

مداخله خارجی در جامعه

نحوه گزارش تهدید و ارباب از سوی دولت های خارجی

FACTSHEET / April 2023

afp.gov.au

مقدمه

مداخله خارجی تهدیدی جدی برای مردم استرالیا، حاکمیت و امنیت و یکپارچگی نهادهای ملی ما است. تهدیدهای مداخله خارجی به یک بخش از جامعه استرالیا محدود نمی شود و توسط فقط یک دولت-ملت واحد انجام نمی شود. بازیگران دولت های خارجی متخاصم (کشورهایی که فعالیت های خصمانه علیه سایر کشورها انجام می دهند) در حال ایجاد و پیگیری فرصت هایی برای مداخله در کار تصمیم گیرندگان استرالیایی در تمام سطوح دولتی و در طیف وسیعی از بخش ها هستند، از جمله: نهادهای دموکراتیک. آموزش و پژوهش؛ رسانه و ارتباطات؛ زیرساخت های حیاتی؛ و مهمتر از همه، جوامع متنوع فرهنگی و زبانی ما (CALD).

مداخله خارجی در جامعه

مداخله خارجی در جامعه به عنوان تهدید و اربابی تعریف می شود که توسط دولت های خارجی هدایت، نظارت یا تأمین مالی می شود و جوامع CALD را هدف قرار می دهد تا آسیب و تأثیری بر شیوه زندگی چندفرهنگی استرالیا وارد کند. دولت های خارجی ممکن است برای اهداف مختلفی در جوامع مداخله کنند:

- ساکت کردن انتقاد از سیاست های داخلی و خارجی دولت خارجی
- برای نظارت بر فعالیت های (آفلاین و آنلاین) اعضای گروه های CALD
- ترویج دیدگاه ها و سیاست های دولت خارجی
- به دست آوردن اطلاعات به نفع دولت خارجی
- تأثیر گذاشتن بر دیدگاه ها و نظرات جمعیت وسیع تر.

مداخله خارجی در جامعه می تواند شکل های متعددی داشته باشد

از جمله:

- حمله یا تهدید به حمله
- باج گیری
- آدم ربایی، بازداشت غیرقانونی یا سلب آزادی
- تعقیب و نظارت فیزیکی یا الکترونیکی ناخواسته
- اجبار یک فرد با تهدید خانواده یا اطرافیان خود در خارج از کشور برای مجبور کردن آنها به پیروی کردن
- کمپین های اطلاعات نادرست آنلاین از طریق رسانه های اجتماعی برای بی اعتبار کردن یک فرد یا گروه.

نکته مهم، برای ایجاد مداخله خارجی بر اساس *قانون جزایی 1995 (Cth)*، این فعالیت باید به یک دولت خارجی یا نماینده آن مرتبط باشد. در ارزیابی جرم، سازمان های مجری قانون ممکن است جرایم ایالت یا قلمرو استرالیا را نیز در نظر بگیرند.

چه کسی هدف قرار گرفته می شود؟

دولت های خارجی ممکن است افراد زیر را هدف قرار دهند:

- اتباع سابق یا فعلی مقیم استرالیا
- فعالان سیاسی و حقوق بشر
- دگراندیشان
- خبرنگاران
- مخالفان سیاسی
- گروه های اقلیت مذهبی یا قومی.

من برای کمک چه کاری می توانم انجام دهم؟

در حالی که همه گزارش های مداخله خارجی در جامعه پاسخ آشکار AFP را ایجاد نمی کنند، هر گزارش به ایجاد تصویری از مسائل نوظهور کمک می کند.

هرگونه نگرانی و/یا موارد مداخله خارجی در جامعه را می توان به خط تلفن امنیت ملی (NSH) گزارش کرد.

- NHS به صورت ۲۴ ساعته و ۷ روز هفته کار می کند و نقطه تماس مرکزی برای گزارش نگرانی ها در مورد دخالت احتمالی خارجی در جامعه است.
- اپراتورهای NSH می دانند با اطلاعاتی که ارائه می دهید چه کنند، و در صورت لزوم، آن ها را برای ارزیابی در اختیار سازمان های مجری قانون و امنیتی قرار می دهند.
- اپراتورهای NSH هر تماس را جدی می گیرند و برای تمام اطلاعات دریافتی ارزش قائل هستند.
- ما می دانیم که گزارش یک موضوع نگران کننده می تواند گام بزرگی باشد. ما حق شما برای حفظ حریم خصوصی را جدی می گیریم. اگر می خواهید ناشناس بمانید، لطفاً به اپراتور بگویید.
- به دلیل ماهیت حساس اطلاعات، در مورد نتیجه تماس یا ایمیل خود مشاوره دریافت نخواهید کرد.

اطلاعاتی که ارائه می کنید ممکن است قطعه گم شده ای باشد که AFP برای کمک به جلوگیری از مداخله خارجی در جامعه به آن نیاز دارد.

چندین راه برای تماس با NSH وجود دارد:

- تماس بگیرید: **1800 123 400**
 - از خارج از استرالیا: 1300 123 401 (+61)
 - برای کاربران TTY (کاربران کم شنوا): 1800 234 889
 - اگر به مترجم نیاز دارید، لطفاً با سرویس ترجمه کتبی و شفاهی به شماره 131450 تماس بگیرید و از آنها بخواهید با خط تلفن امنیت ملی تماس بگیرند.

- پیامک
- لطفاً اطلاعات خود را از طریق پیامک به 0498 562 549 ارسال کنید.
- ایمیل:
- لطفاً اطلاعات خود را از طریق ایمیل به این آدرس بفرستید: hotline@nationalecurity.gov.au
- پست
- اطلاعات خود را به آدرس زیر پست کنید:

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

سایر راه های گزارش دادن

- در صورت لزوم همچنین می توانید نگرانی های خود را از طریق طیف وسیعی از روش های دیگر گزارش دهید.
- eSafety به حذف محتوای آنلاین توهین آمیز جدی کمک می کند. شما می توانید سوء استفاده آنلاین جدی را به کمیسیون امنیت eSafety در esafety.gov.au/report گزارش دهید.
 - اگر به هر نحوی احساس خطر یا ناامنی می کنید، می توانید از طریق زیر تماس بگیرید:
 - پلیس - از طریق شماره تلفن 000 برای تهدیدهای فوری
 - پلیس - از طریق شماره تلفن 131444 برای حضور پلیس در حوادث غیرتهدید کننده جان.
 - می توانید یک جرم کامنولت را از طریق فرم آنلاین گزارش جرم کامنولت در forms.afp.gov.au/online-forms/report-a-crime به AFP گزارش دهید. برای اطلاعات بیشتر در مورد اینکه چه چیزی یک جرم کامنولت است، لطفاً به afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime مراجعه کنید.
 - هر عضوی از جامعه می تواند فعالیت های مشکوک به جاسوسی یا مداخله خارجی را با صحبت مستقیم با یکی از اعضای AFP (از جمله تیم ارتباطی با جامعه AFP) گزارش کند.

با گزارش مداخله خارجی در جامعه چه انتظاری می توانم داشته باشم؟

- AFP نمی تواند هر گزارشی از مداخله خارجی در جامعه را بررسی کند. هر تماس با NSH یا گزارش جرم بر اساس مورد به مورد ارزیابی می شود تا مشخص شود آیا جرم جنایی شناسایی شده است یا خیر. نتایج ارائه یک گزارش عبارتند از:
- ممکن است پاسخی داده نشود زیرا این موضوع از آستانه قانونی برای اقدام پلیس برخوردار نیست
 - AFP ممکن است تحقیق کند
 - یکی از سرویس های دیگر پلیس یا یک آژانس دولتی ممکن است به این موضوع رسیدگی کند.
- در مورد جرائمی که در خارج از استرالیا رخ می دهد، محدودیت های قضایی صدق می کند.

انواع تهدید

اگر به صورت حضوری تهدید می شوید

- تهدید را دقیقاً همانطور که اطلاع داده شده است بنویسید یا ثبت کنید.
- تعداد زیادی جزئیات توصیفی درباره فردی که تهدید کرده است (نام، جنسیت، قد، وزن، رنگ مو و چشم، صدا، لباس، یا هر ویژگی متمایز دیگری) ثبت کنید.
- تهدید را به پلیس گزارش دهید.

اگر از طریق تلفن تهدید می شوید

- در صورت امکان، به دیگران در نزدیکی خود علامت دهید تا گوش کنند و به پلیس اطلاع دهند.
- در صورت امکان تماس را ضبط کنید.
- عبارت دقیق تهدید را بنویسید.
- هر گونه اطلاعات را از صفحه نمایش الکترونیکی گوشی کپی کنید.
- برای گفتگو در مورد جزئیات با پلیس در دسترس باشید.

اگر از طریق وسایل الکترونیکی از جمله پیام متنی، پیام مستقیم/خصوصی، رسانه های اجتماعی یا ایمیل تهدید می شوید

- پیام ها را حذف نکنید.
- اطلاعات پیام (خط موضوع، تاریخ، زمان، فرستنده و غیره) را چاپ، عکس، اسکرین شات، یا کپی کنید. مطمئن شوید که پیام هایی را که به صورت موقت طراحی شده اند ذخیره کرده یا از آن عکس بگیرید.
- فوراً به پلیس اطلاع دهید که تهدیدی دریافت کرده اید.
- تمام شواهد الکترونیکی را حفظ کنید.

برای محافظت از خود در برابر این نوع تهدیدات، نکات زیر را دنبال کنید:

- پیام های الکترونیکی یا پیوست های فرستنده ناشناس را باز نکنید
- در شبکه های اجتماعی با افراد ناشناس یا ناخواسته ارتباط برقرار نکنید
- مطمئن شوید که تنظیمات امنیتی شما در دستگاه ها/حساب های تان روی بالاترین سطح حفاظت تنظیم شده است
- مجرمین سایبری می توانند دستگاه های الکترونیکی شما را به خطر بیندازند و اطلاعات شخصی را افشا کنند
- فوراً با مؤسسات مالی خود تماس بگیرید تا از حساب های خود در برابر سرقت هویت محافظت کنید
- از عبارات عبور قوی استفاده کنید و از یک عبارت عبور برای چندین وب سایت استفاده نکنید
- از به روز بودن برنامه های ضد ویروس و ضد بدافزار اطمینان حاصل کنید
- در صورت نیاز به روز رسانی سیستم و نرم افزار را اعمال کنید
- احراز هویت دو مرحله ای را اعمال کنید
- به طور منظم از داده ها پشتیبان تهیه کنید
- دستگاه تلفن همراه خود را ایمن کنید
- تفکر و آگاهی امنیت سایبری خود را توسعه دهید
- برای اطلاعات بیشتر، به cyber.gov.au مراجعه کنید.