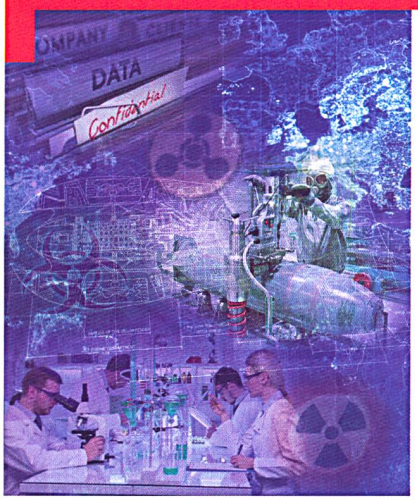
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: 6

Artikel: Prolifération et espionnage économique : des menaces qui touchent aussi les entreprises suisses
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-823414



Le programme Prophylax : sensibilisation à la prolifération et à l'espionnage économique. © Service de renseignement de la Confédération (SRC).

Renseignement

Prolifération et espionnage économique : Des menaces qui touchent aussi les entreprises suisses

Service de renseignement de la Confédération (SRC)

La cyberattaque contre la compagnie suisse Ruag en 2016, la mise sous écoute des pourparlers sur le nucléaire iranien à Genève en 2015 ou encore des agents de renseignement étrangers sous couverture diplomatique – la Suisse se voit régulièrement confrontée à des activités d'espionnage. Dans certains cas, elles sont étroitement liées à des activités de prolifération. Les biens de haute technologie et le savoir-faire suisses sont reconnus à travers le monde. Ils attirent non seulement l'intérêt des entreprises concurrentes, mais aussi celui des acteurs étatiques étrangers, tels que des pays à risques, qui essayent de contourner les mesures de contrôle à l'exportation mises en place par la communauté internationale.

La Suisse, avec son industrie de haute technologie, est une cible attrayante pour des acteurs étrangers, tels que des services de renseignement. Ils recherchent illégalement des informations et technologies sensibles ou des biens contrôlés afin de soutenir le développement technologique de leur pays et de favoriser leur propre industrie ou leurs programmes de développement d'armes de destruction massive. Pour beaucoup de services de renseignement étrangers, cela fait partie intégrante de leurs tâches. Suite à la digitalisation, l'accès illégal à des informations ou données confidentielles ne s'effectue plus seulement par des méthodes d'espionnage classiques, mais de plus en plus aussi par des moyens relevant du domaine des technologies de l'information et de la communication (cyberespionnage). Les conséquences pour une entreprise victime d'espionnage ne sont pas négligeables : pertes financières, perte de parts de marché, atteinte à la réputation, etc.

Créé en 2004, le programme de prévention et de sensibilisation Prophylax du Service de renseignement de la Confédération (SRC) a pour but d'informer et de sensibiliser les entreprises, les hautes écoles et les instituts de recherche suisses sur les menaces émanant de la prolifération[1] et de l'espionnage économique[2]. Dans le cadre d'une discussion confidentielle sur base volontaire, le SRC, en coopération étroite avec les services de renseignement cantonaux, explique pourquoi et comment les activités de prolifération et d'espionnage peuvent poser un risque pour l'entreprise concernée. Il lui montre également des mesures préventives permettant d'identifier et de se protéger contre de telles activités.

L'exportation de biens à double usage et de technologies critiques est soumise à un contrôle et doit être approuvée par le Secrétariat d'Etat à l'économie (SECO). Des pays à risques, tels que le Pakistan ou l'Iran, dépendent de tels biens ou du savoir-faire nécessaire pour le développement de ces biens afin de faire progresser leurs programmes de développement d'armes de destruction massive. Ils tentent de contourner les contrôles en utilisant différentes méthodes et des réseaux d'acquisition clandestins. Pour les fournisseurs, cela rend difficile l'identification de l'utilisation finale de leur produit. La détection à temps et l'entrave aux efforts d'acquisitions illégales de biens est l'un des buts principaux des entretiens de sensibilisation Prophylax et contribue à l'affermissement du contrôle des exportations de biens (notamment de biens à double usage) et de technologies critiques et afférents à la prolifération.

Les activités d'espionnage et de prolifération sont souvent liées. A travers les contacts de sensibilisation

1 On entend par prolifération d'une part la dissémination d'armes de destruction massive et de leurs vecteurs (missiles balistiques, missiles de croisière et drones) et, d'autre part, des biens d'équipement, matériaux et technologies nécessaires à leur fabrication (biens à double usage).

2 L'espionnage comprend l'ensemble des actions en faveur d'un État, d'une entreprise ou d'une personne dans le but de rechercher des informations protégées ou secrètes dans les domaines militaire, politique, économique, scientifique et technologique au préjudice d'un pays, d'une entreprise ou d'une personne.

Prophylax, le SRC rend les entreprises plus attentives au maniement consciencieux de leurs informations sensibles afin d'empêcher une fuite involontaire d'informations et de données. Les activités d'espionnage mises en œuvre par des acteurs étrangers peuvent p. ex. se produire sous couvert d'une visite de délégation au sein de l'entreprise, d'une participation à des entreprises et à des projets de recherche communs ou encore par les moyens de l'ingénierie sociale (p. ex. hameçonnage ciblé, demandes de contacts par le biais des réseaux sociaux tel que Linkedin, etc.). La mise en place de mesures de sécurité adéquates peut offrir une certaine protection contre une fuite de données involontaire. La première ligne de défense est le comportement de l'individu ; la sensibilisation des employés est donc essentielle. Une attention particulière doit aussi être portée aux voyages d'affaires à l'étranger, p. ex. en n'emportant avec soi que les appareils électroniques et les documents absolument nécessaires et en les gardant toujours avec soi.

Informations et contact :
www.ndb.admin.ch/espionnage-economique pour des informations complémentaires sur l'espionnage économique ainsi que la brochure Prophylax, laquelle contient également des conseils pour les voyages d'affaires à l'étranger. On y trouve aussi le film de sensibilisation « En ligne de mire », qui montre les méthodes d'espionnage employées par des acteurs étrangers pour se procurer un accès à des informations et des données confidentielles.

prophylax@ndb.admin.ch SRC

Ce code QR vous dirigera vers le film « En ligne de mire » du SRC. Celui-ci est disponible en version originale allemande sans sous-titres ou avec des sous-titres en français, italien ou anglais. Des informations plus détaillées sur les méthodes et procédés d'espionnage présentés dans le court-métrage sont disponibles dans le guide correspondant sur la page officiel du SRC

News

Russie : Petite leçon de propagande

Comme l'avait indiqué le défecteur Youri Bezmenov, le renseignement russe est moins académique que ses homologues occidentaux et accorde plus de moyens à l'influence qu'au cumul de renseignements.

Après quelques années de recul, il semble désormais possible de dégager tes raisons de l'efficacité de la nouvelle *Dezinformaizia* russe. La priorité est d'abord d'instrumentaliser et d'alimenter tous les groupes contestataires, des néo-nazis aux islamistes jusqu'aux écologistes, représentant chacun des lignes d'opérations convergeant vers un unique effet final recherché: la diabolisation de l'atlantisme. Pour éviter la contre-information de l'Occident et l'impact de ses valeurs sur l'opinion publique, il est stratégique pour le Kremlin de saturer les médias russophones et les relais informels de thèmes anxiogènes (assassinat des Russes dans les rues de Kiev, attaques contre l'orthodoxie, encerclement par les troupes de l'OTAN).

Désorienter, créer la confusion pour convaincre les masses que rien n'est vrai et que tout est très compliqué, procède du même dessein. Il suffit ensuite de les rassurer, de les unir et de leur permettre de s'identifier derrière l'illusion d'un pouvoir fort et conquérant. D'où la vague de contre-sanctions contre la Pologne et la Turquie, qui ont suivi les sanctions économiques occidentales après la Crimée. C'est la conquête de la première impression de l'opinion publique qui est l'enjeu de toutes les campagnes d'information. Dès les premières manifestations de la place Maidan, les statistiques des titres accrocheurs de l'infosphère russe évoquant le rôle des sympathisants néo-nazis ont explosé.

A l'extérieur, l'adversaire doit être sidéré, démoralisé, paralysé: clichés et vidéos de corps mutilés ont été répandus sur Internet tant lors du conflit en Géorgie qu'en Syrie ou dans le Dombass. Et quand les preuves de la désinformation russe deviennent indiscutables, des campagnes nauséabondes ciblent les témoins pour les discréditer, pour faire endosser à l'adversaire la responsabilité de ses propres actes. Puis de nouveaux événements sont créés de toute pièce, afin de détourner l'attention de l'opinion publique. L'opération la plus magistrale est sans doute celle qui a fait croire à l'attaque terroriste de l'usine chimique de Columbia : dossier de presse auprès des médias occidentaux partenaires, chaînes YouTube, pages sur Wikipédia, fausses acquisitions d'écran sur CNN, fausses interviews, des douzaines de comptes créés pour l'occasion débitant des centaines de tweets par heure ont même ciblé les habitants des agglomérations voisines pour provoquer des mouvements de panique...

TTU No. 1080, 18 octobre 2017.