

L'ingérence étrangère dans la Communauté

Comment signaler les menaces et l'intimidation de gouvernements étrangers

FACTSHEET / April 2023

afp.gov.au

Introduction

L'ingérence étrangère représente une grave menace pour les Australiens, la souveraineté et la sécurité du pays, ainsi que pour l'intégrité de nos institutions nationales. Les menaces d'ingérence étrangère ne sont pas limitées à un secteur de la communauté australienne ni perpétrées par un seul État-nation. Des acteurs étatiques étrangers hostiles (des pays qui entreprennent des activités hostiles contre d'autres pays) créent et recherchent des opportunités d'interférer avec les décideurs australiens à tous les niveaux de gouvernement et dans divers secteurs, notamment : les institutions démocratiques ; l'éducation et la recherche ; les médias et communications ; les infrastructures critiques ; et surtout, nos communautés culturellement et linguistiquement diverses (CALD).

L'ingérence étrangère dans la communauté

L'ingérence étrangère dans la communauté est définie comme des menaces et des intimidations dirigées, supervisées ou financées par des gouvernements étrangers et ciblées sur les communautés CALD afin de nuire et d'avoir un impact sur le mode de vie multiculturel de l'Australie. Les gouvernements étrangers peuvent s'immiscer dans les communautés à diverses fins :

- faire taire les critiques des politiques intérieures et extérieures du gouvernement étranger
- pour surveiller les activités (hors ligne et en ligne) des membres des groupes CALD
- promouvoir les opinions et les politiques du gouvernement étranger
- pour obtenir des informations au profit du gouvernement étranger
- pour influencer les points de vue et les opinions de la population en général.

L'ingérence étrangère dans la communauté peut prendre plusieurs formes

Y compris:

- Agression ou menaces d'agression
- Chantage
- Enlèvement, détention illégale ou privation de liberté
- Harcèlement et surveillance physique ou électronique indésirable
- Contrainte d'un individu en menaçant sa famille ou ses associés à l'étranger pour les forcer à se conformer
- Campagnes de désinformation en ligne via les médias sociaux pour discréditer un individu ou un groupe.

Il est important de noter que pour constituer une ingérence étrangère en vertu de la *Loi de 1995 sur le Code criminel* (Cth), l'activité doit être liée à un gouvernement étranger ou à son mandataire. Lors de l'évaluation de la criminalité, les forces de l'ordre peuvent également tenir compte des infractions de l'État ou du territoire australien.

Qui est visé ?

Les gouvernements étrangers peuvent cibler :

- des ressortissants anciens ou actuels résidant en Australie
- des militants politiques et des droits de l'homme
- des dissidents
- des journalistes
- des opposants politiques
- des groupes religieux ou ethniques minoritaires.

Que puis-je faire pour aider ?

Bien que tous les rapports d'ingérence étrangère dans la communauté ne génèrent pas une réponse flagrante de l'AFP, chaque rapport **aide à dresser un tableau** des problèmes émergents.

Toute préoccupation et/ou tout cas d'ingérence étrangère dans la communauté peut être signalé à la **National Security Hotline (NSH)**.

- La NSH fonctionne 24 heures sur 24, 7 jours sur 7 et est le point de contact central pour signaler les préoccupations concernant une éventuelle ingérence étrangère dans la communauté.
- Les opérateurs NSH sauront quoi faire avec les informations que vous fournissez et, le cas échéant, ils les transmettront aux forces de l'ordre et aux agences de sécurité pour évaluation.
- Les opérateurs NSH prennent chaque appel au sérieux et apprécient toutes les informations reçues.
- Nous savons que signaler un sujet de préoccupation peut être une étape importante. Nous prenons votre droit à la vie privée au sérieux. Veuillez indiquer à l'opérateur si vous souhaitez rester anonyme.
- En raison de la nature sensible des informations, vous ne recevrez aucun avis sur le résultat de votre appel ou de votre e-mail.

Les informations que vous fournissez peuvent être la pièce manquante dont l'AFP a besoin pour aider à prévenir l'ingérence étrangère dans la communauté.

Il existe plusieurs manières de contacter la **NSH** :

- Appelez le : 1800 123 400
 - Depuis l'extérieur de l'Australie : (+61) 1300 123 401
 - Pour les utilisateurs TTY (utilisateurs malentendants): 1800 234 889
 - **Si vous avez besoin d'un interprète, veuillez appeler le Service de traduction et d'interprétation au 131 450 et leur demander d'appeler la hotline de la sécurité nationale**
- SMS
 - Veuillez envoyer vos informations par SMS au 0498 562 549

- E-mail
 - Veuillez envoyer vos informations par e-mail à : hotline@nationalecurity.gov.au
- Poste :
 - Veuillez envoyer vos informations à :

National Security Hotline
Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Autres façons de signaler

Vous pouvez également signaler vos préoccupations via une gamme d'autres moyens, le cas échéant.

- eSafety permet de supprimer les contenus en ligne gravement abusifs. Vous pouvez signaler un **abus en ligne grave** au commissaire à la sécurité électronique sur esafety.gov.au/report
- Si vous vous sentez menacé ou en danger de quelque manière que ce soit, vous pouvez contacter :
 - **La police - au 000 pour menaces immédiates**
 - **La police - au 13 14 44 pour la présence de la police lors d'incidents ne mettant pas la vie en danger.**
- Vous pouvez signaler un crime du Commonwealth à l'AFP via un formulaire en ligne "Report a Commonwealth crime" à l'adresse forms.afp.gov.au/online_forms/report_a_crime. Pour plus d'informations sur ce qui constitue un crime de Commonwealth, veuillez consulter afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime.
- Tout membre de la communauté peut signaler des soupçons d'espionnage ou d'ingérence étrangère en s'adressant directement à un membre de l'AFP (y compris l'équipe de liaison communautaire de l'AFP).

À quoi puis-je m'attendre en signalant une ingérence étrangère dans la communauté ?

L'AFP ne peut pas enquêter sur chaque signalement d'ingérence étrangère dans la communauté. Chaque appel à la NSH ou signalement d'un crime est évalué au cas par cas pour déterminer si une infraction pénale est identifiée. Les résultats de la rédaction d'un rapport comprennent :

- il se peut qu'il n'y ait pas de réponse parce que l'affaire n'atteint pas un seuil législatif pour que la police prenne des mesures
- l'AFP peut enquêter
- un autre service de police ou un organisme gouvernemental peut s'occuper de l'affaire.

Pour les infractions commises en dehors de l'Australie, des limites juridictionnelles s'appliquent.

Types de menaces

Si vous êtes menacé en personne

- Notez ou enregistrez la menace exactement telle qu'elle a été communiquée.
- Enregistrez autant de détails descriptifs sur la personne qui a proféré la menace (nom, sexe, taille, poids, couleur des cheveux et des yeux, voix, vêtements ou tout autre trait distinctif).
- Signalez la menace à la police.

Si vous êtes menacé au téléphone

- Si possible, faites signe à d'autres personnes à proximité pour écouter et avertir la police.
- Enregistrez l'appel si possible.
- Notez le libellé exact de la menace.
- Copiez toute information de l'affichage électronique du téléphone.
- Soyez disponible pour discuter des détails avec la police.

Si vous êtes menacé par des moyens électroniques, y compris par SMS, message direct/privé, réseaux sociaux ou e-mail

- Ne supprimez pas les messages.
- Imprimez, photographiez, faites une capture d'écran ou copiez les informations du message (objet, date, heure, expéditeur, etc.). Assurez-vous d'enregistrer ou de prendre une capture d'écran des messages conçus pour être temporaires.
- Informez immédiatement la police que vous avez reçu une menace.
- Conservez toutes les preuves électroniques.

Pour vous protéger de ces types de menaces, suivez ces conseils:

- N'ouvrez pas les messages électroniques ou les pièces jointes d'expéditeurs inconnus
- Ne communiquez pas sur les réseaux sociaux avec des personnes inconnues ou non sollicitées
- Assurez-vous que les paramètres de sécurité de vos appareils/comptes sont réglés au niveau de protection le plus élevé
- Les cybercriminels peuvent compromettre vos appareils électroniques et révéler des informations personnelles
- Contactez immédiatement vos institutions financières pour protéger vos comptes contre le vol d'identité
- Utilisez des phrases secrètes fortes et n'utilisez pas la même phrase secrète pour plusieurs sites Web.
- Assurez-vous que les applications antivirus et anti-programmes malveillants sont à jour
- Appliquez les mises à jour système et logicielles au besoin
- Appliquez l'authentification à deux facteurs
- Sauvegardez régulièrement vos données
- Sécurisez votre appareil mobile
- Développez votre réflexion et votre sensibilisation à la cybersécurité
- Pour plus d'informations, visitez cyber.gov.au .