

Can thiệp Nước ngoài vào Cộng đồng

Làm thế nào để báo cáo các mối đe dọa và dọa nạt từ chính phủ nước ngoài

FACTSHEET / March 2023

afp.gov.au

Giới thiệu

Sự can thiệp của nước ngoài thể hiện mối đe dọa nghiêm trọng đối với người dân, chủ quyền và an ninh của nước Úc và sự toàn vẹn của các thể chế quốc gia của chúng ta. Những mối đe dọa từ sự can thiệp của nước ngoài không chỉ giới hạn ở một khu vực của cộng đồng Úc cũng như không do một quốc gia duy nhất gây ra. Các chủ thể thù địch của nhà nước nước ngoài (các quốc gia thực hiện hoạt động thù địch để chống lại các quốc gia khác) đang tạo ra và theo đuổi những cơ hội để can thiệp vào những người ra quyết định của nước Úc ở tất cả các cấp chính quyền và trên nhiều lĩnh vực, bao gồm: các thể chế dân chủ; giáo dục và nghiên cứu; truyền thông và thông tin liên lạc; cơ sở hạ tầng quan trọng; và quan trọng là các cộng đồng đa dạng về văn hóa và ngôn ngữ (CALD) của chúng ta.

Sự can thiệp của nước ngoài về cộng đồng

Sự can thiệp của nước ngoài vào cộng đồng được định nghĩa là sự dọa nạt và đe dọa do các chính phủ nước ngoài chỉ đạo, giám sát hoặc tài trợ và nhắm vào các cộng đồng CALD để nhằm làm tổn hại và tác động đến lối sống đa văn hóa của Úc. Chính phủ nước ngoài có thể can thiệp vào các cộng đồng vì nhiều mục đích khác nhau:

- để dập tắt sự chỉ trích về chính sách đối nội và đối ngoại của chính phủ nước ngoài
- để giám sát các hoạt động (ngoại tuyến và trực tuyến) của các thành viên của các nhóm CALD
- để thúc đẩy quan điểm và chính sách của chính phủ nước ngoài
- để lấy được thông tin cho lợi ích của chính phủ nước ngoài
- để ảnh hưởng đến quan điểm và ý kiến của dân số rộng lớn hơn

Sự can thiệp nước ngoài vào cộng đồng có thể dưới nhiều hình thức

Bao gồm:

- Hành hung hoặc đe dọa hành hung
- Tống tiền
- Bắt cóc, giam giữ bất hợp pháp hoặc tước đoạt quyền tự do
- Rình rập và giám sát vật lý hoặc điện tử không mong muốn
- Ép buộc một cá nhân bằng cách đe dọa gia đình hoặc những người cộng sự của họ ở nước ngoài để buộc họ phải tuân theo

- Các chiến dịch thông tin sai lệch trực tuyến thông qua phương tiện truyền thông xã hội để hạ uy tín của một cá nhân hoặc tập thể.

Quan trọng là, để cấu thành sự can thiệp của nước ngoài theo Đạo luật Bộ luật Hình sự 1995 (Cth), hoạt động này phải được liên kết với một chính phủ nước ngoài hoặc người đại diện của chính phủ đó. Khi đánh giá tội phạm, các cơ quan hành pháp cũng có thể xem xét các hành vi phạm tội của Tiểu bang hoặc Lãnh thổ Úc.

Mục tiêu là ai?

Các chính phủ nước ngoài có thể nhắm đến:

- Cựu công dân hoặc công dân hiện tại cư trú tại Úc
- Các nhà hoạt động chính trị và nhân quyền
- Những người bất đồng chính kiến
- Các nhà báo
- Các đối thủ chính trị
- Các nhóm tôn giáo hoặc dân tộc thiểu số.

Tôi có thể làm gì để giúp đỡ?

Mặc dù không phải tất cả các báo cáo về sự can thiệp của nước ngoài vào cộng đồng cũng tạo ra phản hồi rõ ràng từ AFP, nhưng mỗi báo cáo **giúp xây dựng bức tranh** của các vấn đề mới nổi.

Mọi lo ngại và/hoặc trường hợp can thiệp của nước ngoài vào cộng đồng có thể được báo cáo cho **National Security Hotline (NSH - Đường dây nóng An ninh Quốc gia)**.

- NSH hoạt động 24 giờ mỗi ngày, 7 ngày một tuần và là đầu mối liên hệ trung tâm để báo cáo những lo ngại về khả năng can thiệp của nước ngoài vào cộng đồng.
- Những điều hành viên của NSH sẽ biết phải làm gì với những thông tin mà quý vị cung cấp và khi thích hợp, họ sẽ chuyển thông tin đó cho các cơ quan hành pháp và an ninh để đánh giá.
- Các điều hành viên của NSH nhận từng cuộc gọi một cách nghiêm túc và xem trọng tất cả những thông tin nhận được.
- Chúng tôi biết rằng việc báo cáo một vấn đề đáng lo ngại có thể là một bước tiến lớn. Chúng tôi xem trọng quyền riêng tư của quý vị. Xin vui lòng nói cho điều hành viên biết nếu quý vị muốn ẩn danh.
- Do tính chất nhạy cảm của thông tin, quý vị sẽ không nhận được lời khuyên về kết quả cuộc gọi hoặc thư điện tử (email) của mình.

Thông tin quý vị cung cấp có thể là mảnh ghép còn thiếu mà AFP cần để giúp ngăn chặn sự can thiệp của nước ngoài vào cộng đồng.

Có một vài cách để liên lạc với **NSH**:

- **Gọi: 1800 123 400**
 - Từ bên ngoài nước Úc: (+61) 1300 123 401

- Đối với người dùng TTY (người dùng khiếm thính): 1800 234 889
- **Nếu quý vị cần thông dịch viên, vui lòng gọi Dịch vụ Biên Phiên dịch qua số 131 450 và yêu cầu họ gọi cho Đường dây nóng An ninh Quốc gia**
- **SMS (Tin nhắn)**
 - Vui lòng gửi thông tin của quý vị qua tin nhắn đến số 0498 562 549
- **Email (thư điện tử)**
 - Vui lòng gửi thông tin của quý vị qua email tới: hotline@nationalsecurity.gov.au
- **Bưu điện:**
 - Vui lòng gửi thông tin của quý vị đến
National Security Hotline
Department of Home Affairs
PO Box 25
Belconnen ACT 2.616

Các cách khác để báo cáo

Quý vị cũng có thể báo cáo mối lo ngại của mình thông qua một loạt các phương tiện khác khi phù hợp.

- eSafety giúp loại bỏ nội dung trực tuyến lạm dụng nghiêm trọng Quý vị có thể báo cáo lạm dụng trực tuyến nghiêm trọng cho eSafety Commissioner (Ủy viên An toàn Điện tử) tại esafety.gov.au/report.
- Nếu quý vị cảm thấy **bị đe dọa và bất an** theo bất kỳ cách nào, quý vị có thể liên lạc:
 - **Cảnh sát - qua số 000 đối với các mối đe dọa tức thời**
 - **Cảnh sát - qua số 13 14 44 để cảnh sát có mặt tại các sự cố không đe dọa đến tính mạng.**
- Quý vị có thể báo cáo tội phạm Khó tính vướng chung cho AFP thông qua biểu mẫu Báo cáo tội phạm Khó tính vướng chung trực tuyến tại forms.afp.gov.au/online_forms/report_a_crime. Để biết thêm thông tin về những gì cấu thành Tội phạm Liên bang, vui lòng xem afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime.
- Bất kỳ thành viên nào của cộng đồng đều có thể báo cáo các hoạt động bị nghi ngờ là gián điệp hoặc can thiệp nước ngoài bằng cách nói chuyện trực tiếp với một thành viên của AFP (bao gồm cả Nhóm liên lạc cộng đồng của AFP).

Tôi có thể mong đợi điều gì khi báo cáo sự can thiệp của nước ngoài vào cộng đồng?

AFP không thể điều tra mọi báo cáo về sự can thiệp của nước ngoài vào cộng đồng. Mỗi cuộc gọi đến NSH hoặc báo cáo tội phạm được đánh giá trên cơ sở từng trường hợp để xác định xem có bất kỳ hành vi phạm tội nào được xác định hay không. Kết quả của việc lập báo cáo bao gồm:

- có thể không có phản hồi vì vấn đề không đáp ứng ngưỡng lập pháp để cảnh sát hành động
- AFP có thể điều tra
- một cơ quan cảnh sát hoặc cơ quan chính phủ khác có thể giải quyết vấn đề.

Đối với các hành vi phạm tội xảy ra bên ngoài nước Úc, các giới hạn về thẩm quyền sẽ được áp dụng.

Các loại đe dọa

Nếu quý vị bị đe dọa trực tiếp

- Viết xuống hoặc ghi lại mỗi đe dọa chính xác như nó đã được truyền đạt
- Ghi lại càng nhiều chi tiết mô tả càng tốt về người đã đe dọa (tên, giới tính, chiều cao, cân nặng, tóc và màu mắt, giọng nói, quần áo hoặc bất kỳ đặc điểm nhận dạng nào khác).
- Báo cáo mỗi đe dọa cho cảnh sát.

Nếu quý vị bị đe dọa qua điện thoại

- Nếu có thể, hãy báo hiệu cho những người khác gần đó lắng nghe và thông báo cho cảnh sát.
- Ghi âm cuộc gọi nếu có thể.
- Viết ra từ ngữ chính xác của mỗi đe dọa.
- Sao chép bất kỳ thông tin nào từ màn hình điện tử của điện thoại.
- Sẵn sàng thảo luận chi tiết với cảnh sát.

Nếu quý vị bị đe dọa qua các phương tiện điện tử bao gồm qua tin nhắn văn bản, tin nhắn trực tiếp/riêng tư, mạng xã hội hoặc email

- Đừng xóa các tin nhắn.
- In, chụp ảnh, chụp màn hình hoặc sao chép thông tin tin nhắn (dòng chủ đề, ngày, giờ, người gửi, v.v.). Đảm bảo lưu hoặc chụp ảnh màn hình các tin nhắn được thiết kế tạm thời.
- Thông báo ngay cho cảnh sát rằng quý vị đã nhận được một lời đe dọa.
- Bảo quản tất cả bằng chứng điện tử.

Để bảo vệ quý vị khỏi các loại mối đe dọa này, hãy làm theo những gợi ý sau:

- Không mở tin nhắn điện tử hoặc tệp đính kèm từ những người gửi mình không biết
- Không giao tiếp trên phương tiện truyền thông xã hội với các cá nhân không biết hoặc không mong muốn
- Đảm bảo cài đặt bảo mật trên thiết bị/tài khoản của quý vị được đặt ở mức bảo vệ cao nhất
- Tội phạm mạng có thể xâm phạm các thiết bị điện tử của quý vị và tiết lộ thông tin cá nhân
- Liên hệ ngay với các tổ chức tài chính của quý vị để bảo vệ tài khoản của quý vị khỏi hành vi trộm cắp danh tính
- Sử dụng cụm mật khẩu mạnh và không sử dụng cùng một cụm mật khẩu cho nhiều trang mạng
- Đảm bảo các ứng dụng chống vi-rút và chống phần mềm độc hại được cập nhật
- Áp dụng các bản cập nhật hệ thống và phần mềm theo yêu cầu
- Áp dụng việc xác thực hai yếu tố
- Sao lưu dữ liệu thường xuyên
- Bảo mật thiết bị di động của quý vị
- Phát triển tư duy và nhận thức về An toàn mạng của quý vị
- Để biết thêm thông tin, hãy truy cập cyber.gov.au.