İcmaya xarici müdaxilə

Xarici hökumətlərin təhdid və hədə-qorxularını necə bildirmək olar

**FACTSHEET** / April 2023 **afp.gov.au**

# Müqəddimə

Xarici müdaxilə Avstraliya xalqına, suverenliyinə və təhlükəsizliyinə və milli institutlarımızın bütövlüyünə ciddi təhlükə yaradır. Xarici müdaxilə təhdidləri Avstraliya icmasının bir sektoru ilə məhdudlaşmır və ya tək bir milli dövlət tərəfindən həyata keçirilmir. mütaxasim xarici dövlət aktyorları (digər ölkələrə qarşı düşmənçilik fəaliyyəti göstərən ölkələr) Avstraliya hökumətin bütün səviyyələrində və bir sıra sektorlarda, o cümlədən: demokratik təsisatlar; təhsil və tədqiqat; media və rabitə; kritik infrastruktur; və ən əsası, mədəni və dil baxımından müxtəlif ictimalarımızi (CALD) müdaxilə etmək imkanları yaradır və ardınca gedirlər.

# İcmaya xarici müdaxilə

İcmaya xarici müdaxilə Avstraliyanın multikultural həyat tərzinə zərər və təsir göstərmək məqsədilə xarici hökumətlər tərəfindən yönəldilmiş, nəzarət edilən və ya maliyyələşdirilən və CALD icmalarına yönəlmiş təhdid və hədə-qorxu kimi müəyyən edilir. Xarici hökumətlər bir sıra məqsədlər üçün icmalara müdaxilə edə bilər:

* xarici hökumətin daxili və xarici siyasətinin tənqidini susdurmaq
* CALD qruplarının üzvlərinin fəaliyyətinə (oflayn və onlayn) nəzarət etmək
* xarici hökumətin fikir və siyasətini təbliğ etmək
* xarici hökumətin xeyrinə məlumat əldə etmək
* daha geniş əhalinin fikir və rəylərinə təsir etmək.

# İcmaya xarici müdaxilə müxtəlif formalarda ola bilər

cümlədən:

* Hücum və ya hücum təhdidləri
* Şantaj
* Adam oğurluğu, qanunsuz həbs və ya azadlıqdan məhrum etmə
* izləmak və arzuolunmaz fiziki və ya elektron nəzarət
* Şəxsin ailəsini və ya xaricdəki iş tərəfdaşlar ını hədələyərək onlara əməl etməyə məcbur etmək
* Bir şəxsi və ya qrupu gözdən salmaq üçün sosial media vasitəsilə onlayn dezinformasiya kampaniyaları.

Əhəmiyyətli odur ki, *1995-ci il Cinayət Məcəlləsinə* (Cth) uyğun olaraq xarici müdaxiləni təşkil etmək üçün fəaliyyət xarici hökumət və ya onun vəkil etdiyi şəxslə əlaqələndirilməlidir. Cinayəti qiymətləndirərkən hüquq-mühafizə orqanları Avstraliya əyaləti və ya ərazisi cinayətlərini də nəzərdən keçirə bilər.

# Kim hədəfdədir?

Xarici hökumətlər aşağıdakıları hədəfləyə bilər:

* Avstraliyada yaşayan keçmiş və ya indiki vətəndaşlar
* Siyasi və insan hüquq müdafiəçiləri
* Dissidentlər (narazilər)
* Jurnalistlər
* Siyasi müxaliflər
* Dini və ya etnik azlıq qrupları.

# Kömək etmək üçün nə edə bilərəm?

İcmaya xarici müdaxilə ilə bağlı bütün raporlar AFP-nin açıq-aşkar reaksiyasını yaratmasa da, hər bir rapor ortaya çıxan problemlərin **mənzərəsini yaratmağa kömək edir**.

İcmaya hər hansı narahatlıq və/ya xarici müdaxilə halları barədə Milli Təhlükəsizlik Qaynar Xəttinə **(National Security Hotline) (NSH)** məlumat verilə bilər.

* NSH gündə 24 saat, həftənin 7 günü fəaliyyət göstərir və cəmiyyətə mümkün xarici müdaxilə ilə bağlı narahatlıqları bildirmək üçün mərkəzi əlaqə nöqtəsidir.
* NSH operatorları təqdim etdiyiniz məlumatla nə edəcəyini biləcəklər və lazım olduqda, qiymətləndirmə üçün hüquq-mühafizə və təhlükəsizlik orqanlarına ötürəcəklər.
* NSH operatorları hər bir zəngə ciddi yanaşır və alınan bütün məlumatları qiymətləndirir.
* Biz bilirik ki, narahatlıq doğuran bir məsələ barədə məlumat vermək böyük bir addım ola bilər. Məxfilik hüququnuzu ciddi qəbul edirik. Anonim qalmaq istəyirsinizsə operatora bildirin.
* Məlumatın həssas təbiətinə görə, zənginizin və ya e-poçtunuzun nəticəsi ilə bağlı məsləhət almayacaqsınız.

Təqdim etdiyiniz məlumat AFP-nin icmaya xarici müdaxilənin qarşısını almaq üçün ehtiyac duyduğu çatışmazlıq ola bilər.

**NSH** ilə əlaqə qurmağın bir neçə yolu var:

* **Zəng edin: 1800 123 400**
	+ Avstraliyadan kənardan: (+61) 1300 123 401
	+ TTY istifadəçiləri üçün (eşitmə qabiliyyəti olmayan istifadəçilər): 1800 234 889
	+ **Əgər tərcüməçiyə ehtiyacınız varsa, lütfən, 131 450 nömrəsinə Tərcümə və Tərcüməci Xidmətinə zəng edin və Milli Təhlükəsizlik Qaynar Xəttinə (National Security Hotline) zəng etməyi xahiş edin.**
* **SMS**
	+ Zəhmət olmasa məlumatlarınızı 0429 771 822 nömrəsinə mesajla göndərin
* **E-poçt**
	+ Zəhmət olmasa məlumatlarınızı e-poçt vasitəsilə hotline@nationalsecurity.gov.au ünvanına göndərin
* **Post:**
	+ Zəhmət olmasa məlumatlarınızı poçt vasitəsilə bu ünvana göndərin:

National Security Hotline

Department of Home Affairs

PO Box 25

Belconnen ACT 2616

# Hesabatın digər yolları

Siz həmçinin lazım olduqda bir sıra digər vasitələrlə öz narahatlıqlarınızı bildirə bilərsiniz.

* eSafety ciddi sui-istifadə edən onlayn məzmunu silməyə kömək edir. **Ciddi onlayn sui-istifadə barədə** [esafety.gov.au/report](http://www.esafety.gov.au/report) ünvanında eTəhlükəsizlik Müvəkkilinə (eSafety Commissioner) məlumat verə bilərsiniz .
* Əgər özünüzü **təhlükə altında və ya hər hansı şəkildə təhlükədə** hiss edirsinizsə **,** aşağıdakılarla əlaqə saxlaya bilərsiniz **:**
	+ **Polis - dərhal təhdidlər üçün 000-da**
	+ **Polis - həyati təhlükəsi olmayan hadisələrdə polisin iştirakı üçün 13 14 44-də.**
* Siz [forms.afp.gov.au/online\_forms/report\_a\_crime](https://forms.afp.gov.au/online_forms/report_a_crime) ünvanında onlayn Birlik Cinayəti Hesabat forması (online Report a Commonwealth Crime form) vasitəsilə Birlik cinayəti (Commonwealth Crime) haqqında AFP-yə məlumat verə bilərsiniz. Birlik Cinayətlərinin nədən ibarət olması haqqında ətraflı məlumat üçün [afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime](https://www.afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime) ünvanına baxın.
* İcmanın istənilən üzvü AFP-nin üzvü ilə (o cümlədən AFP-nin İcma ilə Əlaqələr Qrupu da daxil olmaqla) birbaşa danışaraq şübhəli casusluq və ya xarici müdaxilə fəaliyyətləri barədə məlumat verə bilər.

# Cəmiyyətə xarici müdaxilə barədə məlumat verməklə nə gözləyə bilərəm?

AFP cəmiyyətə xarici müdaxilə ilə bağlı hər xəbəri araşdıra bilməz. NSH-ə edilən hər bir çağırış və ya cinayət xəbəri hər hansı bir cinayətin müəyyən edilib-edilmədiyini müəyyən etmək üçün ayrı-ayrılıqda qiymətləndirilir. Hesabatın hazırlanmasının nəticələrinə aşağıdakılar daxildir:

* heç bir cavab olmaya bilər, çünki məsələ polisin hərəkətə keçməsi üçün qanunvericilik həddinə uyğun gəlmir
* AFP araşdıra bilər
* məsələ ilə başqa polis xidməti və ya dövlət orqanı məşğul ola bilər.

Avstraliyadan kənarda baş verən cinayətlər üçün yurisdiksiya məhdudiyyətləri tətbiq olunur.

# Təhdidlərin növləri

## Əgər şəxsən hədələnirsinizsə

* Təhdidi tam olaraq bildirildiyi kimi yazın və ya qeyd edin.
* Təhdidi edən şəxs haqqında çoxlu təsviri təfərrüatları qeyd edin (adı, cinsi, boyu, çəkisi, saç və göz rəngi, səs, geyim və ya hər hansı digər fərqləndirici xüsusiyyətlər).
* Təhdidi polisə bildirin.

## Əgər telefonla hədələnirsinizsə

* Mümkünsə, yaxınlıqdakı insanlara qulaq asmaq və polisə məlumat vermək üçün işarə verin.
* Mümkünsə zəngi qeyd edin.
* Təhdidin dəqiq ifadəsini yazın.
* Telefonun elektron ekranından istənilən məlumatı kopyalayın.
* Təfərrüatları polislə müzakirə etmək üçün hazır olun.

## Mətn mesajı, birbaşa/şəxsi mesaj, sosial media və ya e-poçt da daxil olmaqla elektron vasitələrlə hədələnirsinizsə

* Mesajları silməyin.
* Mesaj məlumatını (mövzu sətri, tarix, vaxt, göndərən və s.) çap edin, fotoşəkili, ekran görüntüsünü və ya kopyalayın. Müvəqqəti olmaq üçün hazırlanmış mesajları yadda saxladığınızdan və ya skrinşotunu çəkdiyinizdən əmin olun.
* Təhlükə almağınız barədə dərhal polisə xəbər verin.
* Bütün elektron sübutları qoruyun.

Özünüzü bu cür təhlükələrdən qorumaq üçün bu tövsiyələrə əməl edin:

• Naməlum göndəricilərdən gələn elektron mesajları və ya qoşmaları açmayın

• Sosial mediada naməlum və ya istənməyən şəxslərlə ünsiyyət qurmayın

• Cihazlarınızda/hesablarınızda təhlükəsizlik parametrlərinizin ən yüksək qoruma səviyyəsinə qoyulduğundan əmin olun

• Kiber cinayətkarlar sizin elektron cihazlarınızı ələ keçirə və şəxsi məlumatlarınızı ifşa edə bilərlər

• Hesablarınızı şəxsiyyət oğurluğundan qorumaq üçün dərhal maliyyə qurumlarınızla əlaqə saxlayın

• Güclü parol ifadələrindən istifadə edin və birdən çox sayt üçün eyni paroldan istifadə etməyin

• Anti-virus və anti-zərərli proqram tətbiqlərinin yeni olduğundan əmin olun

• Lazım olduqda sistem və proqram yeniləmələrini tətbiq edin

• İki faktorlu autentifikasiya tətbiq edin

• Məlumatların müntəzəm olaraq ehtiyat nüsxəsini çıxarın

• Mobil cihazınızı qoruyun

• Cyber Secure düşüncənizi və məlumatlılığınızı inkişaf etdirin

• Əlavə məlumat üçün cyber.gov.au saytına daxil olun.