Fiche 11
Évaluez les risques d'opérations d'influence

Plusieurs États comme la Russie, la Chine[16], utilisent la désinformation comme une cyberarme pour déstabiliser les démocraties. En tant que titulaire de charge publique, vous pourriez être vulnérable à ces opérations d'influence. Il est important que vous soyez en mesure de les repérer, afin de protéger votre institution. Ces dernières sont parfois difficiles à détecter, car elles peuvent prendre la forme de manœuvres diffuses de parties prenantes non gouvernementales, mais certains indices devraient vous mettre la puce à l'oreille…

Points de vigilance au Québec et au Canada

Les activités d'influence étatique. Selon un rapport du Centre canadien pour la cybersécurité évaluant les principales cybermenaces pour 2025-2026, il faut faire preuve de vigilance vis-à-vis des activités de la Chine et de la Russie principalement, ainsi que l'Iran, la Corée du Nord et l'Inde[56]. Ces menaces changent rapidement, notamment à cause de l'évolution des politiques américaines, non encore documentées dans ce rapport.

Les domaines d'activité sensibles. Portez une attention particulière aux investissements étrangers et aux collaborations de recherche et développement pour :

- **L'exploitation de minéraux critiques et stratégiques**[57], comme le graphite, le nickel, le cobalt et les éléments du groupe du platine, le lithium, les terres rares, le titane, le niobium, le zinc et le cuivre;
- **Les technologies considérées comme sensibles**[58] **:** infrastructures numériques, intelligence artificielle et mégadonnées, robotique et systèmes autonomes, technologies aérospatiales, etc. (voir la liste complète dans la section Pour aller plus loin).

Quelques techniques d'ingérence[62]

- élicitation : soutirer des informations;
- relations sociales intéressées;
- coercition : chantage et menaces;
- corruption et financement illégal;
- cyberattaques : via le hameçonnage;
- désinformation sur les médias sociaux.

Pour aller plus loin

Fiche 11
Évaluez les risques d'opérations d'influence

Distinguez l'influence légitime de celle qui ne l'est pas

Il est accepté que des personnes mènent des opérations d'influence auprès des décisionnaires politiques, de manière transparente et avec des moyens légitimes (voies diplomatiques, activités encadrées par Lobbyisme Québec)[59]. Cela devient problématique lorsque des personnes ou des organisations :

- **manquent de transparence.** Affiliations masquées, octroi occulte de financement, actions coercitives sur des individus, etc;
- **ont une intention malveillante.** Volonté d'acquérir un avantage géopolitique, militaire ou stratégique au détriment des intérêts du gouvernement en place.

Toutes sortes d'activités se situent dans une zone grise en matière de légitimité, dans laquelle il convient de faire preuve de vigilance[60], et notamment dans le cyberespace, qui est très peu réglementé.

Posez les bons gestes[62]

- **Mettez à jour vos pratiques de cybersécurité,** par exemple sur la base de la Directive gouvernementale[63] et du *Guide de sensibilisation sur la sécurité de l'information* du gouvernement du Québec.
- **Mettez en place une veille ciblée,** en particulier dans des domaines d'activités sensibles cités plus haut Fiche 10.
- **Assurez-vous de bien connaître vos partenaires,** leurs intentions, leur affiliation étatique et idéologique, etc.
- **Informez votre personnel et vos partenaires** de votre posture et de vos politiques en matière d'opérations d'influence.
- **Signalez toute activité suspecte et tout incident** d'intimidation, de harcèlement, de coercition ou de menace aux autorités de votre institution, au Service canadien du renseignement de sécurité, ou à votre service de police local.
- **Poursuivez et diversifiez des activités diplomatiques saines** dans votre domaine d'activité, notamment les activités de diplomatie scientifique qui permettent de renforcer notre capacité collective à accéder aux données probantes à l'échelle mondiale[64].

Pour aller plus loin