

समुदायमा हुने विदेशी हस्तक्षेप

विदेशी सरकारहरुबाट दिइने धम्कीहरु र तर्साउने कार्यलाई कसरी रिपोर्ट गर्ने

FACTSHEET / March 2023

afp.gov.au

परिचय

विदेशी हस्तक्षेपमा अष्ट्रेलियाका मानिसहरु, सार्वभौमसत्ता र सुरक्षा, र हाम्रा राष्ट्रिय संस्थाहरुका अखण्डता प्रति हुने गम्भीर धम्की पर्दछ। विदेशी हस्तक्षेपका धम्कीहरु अष्ट्रेलियाली समुदायको केवल एक क्षेत्रमा सीमित छैनन्, न त कुनै एक्लो राष्ट्रले मात्र त्यस्ता अपराध गरेको छन्। शत्रुतापूर्ण सम्बन्ध रहेको विदेशी राष्ट्रको पात्रहरु (त्यस्ता देशहरु जसले अन्य देशहरु विरुद्ध शत्रुतापूर्ण कृयाकलाप गर्छन्) ले अष्ट्रेलियाली निर्णयकर्ताहरुसङ्ग सरकारका सबै तहहरुमा, र प्रजातान्त्रिक संस्थाहरु; शिक्षा र अनुसन्धान; मिडिया र सञ्चार; महत्वपूर्ण पूर्वाधार; र महत्वपूर्णरूपमा, हाम्रा सांस्कृतिक र भाषिकरूपले विविध समुदायहरु लगायत विभिन्न क्षेत्रहरुमा हस्तक्षेप गर्ने अवसरहरु सृजना गरिरहेका र प्राप्त गर्न प्रयत्न गरिरहेका छन्।

समुदायमा हुने विदेशी हस्तक्षेप

समुदायमा हुने विदेशी हस्तक्षेपलाई अष्ट्रेलियाको बहुसाँस्कृतिक जीवनशैलीमा हानी र प्रभाव पार्नको लागि सांस्कृतिक र भाषिकरूपले विविध समुदायहरुलाई लक्षित गरी विदेशी सरकारहरुद्वारा निर्देशित, सुपरिवेक्षित वा आर्थिक सहयोगमा गरिएको धम्किहरु र तर्साउने कार्य भनी परिभाषित गरिएको छ। विभिन्न प्रयोजनहरुका लागि विदेशी सरकारहरुले समुदायमा हस्तक्षेप गर्न सक्छ:

- विदेशी सरकारको आन्तरिक र बाह्य नीतिहरुको आलोचनालाई दबाउन
- सांस्कृतिक र भाषिकरूपले विविध समुदायहरुका सदस्यहरुका कृयाकलापहरु (अफलाइन र अनलाइन) को अनुगमन गर्न
- विदेशी सरकारको दृष्टिकोण र नीतिहरुको प्रबर्द्धन गर्न
- विदेशी सरकारको फाइदाको लागि जानकारी प्राप्त गर्न
- फैलिएको जनसंख्याको दृष्टिकोणहरु र विचारहरुलाई प्रभाव पार्न।

समुदायमा हुने विदेशी हस्तक्षेपले धेरै स्वरूपहरु लिन सक्छ

निम्न लगायत समावेश छ:

- आक्रमण (Assault) वा आक्रमणको धम्कीहरु
- धम्किद्वारा पैसा वा अन्य चीजको माग गर्नु (Blackmail)
- अपहरण, गैरकानूनीरूपमा थुनु वा स्वतन्त्रताबाट बञ्चित गर्नु
- पिछा गर्ने (Stalking) र नचाहिदो रूपमा भौतिक वा विद्युतिय निगरानी गर्ने
- कुनै व्यक्तिको परिवारलाई धम्की दिएर वा विदेशमा रहेका उनीहरुका सम्बन्धित व्यक्तिहरुलाई पालना गराउन दबाव दिएर त्यस व्यक्तिलाई बाध्य पार्ने

- एक व्यक्ति वा समूहलाई बदनाम गर्न सामाजिक सञ्जाल मार्फत अनलाइन गलत जानकारी अभियानहरू।

महत्वपूर्णरूपमा, क्रिमिनल कोड एक्ट १९९५ (Criminal Code Act 1995 - Cth) अन्तर्गत विदेशी हस्तक्षेप स्थापित हुन, त्यस्तो कृयाकलाप विदेशी सरकार वा त्यसको प्रतिनिधिसङ्घ जोडिएको हुनै पर्छ। आपराधिकतालाई मुल्याङ्कन गर्दा, कानून कार्यान्वयन एजेन्सीहरूले अष्ट्रेलियाली स्टेट वा टेरिटरि अपराधहरूलाई पनि विचार गर्न सक्छ।

को लक्षित हो?

विदेशी सरकारहरूले निम्नलाई तारो बनाउन सक्छन्:

- अष्ट्रेलियामा बसिरहेका भूतपूर्व वा हालका नागरिकहरू
- राजनीतिक र मानव अधिकारका कार्यकर्ताहरू
- असहमतहरू
- पत्रकारहरू
- राजनीतिक विरोधीहरू
- धार्मिक वा जातिय अल्पसंख्यक समूहहरू।

सहयोग गर्न मैले के गर्न सक्छु?

समुदायमा हुने हस्तक्षेपको सबै रिपोर्टहरूले अष्ट्रेलियाली संघीय प्रहरीको स्पष्ट ध्यान नताने पनि, प्रत्येक रिपोर्टले उदय भइरहेका मुद्दाहरूका **स्वरूप विकास गर्नमा सहयोग गर्छ**।

कुनै चासोहरू र/वा समुदायमा हुने विदेशी हस्तक्षेपका उदाहरणलाई **राष्ट्रिय सुरक्षा हटलाइन (NSH)** मा रिपोर्ट गर्न सकिन्छ।

- राष्ट्रिय सुरक्षा हटलाइन दिनको २४ घण्टै, हप्ताको ७ दिनै चालु हुन्छ र संभावित समुदायमा हुने विदेशी हस्तक्षेप बारे चासोहरू रिपोर्ट गर्नको लागि सम्पर्क गर्ने केन्द्रिय स्थान हो।
- तपाईंले प्रदान गर्नु हुने जानकारीलाई के गर्ने भनी राष्ट्रिय सुरक्षा हटलाइन अपरेटरहरूलाई थाहा हुन्छ, र जहाँ उपयुक्त हुन्छ, मुल्याङ्कनको लागि उनीहरूले कानून कार्यान्वयन र सुरक्षा एजेन्सीहरूलाई सो जानकारी उपलब्ध गराउने छन्।
- राष्ट्रिय सुरक्षा हटलाइन अपरेटरहरूले फोनबाट प्राप्त गर्ने प्रत्येक जानकारीलाई गम्भीररूपमा लिन्छन् र सबै प्राप्त भएको जानकारीलाई महत्व दिन्छन्।
- हामीलाई थाहा छ कि चासोको विषय रिपोर्ट गर्नु एक ठूलो कदम हुन सक्छ। तपाईंको गोपनीयताको अधिकारलाई हामीले गम्भीररूपमा लिन्छौं। यदि तपाईं बेनामी रहन चाहनु हुन्छ भने कृपया अपरेटरलाई बताउनु होला।
- संवेदनशील प्रकृतिको जानकारी भएकोले, तपाईंको फोन कल वा इमेलको नतिजाको जवाफ तपाईंले पाउनु हुने छैन।

तपाईंले प्रदान गर्नु हुने जानकारी समुदायमा हुने विदेशी हस्तक्षेप रोक्न सहयोग गर्न अष्ट्रेलियाली संघीय प्रहरीलाई चाहिने सुचना हुन सक्छ।

राष्ट्रिय सुरक्षा हटलाइन (NSH) लाई सम्पर्क गर्ने केही तरिकाहरू छन्:

- **फोन: 1800 123 400**
 - अष्ट्रेलिया बाहिरबाट: (+61) 1300 123 401

- टिटिवाई (TTY) प्रयोगकर्ताहरूको लागि (सुन्न कठिनाइ भएका प्रयोगकर्ताहरू): 1800 234 889
- यदि दोभाषेको आवश्यकता भएमा, कृपया ट्रान्सलेटिङ एण्ड इन्टरप्रेटिङ सर्भिसलाई १३१ ४५० मा फोन गर्नुहोस् र उनीहरूलाई राष्ट्रिय सुरक्षा हटलाइनमा सम्पर्क गराउन भन्नुहोस्
- एस एम एस (SMS)
 - कृपया तपाईंको जानकारी टेक्स्ट मेसेज मार्फत 0429 771 822 मा पठाउनु होस्
- इमेल
 - कृपया तपाईंको जानकारी इमेल मार्फत पठाउनु होस्: hotline@nationalsecurity.gov.au
- हुलाक मार्फत:
 - कृपया तपाईंको जानकारी निम्न ठेगानामा पठाउनु होस्:
National Security Hotline
Department of Home Affairs
PO Box 25
Belconnen ACT 2616

रिपोर्ट गर्ने अन्य तरिकाहरू

उपयुक्त भएमा, तपाईंको चासोहरू अन्य विभिन्न तरिकाहरू मार्फत तपाईंले रिपोर्ट गर्न सक्नु हुन्छ।

- इसेफ्टि (eSafety) ले गंभीररूपका अपमानजनक अनलाइन सामग्री हटाउन सहयोग गर्छ। तपाईंले गंभीर अनलाइन दुर्व्यवहार इसेफ्टि आयुक्त (eSafety Commissioner) लाई esafety.gov.au/report मा रिपोर्ट गर्न सक्नु हुन्छ।
- यदि तपाईंले कुनै तरिकाद्वारा **धम्कि पाएको वा असुरक्षित** महशुस गर्नु भएमा, तपाईंले निम्न स्थानमा सम्पर्क गर्न सक्नु हुन्छ:
 - **प्रहरी - तत्काल धम्किहरूका लागि ००० (तिन शून्य) मा**
 - **प्रहरी - ज्यान जोखिममा नहुने धम्किपूर्ण घटनाहरूका लागि १३ १४ ४४ मा।**
- अष्ट्रेलियाली संघीय प्रहरीलाई तपाईंले संघीय अपराधको रिपोर्ट अनलाइन संघीय अपराध फाराम मार्फत forms.afp.gov.au/online_forms/report_a_crime मा रिपोर्ट गर्न सक्नु हुन्छ। संघीय अपराधमा के के पर्छन् भनी थप जानकारीको लागि, कृपया afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime मा हेर्नुहोस्।
- समुदायका कुनै पनि सदस्यले शंकास्पद जासूसी वा विदेशी हस्तक्षेपका कृत्याकलापहरू अष्ट्रेलियाली संघीय प्रहरी (अष्ट्रेलियाली संघीय प्रहरीको सामुदायिक सम्पर्क टोली लगायत) का सदस्यसङ्ग सिधै कुराकानी गरेर रिपोर्ट गर्न सक्नुहुन्छ।

समुदायमा हुने विदेशी हस्तक्षेपको रिपोर्ट गर्दा मैले के अपेक्षा राख्न सक्छु?

समुदायमा हुने विदेशी हस्तक्षेपको प्रत्येक रिपोर्टको अनुसन्धान अष्ट्रेलियाली संघीय प्रहरीले गर्न सक्दैन। यदि कुनै अपराधिक दोषीको पहिचान गरिएको निर्धारण गर्न, राष्ट्रिय सुरक्षा हटलाइनले प्राप्त गर्ने प्रत्येक फोन कल वा रिपोर्ट गरिएको अपराधको छुट्टा छुट्टै केस (case-by-case) को आधारमा मुल्याङ्कन गरिन्छ। रिपोर्ट गर्दाको नतिजाहरूमा निम्न समावेश छन्:

- त्यहाँ कुनै प्रतिक्रिया नहुन सक्छ किनभने प्रहरीको लागि कारवाही अघि बढाउन, भएको प्रमाणले विधान अनुसारको थ्रेसहोल्ड (Legislative threshold) पूरा गर्न सक्दैन।
- अष्ट्रेलियाली संघीय प्रहरीले अनुसन्धान गर्न सक्छ
- अन्य प्रहरी सेवा वा सरकारी एजेन्सीले यस बारे कार्य गर्न सक्छ।

अष्ट्रेलिया बाहिर घटने अपराधहरुका लागि, अधिकार क्षेत्रका सीमितता लागु हुन्छ।

धम्कीहरुका प्रकारहरु

यदि तपाईंलाई प्रत्यक्ष भेटेरै धम्क्याएमा

- तपाईंलाई बताइए अनुसारको धम्की ठ्याक्कै लेख्नुहोस् वा रेकर्ड गर्नुहोस्।
- तपाईंलाई धम्क्याएको व्यक्ति बारेको विस्तृत जानकारी सकेसम्म धेरै खुलाएर रेकर्ड राख्नुहोस् (नाम, जेन्डर, उचाइ, वजन, कपाल र आँखाको रङ्ग, आवाज, लगाएको लुगा, वा कुनै अन्य चिनिने हुलिया)।
- प्रहरीलाई धम्कीको रिपोर्ट गर्नुहोस्।

यदि तपाईंलाई टेलिफोनबाट धम्क्याएमा

- यदि संभव भए, नजिकै रहेकाहरुलाई सुन्न र प्रहरीलाई खबर गर्न संकेत गर्नुहोस्।
- संभव भए कुराकानीको रेकर्ड गर्नुहोस्।
- धम्कीमा प्रयोग भएको ठ्याक्कै शब्द लेखेर राख्नुहोस्।
- फोनको इलेक्ट्रोनिक डिस्प्ले (Electronic display) बाट देखिने कुनै जानकारीको प्रतिलिपी उतार्नुहोस्।
- प्रहरीसङ्ग विस्तृतमा छलफल गर्न उपलब्ध हुनुहोस्।

यदि तपाईंलाई टेक्स्ट मेसेज, सिधा/निजी मेसेज, सामाजिक सञ्जाल वा इमेल लगायत विद्युतिय साधनहरु मार्फत धम्क्याएमा

- मेसेजहरुलाई नहटाउनुहोस्।
- मेसेजको जानकारीलाई प्रिन्ट गरेर, फोटो खिचेर, स्क्रिनशट लिएर, वा प्रतिलिपी उतारेर राख्नुहोस् (विषय, मिति, समय, पठाउने व्यक्ति, इत्यादि)। अस्थायीरूपमा डिजाइन गरेका मेसेजहरुको निश्चितरूपमा स्क्रिनशट लिनुहोस् वा सेभ गर्नु गर्नुहोस्।
- तपाईंले धम्की पाउनु भयो भनी तुरुन्तै प्रहरीलाई खबर गर्नुहोस्।
- सबै विद्युतिय प्रमाण जोगाउनुहोस्।

यी प्रकारका धम्कीहरुबाट आफूलाई बचाउन, निम्न सुझावहरु पालना गर्नुहोस्:

- अज्ञात व्यक्तिहरुबाट पठाइएका विद्युतिय मेसेजहरु वा संलग्न डकुमेन्ट नखोल्नुहोस्
- सामाजिक सञ्जालमा अज्ञात वा नचाहिएको व्यक्तिहरुसङ्ग कुराकानी नगर्नुहोस्
- तपाईंको डिभाइसहरु/खाताहरुका सेक्युरिटी सेटिङ्गहरुमा उच्च तहको सुरक्षा सुनिश्चित गर्नुहोस्।
- साइबर अपराधीहरुले तपाईंको विद्युतिय डिभाइसहरुलाई खतरामा पार्न र व्यक्तिगत जानकारी खोलीदिन सक्छन्
- पहिचान चोरी हुनबाट तपाईंको खाताहरु बचाउन तुरुन्तै तपाईंको वित्तिय संस्थाहरुलाई सम्पर्क गर्नुहोस्
- बलियो पासफ्रेज (Passphrases) हरु प्रयोग गर्नुहोस् र धेरै वेबसाइटहरुमा उही पासफ्रेज प्रयोग नगर्नुहोस्
- एन्टि-भाइरस (Anti-virus) र एन्टि-मालवेयर (Anti-malware) एप्लिकेसन्सलाई अप टु डेट राख्नुहोस्
- आवश्यक भए अनुसार सिस्टम र सफ्टवेयर अपडेटहरु लागू गर्नुहोस्
- टु-फ्याक्टर (Two-factor) प्रमाणिकरण लागू गर्नुहोस्
- डाटालाई नियमित ब्याकअप गर्नुहोस्
- तपाईंको मोबाइल डिभाइसलाई सुरक्षित राख्नुहोस्
- तपाईंको साइबर सुरक्षित विचार र सचेतनाको विकास गर्नुहोस्
- थप जानकारीको लागि, cyber.gov.au मा हेर्नुहोस्