Spionageabwehr

Trans-nationale Repression

Leitfaden für Betroffene

Bundesministerium
des Innern

Inhalt

Was ist Transnationale Repression?

Die Bundesregierung hat es sich zum Ziel gesetzt, Transnationaler Repression durch autoritäre Staaten in Deutschland wirksam zu begegnen.

Unter Transnationale Repression (TNR) fällt jedes Handeln eines fremden Staats, durch das von ihm als Gegner eingestufte und im Ausland lebende Personen verfolgt, unterdrückt und/oder einschüchtert werden.

Das Agieren fremder Staaten reicht von der Ausspähung über die Bedrohung und Verfolgung bis hin zu schwersten Gefahren für Leib und Leben. TNR kann unter anderem folgende Formen annehmen:

- Physische Angriffe, die von körperlichen Angriffen über Entführung bis hin zur Ermordung der Person reichen können
- Ausspähung, Bedrohung, Ansprache, Stalking, etc., häufig eingesetzt zur Ausübung psychischen Drucks
- Digitale Transnationale Repression wie Online-Einschüchterung, Verleumdung und Doxing sowie Cyberangriffe gegen Betroffene
- Missbrauch multilateraler oder bilateraler Strafverfolgungsmechanismen wie INTERPOL-Rotecken, Auslieferungsverfahren, Ausschreibung von Reisedokumenten und anderer Formen der zwischenstaatlichen Rechtshilfe
- Missbrauch/Verweigerung konsularischer Dienste durch den Herkunftsstaat
- Bedrohung von Familienangehörigen

Besonders betroffen sind im Ausland lebende Oppositionelle, Menschenrechtsaktivisten, Journalisten sowie Angehörige von Diaspora-Gemeinden.

Wie kann Transnationale Repression gemeldet werden?

1. Unmittelbare Gefährdung

Wenn sich Betroffene in einer **unmittelbaren Gefahr** befinden und/oder eine Straftat anzeigen wollen, sollten sie den **Notruf der Polizei** wählen (110).

2. Mögliche Straftat

Wenn es sich nicht um eine unmittelbare Gefahr handelt, aber eine mögliche Straftat vorliegt, sollte die **lokale Polizeidienststelle** oder das **Landeskriminalamt** (des jeweiligen Bundeslandes) kontaktiert werden. Kontaktdaten (telefonische und E-Mail-Erreichbarkeiten) sind über das Internet abrufbar. Diese Stellen sind auch für individuelle Gefährdungsbewertungen und ggf. die Ergreifung von (Schutz-)Maßnahmen zuständig.

3. Hinweiskanal des Bundesamtes für Verfassungsschutz (BfV)

Betroffene können sich auch vertraulich und rund um die Uhr an den **Hinweiskanal des Bundesamtes für Verfassungsschutz (BfV)** wenden, wenn sie staatliche Stellen oder gar nachrichtendienstliche Akteure hinter dem Vorgehen vermuten:

Rufnummern:

+49 228 99792-6000
+49 30 18792-6000

E-Mail: hinweise@bfv.bund.de

Oder per Kontaktformular über die BfV-Homepage: https://www.verfassungsschutz.de/DE/service/kontakt/formulare/Kontakt_HinweisGeben/kontakt_node.html

Ihr Hinweis wird in jedem Fall geprüft, auch wenn Sie in der Regel keine Rückmeldung des BfV erhalten. In Einzelfällen werden Sie eventuell kontaktiert, falls weitere Informationen benötigt werden. Jede Information ist hilfreich und es sind keine Konsequenzen zu befürchten, wenn ein Hinweis nicht richtig sein sollte.

4. Missbrauch von INTERPOL-Instrumenten

Sollten Sie Opfer eines Missbrauchs von INTERPOL-Instrumenten sein, oder einen entsprechenden Verdacht haben, können Sie sich direkt an die Kommission zur Kontrolle der INTERPOL-Dateien (CCF) wenden. Die Kommission hat drei Aufgabenbereiche, in denen sie Anträge von Einzelpersonen auf Auskunft, Berichtigung oder Löschung von Daten im INTERPOL-Informationssystem bearbeitet. Zur Erfüllung ihrer Aufgaben konsultiert die Kommission direkt das INTERPOL-Generalsekretariat, die nationalen Zentralbüros und andere zuständige Stellen.

https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF

Wie können sich Betroffene schützen?

1. Cybersicherheit

Mögliche Bedrohungsszenarien von fremden Staaten im Cyberraum reichen von einer möglichen Einschüchterung über die Ausspähung persönlicher Netzwerke und Kommunikation bis hin zu Vorbereitungshandlungen von repressiven Handlungen in der Realwelt. Die nachfolgend beispielhaft dargestellten Maßnahmen können das Sicherheitsniveau im Zusammenhang mit Cyberangriffen erhöhen und einen möglichen Schaden entsprechend verringern:

Private Daten

- Gehen Sie restriktiv mit Ihren persönlichen Daten um, insbesondere in sozialen Netzwerken.
- Geben Sie keine persönlichen Daten auf nicht vertrauenswürdigen Webseiten preis.
- Legen Sie ein gesundes Maß an Misstrauen an den Tag.

Cloud-Dienste

- Entscheiden Sie bewusst, welche Cloud-Dienste genutzt werden und was in der Cloud gespeichert werden soll.
- Deaktivieren Sie automatische Upload- und Synchronisations-Funktionen.

E-Mails

- Schützen Sie sich vor Phishing.
  Seien Sie misstrauisch und fragen Sie im Zweifel beim Absender nach.
- Öffnen Sie Links und Anhänge nur nach gründlicher Prüfung.
- E-Mail-Clients sollten so konfiguriert werden, dass sie eventuell vorhandenen HTML-Code und andere aktive Inhalte in E-Mails nicht automatisch interpretieren. Darstellungen von E-Mail als „Nur-Text“ (anstelle von z. B. HTML) reduzieren die Möglichkeiten von Täuschungen.
- Vorschaufunktionen für Datei-Anhänge sollten so konfiguriert werden, dass sie Dateien nicht automatisch interpretieren.

Mobile Geräte

- Nutzen Sie für Kommunikation nur Messengerdienste mit Ende-zu-Ende-Verschlüsselung, die sich für einen sicheren Informationsaustausch eignet (z.B. Signal, Threema). Blockieren Sie Nachrichten von unbekannten Konten und deaktivieren Sie Linkvorschau-Funktionen.
- Beziehen Sie Ihre Apps nur aus vertrauenswürdigen Quellen (z. B. vorinstallierten Appstores).
- Falls Sie ein iPhone nutzen: Prüfen Sie die Aktivierung des sog. „Lockdown“-Modus. Dieser wurde von Apple speziell für den Schutz vor fortgeschrittenen Cyberbedrohungen, wie etwa im Bereich TNR, eingeführt.
- Schalten Sie Ihr mobiles Gerät komplett aus, um Tracking oder Abhören zu verhindern, oder lassen Sie es bei sensiblen Terminen zu Hause.
  Bedenken Sie dabei auch, dass Wearables wie Smart Watches oder Glasses auch entsprechende Funktionen enthalten.
- In den Appstores gibt es Apps, um unbefugtes Tracking mittels Smart Tags zu erkennen.
- Lassen Sie Ihr mobiles Gerät nicht unbeaufsichtigt.

- Halten Sie das Betriebssystem Ihres Mobilgerätes stets aktuell.

- Sichern Sie Ihre Daten regelmäßig.

Social Media
- Passen Sie Ihre Privatsphäre-Einstellungen an.

- Nutzen Sie auf Internetplattformen nach Möglichkeit Pseudonyme.

- Trennen Sie berufliche und private Profile.

- Gewähren Sie nur für Freunde Einsicht auf Ihr privates Profil.

Passwörter:
- Nutzen Sie für jede Anwendung ein individuelles Passwort.

- Ein Passwort-Manager kann helfen, sichere Passwörter zu generieren und zu verwalten.

- Nutzen Sie eine Multi-Faktor-Authentifizierung.

Software:
- Nutzen Sie aktuelle Betriebssysteme und die integrierten Schutzprogramme (z.B. Microsoft Windows Defender).

- Führen Sie unverzüglich die erforderlichen Sicherheitsupdates bei Ihren Betriebssystemen, Programmen und Apps durch.

- Führen Sie regelmäßige Datensicherungen auf externen Speichermedien durch.

WLAN:
- Offene, frei verfügbare WLAN-Hotspots sind unsicher.

- Nutzen Sie einen VPN-Dienst, um Ihre Daten verschlüsselt in einem WLAN zu übertragen.

Weitere Empfehlungen zur Cyber-Sicherheit können Sie beim **Bundesamt für Sicherheit in der Informationstechnik (BSI)** abrufen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

Für ergänzende **Fragen zur IT-Sicherheit Ihrer Systeme** bietet das BSI mit seinem Service-Center Unterstützung an:
https://www.bsi.bund.de/DE/Service-Navi/Kontakt/kontakt_node.html

Zusätzlich können Sie dort auch einen **IT-Sicherheitsvorfall melden**, um Beratung und Hilfe zu erhalten, diesen richtig einzuschätzen und einen Digitalen Ersthelfer zu kontaktieren:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen-und-Buerger/buergerinnen-und-buerger.html?pos=1

2. Persönliche Sicherheit

Betroffene, die um ihre persönliche Sicherheit besorgt sind, können sich schützen, indem sie:

- Ihre persönlichen Daten und Erreichbarkeiten schützen (keine Live-Postings, keinen Live-Standort oder Wohnanschrift teilen, Telefonnummern/ E-Mail-Adressen nur an vertraute und vertrauenswürdige Personen weitergeben).

- Ihre Aktivitäten (Vorträge, Postings, Tätigkeiten etc.) vorübergehend anpassen (siehe unten) und/oder temporär stark öffentlichkeitswirksame Auftritte reduzieren.

- Sich an die örtlichen Polizeidienststellen wenden; diese können einzelfallbezogene, gefahrenabwehrende Maßnahmen treffen. Hierbei handelt es sich um Maßnahmen zum unmittelbaren Schutz der Betroffenen.

Auch im Alltag können Betroffene sich schützen:

- Versuchen Sie, Ihre Routinen und Ihre Zeiten (z. B. zur und von der Arbeit) zu variieren, um es für Personen, schwieriger zu machen, Ihnen zu schaden.

- Wenn möglich, unternehmen Sie Besuche, Meetings und Reisen in Begleitung.

- Wenn Sie Termine wahrnehmen, teilen Sie vertrauten Personen mit, wann Sie zum Termin erscheinen, wieder zurückkehren und was zu veranlassen ist, wenn Sie zum Termin nicht erscheinen oder nicht wieder zurückkehren.

- Achten Sie auf ungewöhnliche Personen oder Umstände in Ihrer Umgebung.

- Wenn Sie sich verfolgt oder beobachtet fühlen, gehen Sie nicht nach Hause, sondern suchen Sie belebte Plätze auf und fragen Sie nach Hilfe.

- Wenn Sie angesprochen werden, bleiben Sie höflich und versuchen Sie sich aus der Situation herauszunehmen.

- Sollten Sie verdächtige Aktivitäten oder Verhaltensweisen feststellen, dokumentieren Sie diese möglichst detailliert (Datum, Uhrzeit, Ort, Beschreibung der beteiligten Personen oder Fahrzeuge und dergleichen). Diese Dokumentation wird für die Polizei nützlich sein.

- Sollten sie bereits aufgrund von Hinweisen einer gegen Sie gerichteten Bedrohung ein Beratungsgespräch mit der Polizei durchgeführt haben und feststellen, dass Sie verfolgt oder beobachtet werden, wenden Sie sich an die Ihnen ggf. mitgeteilte Kontaktnummer der Polizei oder auch jederzeit an die Notfallnummer 110. Erklären Sie die Situation und weisen Sie darauf hin, dass es sich bei Ihnen um eine gefährdete Person handelt.

- Bewerten Sie Ihre bereits veranlassten Sicherheitsmaßnahmen und ob hier weitere Vorsorge erforderlich ist, wie zum Beispiel Verbesserung von Tür- und Fensterschlössern, Installieren von Überwachungskameras, Variieren täglicher Routinen, Beratung durch eine private Sicherheitsfirma.

3. Reisehinweise

Vor der Reise:

- Informieren Sie sich über die Gefährdungs-, Sicherheits-, und Gesetzeslage in Ihrem Zielland.

- Auf der Homepage des Auswärtigen Amtes werden Reise- und Sicherheitshinweise zu verschiedenen Ländern veröffentlicht, die vor einer Reise konsultiert werden sollten: https://www.auswaertiges-amt.de/de/reiseundsicherheit/reise-und-sicherheitshinweise

- Fragen Sie nach Erfahrungen von anderen Reisenden.

- Stellen Sie Kontaktadressen für Notfälle zusammen (Botschaften, Konsulate, medizinische Versorgung, etc.) und tragen Sie sich in die Krisenvorsorgeliste des Auswärtigen Amts ein: https://krisenvorsorgeliste.diplo.de/signin

- Nehmen Sie nach Möglichkeit nicht die IT-Geräte (Smartphones, Tablets, Laptops, Smartwatches, etc.) mit, die Sie hier in Deutschland benutzen.
  Beschaffen Sie sich nur für Reisen vorgesehene Geräte („Burner-Phones“ / Wegwerf-Handys), auf denen nur die notwendigsten Nummern und Daten gespeichert sind.

- Nehmen Sie nur die Dokumente mit, die für die Reise unbedingt gebraucht werden. Fertigen Sie sicherheitshalber Kopien an und verwahren Sie diese an einem sicheren Ort.

- Machen Sie in Einreise- und Anmeldeformularen wahrheitsgemäße, aber möglichst allgemeine Angaben.

Während der Reise:

- Rechnen Sie bei der Einreise im Zielland mit Sicherheitskontrollen als auch mit Gepäckdurchsuchungen.

- Planen Sie Transportmittel und -routen vorab.

- Seien Sie skeptisch bei Kontaktversuchen und Geschenken von Personen, die sie bisher nicht kannten. Reisen Sie, wenn möglich, in Begleitung.

- Halten Sie sich nach Möglichkeit von potentiell gefährlichen Situationen fern (z. B. Protesten).

- Beschränken Sie Gespräche über vertrauliche Inhalte auf ein Minimum.

- Meiden Sie offene Bluetooth- und WLAN-Verbindungen, insbesondere wenn diese von dem Zielland gefordert werden. Sofern sich die Nutzung nicht vermeiden lässt, nutzen Sie nach Möglichkeit einen VPN-Service.

- Verwenden Sie nur eigene Ladegeräte und keine offenen USB-Ports oder fremde Geräte, insb. in Hotelzimmern.

- Lassen Sie Vorsicht gegenüber Dienstleistern und Servicepersonal walten.

Nach der Reise:

- Besprechen Sie die Reise mit Mitreisenden oder vertrauenswürdigen Personen in Deutschland nach.

- Setzen Sie mitgenommene Geräte auf die Werkseinstellungen zurück und löschen Sie alle Daten.
  Oder erwägen Sie gar, diese Geräte zu entsorgen („Burner-Phones“ / Wegwerf-Handys).

- Prüfen Sie Ihre ggf. unterwegs genutzten Online-Benutzerkonten unverzüglich auf verdächtige Aktivitäten (z.B. erfolgte Anmeldungen durch welche Geräte, hinzugefügte neue Nutzer/Gerät, erweiterte Datensicherungen auf unbekannte Systeme) und ändern Sie die Zugangsdaten.

- Notieren Sie auffällige bzw. ungewöhnliche Beobachtungen, Ereignissen und Unregelmäßigkeiten und melden Sie diese ggf. an Ihre zuständige Polizeidienststellen oder an das Bundesamt für Verfassungsschutz.

4. Hilfsangebote

Verschiedene Hilfsangebote für Betroffene von Straftaten sind auf der Webseite www.hilfe-info.de zusammengestellt. Diese hat das Bundesministerium der Justiz und für Verbraucherschutz als zentrales Informationsangebot für Betroffene von Straftaten geschaffen. Die Webseite beinhaltet Informationen zu den opferrechtlichen Belangen nach einer Straftat, u. a. zum Ablauf des Ermittlungs- und Strafverfahrens, zu Hilfs- und Beratungsmöglichkeiten sowie zu finanziellen, praktischen, psychologischen und rechtsmedizinischen Unterstützungsleistungen. Über den Beratungsstellen-Finder können Betroffene eine Opferhilfeeinrichtung in ihrer Nähe suchen.

Impressum

Herausgeber
Bundesministerium des Innern, 11014 Berlin
Internet: www.bmi.bund.de

Stand
Mai 2026

Artikelnummer
BMI26015

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie unter: www.publikationen-bundesregierung.de

www.bmi.bund.de
bsky.app/profile/bmi.bund.de
instagram.com/bmi_bund
linkedin.com/company/bundesinnenministerium
social.bund.de/@bmi
threads.com/@bmi_bund
x.com/BMI_Bund
youtube.com/@BMIBund