et des fonds de recherche, d'être exclus d'instances de recherche internationales, de voir leur réputation entachée et de reculer dans les classements internationaux. La fuite vers l'étranger de résultats de recherche confidentiels peut par ailleurs nuire durablement à la compétitivité internationale de la Suisse dans le domaine de la recherche. Les personnes qui commettent des actes d'espionnage contre les intérêts de la Suisse pour le compte d'un service de renseignement étranger mettent leur avenir en danger. Elles risquent la prison et compromettent leur carrière.

CULTURE OUVERTE

Le niveau élevé en matière de technologies et de connaissances ainsi que l'ouverture et la culture d'accueil des universités, hautes écoles et instituts de recherche suisses sont reconnus dans le monde entier. Des chercheurs étrangers y trouvent par exemple des laboratoires de recherche à la pointe du progrès pour réaliser leurs expériences scientifiques.

Mais l'accès aisé aux bâtiments, la politique de libre-échange d'informations scientifiques, la collaboration avec des entreprises technologiques ainsi que la composition internationale du corps enseignant et étudiant font également des hautes écoles des cibles attractives pour les services de renseignement étrangers. Ces derniers tentent d'obtenir des expertises ou des données de recherche liées à des technologies sensibles (par exemple robotique, nouveaux matériaux, nanotechnologies) afin de combler des lacunes dans les connaissances de leur pays. L'État et son industrie économisent ainsi des frais considérables en matière de recherche, car l'espionnage d'une technologie recherchée ou d'un produit s'avère souvent moins coûteux que l'investissement de ressources financières et humaines dans des projets de recherche et de développement.

EXEMPLE

En 2014, un physicien étranger travaillant dans une université néerlandaise a été arrêté. Il était soupçonné d'avoir fourni des données de recherche confidentielles au service de renseignement extérieur de la Fédération de Russie (SVR). Le physicien avait attiré l'attention de l'Office fédéral allemand de protection de la Constitution (Bundesamt für Verfassungsschutz, BfV) dans le cadre de l'observation d'un officier du SVR agissant sous couverture diplomatique au Consulat général russe de Bonn. Les deux hommes se retrouvaient une fois par mois à Aix-la-Chapelle (Allemagne), où le faux diplomate remettait de l'argent au physicien. Celui-ci effectuait à chaque fois le trajet des Pays-Bas à Aix-la-Chapelle en voiture. Après l'arrestation du physicien, l'université a mené une enquête interne et privé le scientifique de son droit d'accès. Le Ministère de la justice des Pays-Bas a jugé qu'il représentait un « danger pour la sécurité nationale du pays », lui a retiré son visa Schengen et a émis une interdiction d'entrée à son encontre.

COLLABORATION AVEC DES TIERS

De nombreux instituts de recherche coopèrent avec des entreprises privées et des autorités étatiques, qui financent également certains projets de recherche. Les scientifiques impliqués bénéficient donc d'un accès à des expertises et des informations sensibles. Une première application des résultats de recherche sur le marché est nécessaire pour que les investissements en matière de recherche soient rentables pour les entreprises et les autorités. La divulgation de données et résultats de recherche à des tiers à la suite d'une opération d'espionnage équivaut à un vol de moyens financiers. Un tel acte compromet la collaboration avec l'institut de recherche. La reconnaissance espérée par les scientifiques pour la réalisation de travaux de recherche novateurs risque elle aussi d'être compromise, si quelqu'un publie ces résultats ou les utilise en premier.

RECHERCHE

Le SRC estime que la recherche appliquée dans les domaines techniques et scientifiques comme le génie mécanique, la technologie aérospatiale, l'électrotechnique, les sciences des matériaux, la chimie, la biologie ou l'informatique est particulièrement exposée au risque de transfert illégal de connaissances. La recherche fondamentale peut toutefois également s'avérer critique, notamment lorsque des étudiants ou scientifiques acquièrent des méthodes et des techniques qu'ils peuvent transmettre à autrui ou utiliser abusivement à d'autres fins (dual-use research of concern). De plus, les domaines non techniques sont également susceptibles d'éveiller l'intérêt d'une autorité étatique étrangère, notamment lorsqu'ils traitent de thèmes politiques concernant cet Etat.

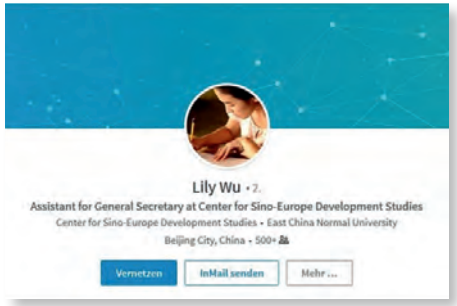
ACTIVITÉS DES SERVICES DE RENSEIGNEMENT ÉTRANGERS

ESPIONNAGE

L'espionnage désigne l'acquisition d'informations et de données dans les domaines de la politique, de l'économie, de l'armée, des sciences et des technologies, au détriment de la Suisse, de ses habitants, ses autorités, ses entreprises ou ses institutions, ainsi que la transmission de ces informations à des acteurs étrangers (État, groupe, entreprise, individu, etc.).

EXEMPLE

Un jeune scientifique d'une université européenne a reçu une demande de contact de la part d'un collaborateur d'un think tank asiatique à travers le réseau professionnel Linkedin. Celui-ci s'est montré intéressé par le travail du scientifique et par un échange entre spécialistes. Le think tank a invité le scientifique et a payé le coût total du voyage et du séjour. Sur place, le scientifique a rencontré les collaborateurs du think tank, qui étaient en réalité des représentants du service de renseignement local. Le service de renseignement a alors tenté de recruter le scientifique comme source d'informations afin d'obtenir des données sensibles relatives à son domaine professionnel.



Faux profil Linkedin utilisé par un service de renseignement chinois pour prendre contact avec des personnes potentiellement intéressantes

TALENT SPOTTING

Pour un officier de renseignement, la participation à des événements universitaires publics (conférences, séminaires, etc.) est l'occasion idéale pour s'entretenir avec les personnes présentes sans attirer l'attention. Il s'intéresse aux experts et tente de leur soutirer des informations confidentielles de manière subtile (par exemple renseignements sur des projets de recherche actuels) en dirigeant habilement la conversation. Il cherche également à identifier des personnes défendant certains points de vue politiques ou idéologiques, ainsi que de jeunes universitaires susceptibles de décrocher un poste sensible au sein d'un organisme gouvernemental ou une position stratégique auprès d'une entreprise dans un domaine de haute technologie. Les relations amicales avec ces personnes sont entretenues sur le long terme, au cas où un nouvel emploi leur donnerait accès à des informations sensibles.

EXEMPLE

Une étudiante européenne s'est rendue dans un pays asiatique pour un séjour académique d'une année. Sur place, un professeur de l'université lui a présenté une collaboratrice du service de renseignement étatique qui se faisait passer pour une étudiante locale. L'étudiante européenne a été invitée à rédiger contre rémunération des rapports pour le compte d'un institut de recherche. Il s'agissait en réalité d'un institut de couverture utilisé par le service de renseignement pour approcher des étudiants européens et les recruter en vue d'une collaboration à long terme.

OBSERVATION DE SES PROPRES CONCITOYENS

Certains services de renseignement surveillent leurs citoyens établis à l'étranger, parmi lesquels des opposants au régime et des membres de diasporas. Ils le font notamment au sein de hautes écoles et d'instituts de recherche, où les services récoltent par exemple des photos et du matériel audio sur des individus prenant part à des réunions publiques de groupes d'opposition. Certains États instrumentalisent en outre des associations d'étudiants nationales établies au sein des universités pour contrôler leurs membres. À cette fin, les ambassades invitent régulièrement des étudiants à leurs événements. De telles activités de surveillance sont illégales en Suisse et enfreignent l'art. 272 du code pénal (service de renseignements politiques).

Les États autoritaires, en particulier, font appel à la loyauté de leurs ressortissants pour servir leur patrie. Ils leur demandent de leur fournir les connaissances qu'ils ont acquises à l'étranger, par exemple en participant à des projets de recherche sur le développement de systèmes d'armes. Certains États récompensent leurs meilleurs étudiants en leur offrant la possibilité de poursuivre leurs études ou leur doctorat à l'étranger durant un ou plusieurs semestres. Ce type de séjour est souvent financé par l'État, qui attend de ces personnes qu'elles lui rendent un service en contrepartie. Les étudiants sont tenus de travailler un certain nombre d'années dans leur pays d'origine après leur retour, au sein d'une entreprise étatique ou privée, ou pour une autorité.

EXEMPLE

Un doctorant étranger inscrit dans une université suisse a pris contact avec la police après s'être senti surveillé par certains de ses compatriotes, membres de l'association des étudiants de leur pays. L'enquête de la police a révélé que ces personnes avaient été chargées par leur ambassade de surveiller d'autres étudiants. Leur mission était de signaler à l'ambassade toute situation où le comportement des étudiants divergeait des attentes et des directives politiques de leur pays.

SÉJOURS D'ÉTUDES À L'ÉTRANGER

Le risque d'être victime d'actes d'espionnage augmente sensiblement lors de séjours à l'étranger. Les étudiants et scientifiques qui effectuent un ou plusieurs semestres au sein d'une haute école ou d'un institut de recherche à l'étranger risquent d'y être abordés par le service de renseignement local. Celui-ci cherchera à obtenir des renseignements sur des connaissances et des technologies ainsi que des données confidentielles et des informations non accessibles au public. Il peut par exemple tenter d'établir une relation durable avec un étudiant et de motiver cette personne à décrocher un poste auprès d'un organisme gouvernemental dans son propre pays, cela afin d'accéder à des informations classées. La transmission de telles informations à un service de renseignement étranger est souvent récompensée par une somme d'argent ou par d'autres avantages. Il s'agit d'un acte d'espionnage pour le compte d'un État étranger.

CYBERATTAQUES

L'infrastructure réseau d'une haute école ou d'un institut de recherche est particulièrement exposée aux cyberattaques en raison du grand nombre d'utilisateurs, de leurs connaissances souvent limitées en matière de protection des informations, des faibles restrictions d'accès et des nombreux points de connexion Internet. Un risque d'espionnage pèse en particulier sur les bases de données électroniques de hautes écoles et d'instituts de recherche, car elles contiennent souvent des informations importantes et sensibles. Les réseaux informatiques des hautes écoles font l'objet d'un nombre croissant de cyberattaques visant par exemple à obtenir des données d'accès ("credential phishing") d'étudiants ou de collaborateurs au moyen de courriels d'hameçonnage (phishing). Mais le pirate informatique peut également se servir de l'infrastructure réseau d'une université comme d'un intermédiaire pour attaquer des entreprises ou des organisations.

EXEMPLES D'ESPIONNAGE

Approche d'étudiants en échange

- Lorsqu'il construit une relation avec un étudiant étranger, l'officier de renseignement ne se présente pas comme collaborateur d'un service de renseignement, mais agit sous couverture, par exemple en se faisant passer pour un étudiant ou un membre d'un think tank, d'un institut de recherche, d'une école de langue ou d'une entreprise de conseil. Il prend contact avec l'étudiant sous un prétexte plausible, en lui proposant par exemple un poste ou un stage intéressant, un mandat pour un article ou un échange linguistique. Il établit le contact soit en personne, soit par voie électronique. Les réseaux sociaux comme Linkedin ou Facebook, en particulier, permettent aux services de renseignement étrangers de recueillir des informations sur une cible et d'établir un premier contact en vue d'un recrutement.

- Un service de renseignement étranger demande à un étudiant d'accomplir un travail donné ou d'obtenir certaines informations contre rémunération. Il ne s'agit pas nécessairement d'informations sensibles. L'objectif est d'évaluer les aptitudes de la personne en tant qu'informateur potentiel.

- Un service de renseignement étranger charge un professeur de recruter des étudiants étrangers.

- Le pays hôte accuse un étudiant d'avoir enfreint la loi ou l'ordre établi, afin de le mettre sous pression et de le forcer à collaborer avec son service de renseignement.

- Sous couvert d'une enquête générale portant sur le séjour des étudiants dans le pays qui les héberge et sur leurs impressions (par exemple au moyen d'un formulaire), le service de renseignement étranger tente d'établir un profil de l'étudiant et d'obtenir des informations sur ses intérêts, ses proches ou ses points faibles.

ABUS DES CONNAISSANCES ET TECHNOLOGIES

PROLIFÉRATION

On entend par prolifération d'une part la dissémination d'armes de destruction massive (armes nucléaires, biologiques et chimiques) ainsi que de leurs vecteurs (missiles balistiques, missiles de croisière, aéronefs hypersoniques et drones), et d'autre part celle d'équipements, de matériaux et de technologies pouvant également être employés dans la fabrication de ces armes (biens à double usage).

EXEMPLE

Un scientifique originaire d'un État souhaitant acquérir un savoir-faire utile en matière de technologie militaire s'est perfectionné auprès d'une haute école suisse, cette technologie de pointe ne pouvant pas être développée dans son propre pays. L'acquisition de cette technologie était pilotée par l'État : le scientifique avait été mandaté par le service de renseignement de son pays d'origine. Comme il s'agissait d'une technologie dite à double usage (à savoir utile aussi bien à des fins civiles que militaires), la haute école suisse ne pouvait que difficilement déterminer dans quelle mesure les connaissances acquises par le scientifique en Suisse étaient destinées à être utilisés pour un projet militaire à l'étranger.

TRANSFERT IMMATÉRIEL DE CONNAISSANCES ET DE TECHNOLOGIES

L'espionnage et le transfert illégal de propriété intellectuelle, de savoir-faire et de technologies (transfert immatériel de technologie, "Intangible Transfer of Technology ITT") qui en découle sont souvent liés à des efforts d'acquisition ayant trait à la prolifération. Des conventions internationales, des sanctions ainsi que des régimes de contrôle des exportations ont été établis pour éviter la prolifération d'armes de destruction massive. Ces réglementations limitent non seulement l'exportation de biens critiques (biens à double usage), mais également celle de connaissances, de technologies et d'assistance technique s'il apparaît que ces éléments risquent d'être utilisés dans un programme de développement ou de production d'armes de destruction massive ou de leurs vecteurs. En effet, un certain savoir-faire peut également être transféré d'un projet de recherche civil vers une application militaire. Les restrictions concernent aussi bien les exportations physiques (par exemple envoi d'un document par voie postale) que les exportations immatérielles, notamment au format électronique (par exemple envoi par services cloud, courriel, fax, FTP). Pour contourner ces mesures de contrôle, les services de renseignement étrangers tentent de recruter des scientifiques qui ont ou avaient accès à des technologies sensibles et qui sont à même de transmettre les informations à ce sujet. Les services de renseignement étrangers envoient également leurs propres officiers de renseignement dans des universités ou des instituts de recherche à l'étranger afin que ceux-ci obtiennent des résultats de recherche et un savoir-faire critique en se faisant passer pour des doctorants ou des scientifiques invités. Dans certains cas, ils obtiennent également l'accès à des infrastructures critiques ou à des laboratoires de recherche d'entreprises privées qui collaborent avec l'université. Des technologies encore en phase de développement qui ne sont pas classifiées peuvent s'avérer intéressantes pour des services de renseignement étrangers, si le champ d'application de la technologie, une fois aboutie, est jugé critique par la suite.

VIOLATION DU PRINCIPE DE CONTRÔLE DES EXPORTATIONS

Les établissements scientifiques n'enquêtent que de manière superficielle sur le profil des nouveaux étudiants ou scientifiques, puisqu'ils s'intéressent essentiellement aux compétences requises pour les besoins de l'étude ou du programme de recherche. S'il s'avère que les collaborateurs d'une haute école ou d'un institut de recherche ont transmis des connaissances critiques qu'ils ont acquises en Suisse (susceptibles par exemple d'être appliquées dans un programme d'armes de destruction massive) à une autorité ou à une entreprise étrangère, la haute école ou l'institut de recherche peuvent être tenus responsables d'avoir violé le principe de contrôle des exportations.

EXEMPLE

Un professeur de physique européen travaillait dans le domaine de la technologie aérospatiale, sur des projets de l'Agence spatiale européenne. Ses recherches concernaient le domaine civil, mais pouvaient également avoir des applications militaires. Le physicien engageait régulièrement des chercheurs étrangers invités, dont une chercheuse chinoise qui prétendait appartenir à l'Académie chinoise des sciences (un institut civil). Sur un réseau social, celle-ci indiquait toutefois l'adresse d'un organisme de recherche militaire chinois sous ses coordonnées et mentionnait un de ses articles traitant de la précision des missiles antisatellites. Le professeur a redoublé de méfiance lorsque la chercheuse chinoise lui a posé de nombreuses questions sur l'application militaire de son domaine de recherche. Il a fini par mettre un terme à leur collaboration.

EXEMPLES D'ACQUISITION

Indicateurs possibles d'une utilisation abusive de connaissances ou d'une fuite de données

- Demandes de partenariats de recherche ou de visites de laboratoires
- Séjours à l'étranger de doctorants ou de scientifiques à des fins de recherche
- Prise de contact par les réseaux sociaux (par exemple Linkedin) ou lors d'événements publics, avec la demande d'un échange ou d'une opinion d'expert sur un sujet spécifique
- Invitations non sollicitées de scientifiques et de professeurs à des conférences ou à des échanges universitaires à l'étranger, demandes de contribution à des revues scientifiques ou d'examen d'articles de recherche (peer review)
- Participation à des conférences scientifiques concernant des technologies à double usage
- Désintérêt d'un doctorant étranger pour les travaux de recherche, mais volonté d'obtenir des droits d'accès étendus aux projets en cours et aux données de recherche ; curiosité marquée, plus prononcée que la moyenne
- Changement de cursus après le début des études (le cursus envisagé par l'étudiant originaire d'un État préoccupant est examiné avec précision avant l'octroi du visa ; ce dernier peut être refusé si l'étudiant souhaite étudier dans un domaine considéré comme critique)
- Perte/vol de matériel de laboratoire ou informatique
- Accès non autorisé aux systèmes informatiques ou aux bases de données de la haute école ou de l'institut de recherche
- Scientifiques invités provenant d'une université ou d'un institut de recherche sanctionnés
- Professeurs et scientifiques originaires d'États préoccupants (states of concern) ou entretenant des relations avec ces États [1]
- Scientifiques invités ou doctorants étrangers bénéficiant d'une bourse financée par l'État, en particulier si l'expertise ou les compétences linguistiques de ces personnes s'avèrent insuffisantes (si elles ne correspondent pas aux connaissances indiquées dans le curriculum vitae)
- Visites de délégations scientifiques étrangères
- Coopérations, programmes d'échange, déclarations d'intention, etc., avec des hautes écoles, laboratoires de recherche, entreprises ou think tanks étrangers liés à l'industrie de l'armement ou qui, selon des sources ouvertes seraient impliqués dans des activités de prolifération ou auraient des liens avec des services de renseignement
- Projets et coopérations de recherche dans des domaines sensibles, financés par une entreprise étrangère (par exemple du domaine de l'armement) ou un État tiers
- Programmes d'études ou instituts de hautes écoles suisses fondés ou financés par des organisations étrangères

[1] Aujourd'hui, sont généralement considérés comme États préoccupants (states of concern) l'Iran, la Corée du Nord, le Pakistan et la Syrie. Il est établi que ces États mènent des programmes de développement d'armes de destruction massive ou qu'ils produisent déjà de telles armes. Ces pays représentent une menace pour la sécurité internationale, car il y a lieu de craindre qu'ils utilisent des armes de destruction massive dans la poursuite d'objectifs politiques ou lors d'un conflit armé.

Abus des connaissances et technologies

MESURES DE PROTECTION ET BONNES PRATIQUES

INSTITUTIONS

- Savoir quelles technologies sont soumises au contrôle des exportations (connaissances des lois en vigueur sur le contrôle des exportations et des biens), implémenter un contrôle interne du respect des prescriptions en matière de contrôle des exportations (programme interne de conformité) et nommer une personne responsable au niveau de la direction pour les questions relatives au contrôle des exportations
- Définir quels sont les secteurs spécialisés et les domaines de recherche critiques au sein de la haute école ou de l'institut de recherche
- Examiner les risques de prolifération dans le domaine des technologies sensibles lors du recrutement d'étudiants ou de scientifiques étrangers dans un domaine spécialisé considéré comme critique
- Contrôler régulièrement l'inventaire du matériel critique du laboratoire
- Nommer une personne responsable de la sécurité de l'information et effectuer des contrôles réguliers en matière de sécurité de l'information
- Sensibiliser régulièrement les scientifiques, les chercheurs, les professeurs et autres collaborateurs de la haute école ou de l'institut de recherche à l'utilisation abusive de données de recherche (recherche à double usage préoccupante), aux biens et technologies à double usage ainsi qu'aux aspects de la sécurité de l'information et de la sécurité informatique
- Restreindre les droits d'accès des collaborateurs, scientifiques et étudiants aux données ainsi qu'au réseau informatique de la haute école ou de l'institut de recherche
- Dissocier les différents réseaux informatiques (réseau de recherche séparé d'Internet et du reste du réseau informatique de l'établissement)
- Créer un réseau de responsables de la sécurité des hautes écoles et instituts de recherche pour l'échange des expériences et des informations relatives à des incidents

PERSONNEL [1]

- Ne pas ouvrir les pièces jointes ou liens contenus dans des courriels provenant de personnes inconnues
- Faire preuve de prudence lors de prises de contact non sollicitées (par courriel, sur les réseaux sociaux, etc.) qui concernent par exemple des partenariats de recherche ou des programmes d'échange
- Crypter le disque dur des ordinateurs de bureau et des ordinateurs portables, à savoir les données qui y sont stockées
- Utiliser une connexion sécurisée (Virtual Private Network, VPN) pour accéder au réseau de la haute école ou de l'institut à distance
- Utiliser impérativement un VPN pour accéder à Internet au moyen de connexions WiFi publique, même celles qui sont protégées par un mot de passe
- (par exemple dans les hôtels, les cafés ou les aéroports). Si les VPN sont bloqués dans le pays hôte,
  accéder à Internet par une connexion 3G/4G/5G en mode itinérance (roaming)
- Ne jamais laisser des ordinateurs portables et tout autre matériel électronique sans surveillance (par exemple pendant une pause-café lors d'une conférence ou même pour aller aux toilettes)
- Ne pas utiliser d'appareils périphériques externes qui ont été offerts ou prêtés (clés USB, disques durs externes, téléphones portables, appareils photo numériques, etc.) et ne pas connecter de tels appareils à des ordinateurs portables ou des réseaux personnels
- Signaler les événements suspects aux responsables de la sécurité de la haute école ou de l'institut de recherche

[1] Scientifiques, professeurs et autres collaborateurs

ÉTUDIANTS

- Veiller à ne pas divulguer des informations personnelles et professionnelles critiques sur les réseaux sociaux (autant que nécessaire, aussi peu que possible)
- Se méfier des propositions financières alléchantes
- Se méfier des prestations de soutien gratuites à l'étranger, en particulier lorsque celles-ci ont trait à l'administration, comme l'octroi d'un visa ou la prolongation d'une autorisation de séjour
- Faire preuve de vigilance, surtout lorsque des personnes se montrent trop curieuses ou envahissantes. Ne pas transmettre d'informations exactes ni faire de promesses, rompre rapidement toute relation avec les personnes qui ont un comportement suspect
- Vérifier si l'institution ou le domaine d'activité indiqué par une personne existe bel et bien et, le cas échéant, si le nom de cette personne figure sur le site internet de l'établissement
- Informer la représentation suisse à l'étranger (ambassade, consulat), l'université d'origine ou le SRC de toute activité suspecte

Des mesures de protection et des consignes de sécurité supplémentaires pour les voyages d'affaires à l'étranger figurent dans la brochure Prophylax.

www.src.admin.ch – FR – Documentation et publications – Recherche – Prophylax – Publications

INFORMATIONS COMPLÉMENTAIRES

ESPIONNAGE ET PROLIFÉRATION

Programme de sensibilisation Prophylax

www.src.admin.ch – FR – Sécurité – Recherche de renseignements – Espionnage économique

Le programme de sensibilisation Prophylax a pour but de protéger la place industrielle et de recherche suisse de fuites involontaires de données et d'efforts déployés pour acquérir illégalement des biens. Avec Prophylax, le SRC sensibilise des entreprises, hautes écoles et instituts de recherche aux menaces et risques qui émanent de l'espionnage et de la prolifération (dissémination d'armes de destruction massive et de leurs vecteurs ainsi que des biens à double usage).

Court-métrage « En ligne de mire »

www.src.admin.ch – FR – Sécurité – Recherche de renseignements – Espionnage économique

Le court-métrage « En ligne de mire » s'inscrit dans le programme de sensibilisation Prophylax conduit par le SRC. Le film a pour but de sensibiliser la place industrielle et de recherche suisse aux menaces qui émanent de l'espionnage économique.

Explications des méthodes d'espionnage présentées dans le film et mesures de protections appropriées: *www.src.admin.ch – Espionnage économique - Documents*

Aide-mémoire et fiches d'information complémentaires

www.src.admin.ch – FR – Sécurité – Recherche de renseignements – Espionnage économique – Documents

- Prophylax
- Que fait le SRC pour lutter contre l'espionnage ?
- Aide-mémoire sur l'espionnage économique
- Management Summary Etude « Wirtschaftsspionage in der Schweiz »
- Sécurité de l'information : aide-mémoire pour PME

CYBERSÉCURITÉ

Centre national pour la cybersécurité (National Cyber Security Centre — NCSC)

www.ncsc.admin.ch

Le Centre national pour la cybersécurité (National Cyber Security Centre — NCSC) est le centre de compétences de la Confédération en matière de cybersécurité et le premier interlocuteur pour les milieux économiques, l'administration, les établissements de formation et la population pour toute question relative à la cybersécurité.

Signalement de courriels d'hameçonnage (phishing)

www.antiphishing.ch

antiphishing.ch est géré par le NCSC. Sa fonction est de fournir aux utilisateurs une interface simple pour signaler des tentatives de phishing.

Norme minimale afin d'améliorer la résilience TIC

www.ofae.admin.ch – Thèmes – TIC – Norme minimale pour les TIC

La numérisation, qui avance à grands pas dans tous les domaines de notre vie, représente pour la Suisse un fort potentiel économique et sociétal. Cette numérisation implique néanmoins aussi de nouveaux risques, que nous devons appréhender rapidement et de manière conséquente. Le document « Norme minimale pour améliorer la résilience informatique » de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) sert de soutien et propose des mesures concrètes pour améliorer la résilience des TIC.

ECONOMIE

Prescriptions en matière de contrôle à l'exportation

www.seco.admin.ch – FR – Economie extérieure et Coopération économique – Relations économiques – Contrôles à l'exportation et sanctions – Elic – Internal Compliance Programme-ICP

Cette fiche explique pourquoi les entreprises exportatrices doivent mettre en place un contrôle interne, expose les bases juridiques suisses pertinentes et précise les critères qu'un programme interne de conformité (en anglais ICP : Internal Compliance Programme) doit remplir. Elle se veut être une aide pour établir un programme de contrôle interne ou pour l'optimiser, s'il en existe déjà un.

Demandes concernant les biens à double usage

www.elic.admin.ch

A partir du 1er octobre 2014, toutes les demandes (demandes d'autorisation, demandes préliminaires, etc.) ayant trait aux biens à double usage, au matériel de guerre ou aux biens militaires spécifiques doivent être saisies et traitées par voie électronique, via Elic. Les dossiers papier ne sont plus traités.

Recherche des données de sanctions

www.seco.admin.ch– FR – Economie extérieure et Coopération économique – Relations économiques – Contrôles à l'exportation et sanctions – Sanctions / Embargos – Sanctions de la Suisse – Recherche des destinataires de sanctions

La Confédération peut édicter des mesures de contrainte pour appliquer des sanctions décrétées par l'Organisation des Nations Unies, par l'Organisation pour la sécurité et la coopération en Europe ou par les principaux partenaires commerciaux de la Suisse (art. 1, al. 1 Loi sur les embargos), et qui visent à faire respecter le droit international public, notamment les droits de l'homme.

La banque de données SESAM permet la recherche de personnes, entreprises et entités sanctionnées.

AUTRES

Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI)

www.sefri.admin.ch

Le Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI, au sein du Département fédéral de l'économie, de la formation et de la recherche DEFR, est le centre de compétences de la Confédération pour les questions de portée nationale ou internationale relevant de la politique de formation, de recherche et d'innovation.

Séjour à l'étranger

www.dfae.admin.ch – FR– Conseils pour les voyages et représentations– Recommandations générales pour tous les voyages– Conseils aux voyageurs en bref

Les Conseils aux voyageurs fournis par le Département fédéral des affaires étrangères (DFAE) donnent des informations sur la situation sécuritaire à l'étranger. Ils viennent compléter d'autres sources. Chaque personne est seule responsable de la préparation et de l'organisation de son voyage.

Recherche biologique, potentiel d'abus et biosûreté

Académie suisse des sciences naturelles (SCNAT)
www.sciencesnaturelles.ch

Recherche biologique, potentiel d'abus et biosûret (swiss academies reports Vol 12 No 3, 2017) est une base de discussion à la question du risque de double usage des résultats de la recherche biologique.

PROCÉDURE EN CAS DE SOUPÇON / CONTACT

En cas de soupçon d'espionnage ou d'activités de prolifération (par exemple demandes de collaboration douteuses ou comportement suspect de la part de doctorants, étudiants, professeurs, scientifiques), n'hésitez pas à prendre contact avec vos responsables de la sécurité, votre police cantonale ou le SRC. Conservez les preuves potentielles et ne supprimez pas les courriels suspects. Le SRC récoltera et analysera les indices. Il garantit un traitement discret de l'affaire.

Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne

www.src.admin.ch
prophylax@ndb.admin.ch

En collaboration avec les services de renseignement cantonaux, le SRC informe, sensibilise et conseille les universités, hautes écoles, entreprises et instituts de recherche suisses et liechtensteinois en matière de prolifération et d'espionnage.

Droits d’image

Page de titre, FHNW Campus Muttenz, © Gataric Fotografie

Page 2, UNIGE, © Righetti Nicolas

Page 4, Lichthof UZH, © Meissner Ursula

Page 6, HSLU

Page 10, EPFL, © Christinat Olivier

Page 16, UZH, © Walter Stefan

Page 22, EPFL, © Christinat Olivier

Page 26, UZH, © Bibliothek Rechtswissenschaftliches Institut, © Walter Stefan

TECHNOPOL
Programme de sensibilisation Prophylax
Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne

www.src.admin.ch
prophylax@ndb.admin.ch

Clôture de la rédaction
Décembre 2022