Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Dienst Überwachung Post- und Fernmeldeverkehr ÜPF

Jahresbericht 2022
Dienst ÜPF

Die Überwachung des Fernmeldeverkehrs ist in einem globalen Kontext zu betrachten. Standardsprache auf internationalen Konferenzen, in länderübergreifenden Gremien und nicht zuletzt in der Telekommunikationsindustrie ist Englisch. Der englische Begriff für die gesetzeskonforme Überwachung – Lawful Interception (LI) – bürgerte sich deshalb auch hierzulande ein. Der Dienst ÜPF trug dem Sprachgebrauch im Jahr 2010 Rechnung. Seitdem hat er seine eigene Website, welche unter www.li.admin.ch zu finden ist.

www.li.admin.ch

Liebe Leserin, lieber Leser

Jede Umsetzung einer Massnahme zur Überwachung des Post- und Fernmeldeverkehrs stellt einen schweren Eingriff in die Grundrechte der betroffenen Person dar. Eingriffe in diese von der Verfassung geschützten Rechte müssen ausdrücklich in einem Gesetz vorgesehen sein. Die konkrete Ausführung der Massnahmen wird in den Umsetzungsverordnungen detailliert geregelt. Zudem muss jede Überwachungsmassnahme von einem Gericht genehmigt werden.

Um es in aller gebotenen Deutlichkeit zu sagen: Zwischen der Ausführung einer Massnahme durch den Dienst ÜPF und deren rechtliche Grundlage darf kein Blatt Papier passen.

Die Fernmeldetechnologie entwickelt sich exponentiell und bietet immer mehr neue Dienste und Kommunikationsmöglichkeiten. Um damit Schritt halten zu können, muss der technische, organisatorische und administrative Rahmen der Fernmeldeüberwachung regelmässig angepasst werden. Dies erfolgt unter der Federführung des Dienstes ÜPF unter Einbezug der Strafbehörden und der Anbieterinnen von Telekommunikationsdiensten.

Auch wenn sich die Fernmeldeüberwachung rasant verändert, bleibt unser gesetzlicher Auftrag derselbe: die Sicherstellung einer wirksamen Strafverfolgung. Eines der Instrumente, das uns dafür zur Verfügung steht, ist der Einsatz des Special-Case-Teams.

«Auch wenn sich die Fernmeldeüberwachung rasant verändert, bleibt unser gesetzlicher Auftrag derselbe: die Sicherstellung einer wirksamen Strafverfolgung.»

Diese mobile Einheit kann auf richterliche Anordnung bei allen in der Schweiz tätigen Providern von Telekommunikationsdienstleistungen Überwachungsmassnahmen durchführen. Wie ein solcher Spezialeinsatz abläuft, wie unsere Experten ausrücken, um vor Ort eine Überwachungsinfrastruktur einzurichten, erfahren Sie ab Seite 15.

Mich persönlich erinnerte der Beitrag an meinen Dienstantritt vor mittlerweile 15 Jahren. Damals war der Dienst ÜPF für die Abwicklung von Spezialfällen auf externe Partner angewiesen. Als gelernter Fernmeldetechniker und Ingenieur war für mich klar, dass dieses Modell in einer Zeit des rasanten technologischen Wandels obsolet werden würde. Deswegen setzt der Dienst ÜPF seit 2010 in all seinen Tätigkeitsgebieten vermehrt auf eigene Kompetenzen. Der Auf- und Ausbau Letzterer erlaubt dem Dienst ÜPF, den Herausforderungen in seinem komplexen und hochspezialisierten Umfeld gerecht zu werden.

Ich wünsche Ihnen eine gute Lektüre.

René Koch
Leiter Dienst ÜPF (bis Mai 2023)

01

ÜBERBLICK

■ Unter Fernmeldedienstanbieterinnen werden unter anderem Mobilfunk-, Telefon-, E-Mail- und Internetdienstanbieterinnen wie Swisscom, Sunrise oder Salt verstanden.

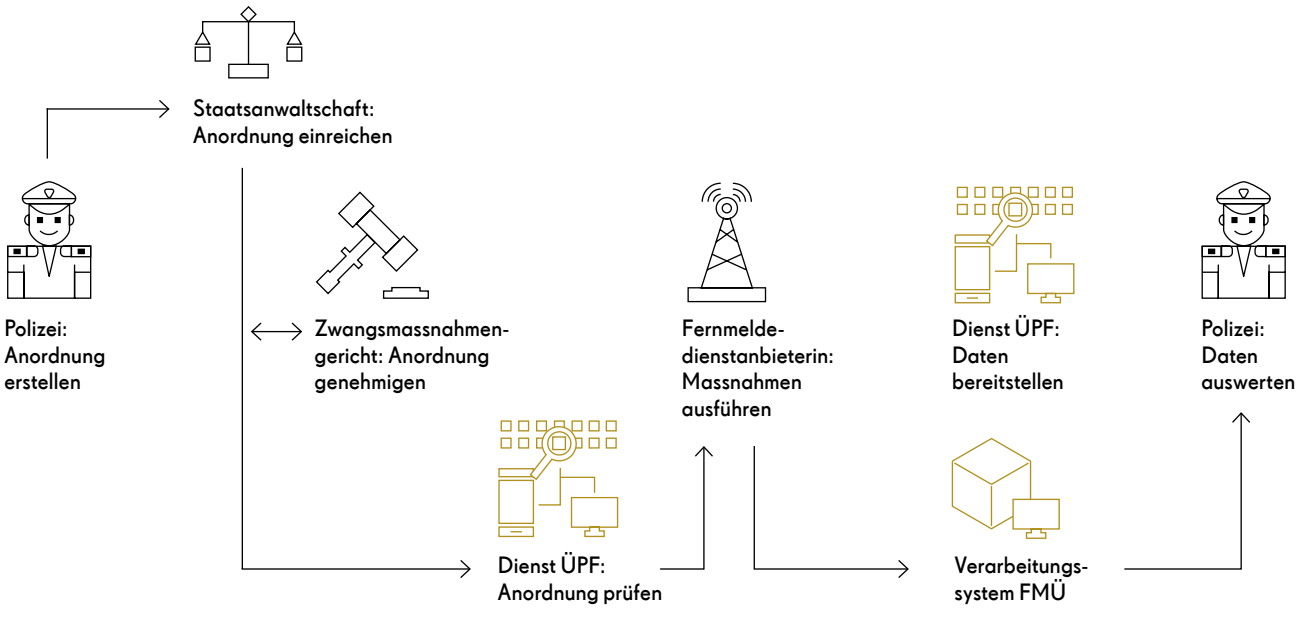
Der Dienst ÜPF in Kürze

Um schwere Verbrechen aufzuklären, haben die Strafbehörden von Bund und Kantonen die Möglichkeit, Massnahmen zur Überwachung des Post- und Fernmeldeverkehrs anzuordnen. Seit 1. Januar 1998 ist der Dienst ÜPF für die Umsetzung dieser Massnahmen zuständig. Gleichzeitig stellt er sicher, dass die geltenden Vorgaben eingehalten werden. Er holt bei den Fernmeldedienstanbieterinnen (FDA) die Daten ein, die von den Strafbehörden oder dem Nachrichtendienst des Bundes (NDB) angefordert werden und übergibt diese den Ermittlern zur Auswertung und Analyse.

Weder die Kriminalität noch die moderne Telekommunikation kennen territoriale Grenzen. Der internationalen Zusammenarbeit kommt daher bei der Verbrechensbekämpfung eine wichtige Bedeutung zu. Der Dienst ÜPF engagiert sich hierzu auf den Gebieten der internationalen Standardisierung sowie des Informations- und Wissensaustauschs mit den entsprechenden ausländischen Dienststellen.

Der Dienst ÜPF ist für die Umsetzung von Überwachungen des Post- und Fernmeldeverkehrs zuständig. Seine Aufgaben erfüllt er unabhängig, selbstständig und weisungsungebunden. Administrativ ist er dem Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) zugewiesen. Er ist in vier Bereiche gegliedert.

Der Überwachungsprozess



Die vier Bereiche

Die Leitung des Dienstes ÜPF (von links nach rechts): René Koch (Leiter Dienst ÜPF und des Bereiches Verwaltungsstrafverfahren), Jean-Louis Biberstein (Bereichsleiter Recht und Controlling/Stv. Leiter Dienst ÜPF), Alexandre Suter (Bereichsleiter Providermanagement) und Michael Galliker (Bereichsleiter Überwachungsmanagement)

Provider-management

Die 22 Mitarbeitenden sind unter anderem für die Erarbeitung und Pflege der technischen Vorgaben, welche die FDA beim Datenaustausch mit dem Dienst ÜPF zu beachten haben, verantwortlich. Ausserdem sind sie für das sogenannte Compliance-Verfahren zuständig. Hierbei prüft der Dienst ÜPF, ob die geforderte Überwachungs- und Auskunftsbereitschaft gewährleistet ist. Gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) müssen die Anbieterinnen jederzeit fähig sein, die von ihnen angebotenen Dienste zu überwachen und die damit zusammenhängenden Auskünfte und Informationen zu erteilen. Es sei denn, sie haben sich von der Pflicht, Überwachungen auszuführen, ordnungsgemäss befreien lassen.

Für die Umsetzung von Überwachungsmassnahmen bei Anbieterinnen, die nicht verpflichtet oder nicht in der Lage sind, dies selber zu tun, entwickelt und betreibt das Providerma-

nagement massgeschneiderte Speziallösungen, sogenannte Spezialfälle. Das übernimmt das «Special Case Team», das unter anderem dann ausrückt, wenn ein Überwachungsauftrag bei einer kleinen Anbieterin – zum Beispiel einem lokalen Kabelnetzbetreiber oder einem Hotel – ansteht. Siehe auch dazu der Bericht «Special Cases» auf Seite 15.

Ausserdem verwalten die Mitarbeitenden die Beziehungen zu mehr als 900 Anbieterinnen, beraten diese in technischen und juristischen Fragen und erlassen im Rahmen ihrer Aufsichtskompetenzen entsprechende Vorgaben und Verfügungen.

Ein vierköpfiges Team ist für das reibungslose Funktionieren der Applikationen des Verarbeitungssystems zuständig, auf dem die Daten ausgeleitet werden.

Weiter unterstützen Experten aus dem Bereich Providermanagement die Entwicklung neuer Anwendungen und engagieren sich in verschiedenen nationalen und internationalen Standardisierungsgremien. Dort geht es zum Beispiel um die Entwicklung und Bereitstellung der Schnittstellenspezifikationen in den 4G- und 5G-Netzwerken.

Überwachungsmanagement

Der Bereich Überwachungsmanagement mit seinen 17 Mitarbeitenden verantwortet die reibungslose Zusammenarbeit des Dienstes ÜPF mit den Strafbehörden und dem NDB.

Das Team berät Polizeikorps, Staatsanwaltschaften, Zwangsmassnahmengerichte und den NDB in allen rechtlichen, technischen, organisatorischen und administrativen Angelegenheiten im Rahmen der Post- und Fernmeldeüberwachung.

Die Mitarbeitenden nehmen die Überwachungsaufträge entgegen, übermitteln sie nach einer formellen Prüfung den Anbieterinnen und stellen sicher, dass die Behörden die angelieferten Daten erhalten. Ebenfalls zu den Aufgaben des Überwachungsmanagements gehören die Rechnungsstellung an die Strafbehörden und den NDB sowie die Auszahlungen der Entschädigungen an die FDA.

Das Team ist die zentrale Anlaufstelle, wenn es Probleme mit dem Verarbeitungssystem gibt oder die Benutzerinnen und Benutzer sonstige Schwierigkeiten bekunden, und begleitet die Entwicklung neuer Anwendungen.

Des Weiteren ist das Überwachungsmanagement für die Schulung der Benutzerinnen und Benutzer zuständig.

Ausserhalb der Bürozeiten unterhält das Überwachungsmanagement den operativen Pikettdienst mit der technischen Unterstützung vor allem durch das Providermanagement. So bleibt der Dienst ÜPF rund um die Uhr erreichbar.

Recht und Controlling

Die Informations- und Kommunikationstechnik (IKT) ist eine der innovativsten Branchen überhaupt. Sie implementiert regelmässig neue Standards, lanciert laufend neue Dienste für immer leistungsfähigere Endgeräte. Für die Überwachung des Fernmeldeverkehrs hat das Folgen: Die technische Schnittstelle zwischen dem Verarbeitungssystem des Dienstes ÜPF und den mehreren hundert Anbieterinnen steht unter einem hohen Anpassungsdruck.

Die Fachleute von Recht und Controlling stellen zusammen mit ihren Kollegen vom Providermanagement sicher, dass die Möglichkeit

zur Fernmeldeüberwachung auch in einem höchst dynamischen technologischen Umfeld jederzeit gewährleistet ist. Sie unterstützen mit ihrem Fachwissen die Planung und Steuerung sämtlicher missionskritischer Informatikprojekte.

Das 16-köpfige Team verantwortet aber nicht nur die fachgerechte Abwicklung der IT-Projekte, sondern auch die Ausarbeitung der benötigten Rechtsgrundlagen zur Sicherstellung der Fernmeldeüberwachung.

In vielen Fällen geht es darum, den Wandel der Technik auf Verordnungsebene abzubilden. Die departementale Verordnung über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) zum Beispiel wird periodisch überprüft und wenn nötig angepasst.

In die Zuständigkeit des Bereichs Recht und Controlling fallen schliesslich die finanzielle Führung, das Reporting sowie die Öffentlichkeitsarbeit. Die Mitarbeitenden beantworten Medienanfragen und stehen den Bürgerinnen und Bürgern für Auskünfte zur Verfügung.

Verwaltungsstrafverfahren

Durch das BÜPF und die zugehörigen Ausführungsverordnungen wurden dem Dienst ÜPF zusätzliche Aufgaben übertragen. Eine von ihnen ist die Durchführung von Verwaltungsstrafverfahren. Dabei übernimmt eine unabhängige Untersuchungsleiterin die Aufgaben analog einer Staatsanwaltschaft.

Seit März 2018 ist der Dienst ÜPF also berechtigt, gegen jene vorzugehen, die ihren gesetzlichen Pflichten im Rahmen der Überwachung des Post- und Fernmeldeverkehrs nicht nachkommen.

Das zweiköpfige Team des Bereichs Verwaltungsstrafverfahren geht Anzeigen nach, stellt den Sachverhalt fest, nimmt die juristische Analyse vor und bestraft gegebenenfalls diese Übertretungen. Die Verfahrensleitung kann Zwangsmassnahmen wie Beschlagnahme und Durchsuchungen anordnen sowie Einvernahmen durchführen.

Nach Abschluss eines Verfahrens erlässt der Dienst ÜPF Strafverfügungen, Strafbescheide und Einstellungsverfügungen.

Rückblick

Januar

Beginn Aufschaltung SLDT für Benutzer
Mit der Lösung SLDT (secure large data transfer) können grössere Datenmengen auf sicherem Weg elektronisch an die Benutzerinnen und Benutzer übermittelt werden. Somit kann in gewissen Fällen auf den Versand per Post von Datenträgern verzichtet werden. Die ersten Polizeiorganisationen haben SLDT zusammen mit dem Dienst ÜPF erfolgreich getestet und den Benutzern wird nun der Zugriff schrittweise gewährt.

Februar

Es finden wieder Schulungen statt, wenn auch nur im kleinen Rahmen
Nach einer langen pandemiebedingten Pause konnten erste Schulungen vor Ort wieder durchgeführt werden. Das inzwischen erarbeitete Angebot an online-Schulungsmaterial bleibt verfügbar und wird weiter ausgebaut.

März

Inkraftsetzung der gesetzlichen Grundlage für die Analysefunktionen
Am 11. März 2022 hat der Bundesrat beschlossen, die gesetzliche Grundlage für die Analysefunktionen am 1. Mai 2022 in Kraft zu setzen. Mit dieser Änderung (Art. 7 und 8 BÜPF) wird die explizite gesetzliche Grundlage geschaffen, um Daten der Fernmeldeüberwachung im Verarbeitungssystem (V-FMÜ) des Dienstes ÜPF analysieren zu können.

April

Webserie «la Suisse sous couverture»
Am 25. April 2022 hat die RTS die Veröffentlichung der zweiten Saison der Webserie «la Suisse sous couverture» angekündigt. Darunter fällt eine Reportage über das Überwachungssystem des Dienstes ÜPF. Dieser kurze, 12 minütige Dokumentarfilm ist unter folgendem Link einzusehen: https://www.youtube.com/watch?v=k-fJ2lQ1aok8.

Mai

Bundesratsantrag «Fernmeldeüberwachung: Personeller und finanzieller Mehrbedarf Dienst ÜPF und ISC-EJPD»
Das Programm Fernmeldeüberwachung (Programm FMÜ)* hat die Ablösung und Weiterentwicklung des Verarbeitungssystems des Dienstes ÜPF zum Ziel. Dieses Programm, welches 2015 initialisiert wurde, wird 2024 abgeschlossen. Dabei wird der Dienst ÜPF neue Komponenten sowie die damit verbundenen Aufgaben von der Programmorganisation übernehmen. Mit dem Antrag soll sichergestellt werden, dass der Dienst ÜPF über die dafür notwendigen Ressourcen verfügt. Der Antrag wurde am 4. Mai 2022 im Bundesrat besprochen und angenommen.

Revision der Ausführungsverordnungen (insb. Anpassungen betreffend 5G)
Am 23. Mai 2022 endete die Vernehmlassung zu den Teilrevisionen der vier Ausführungserlasse des BÜPF. Es sind dazu 68 Stellungnahmen beim Dienst ÜPF eingetroffen. Aufgrund der genannten Eingaben wurden die Entwürfe der Verordnungen angepasst.

Juni

Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus
Das Bundesgesetz über die polizeilichen Massnahmen zur Bekämpfung von Terrorismus (PMT) sieht verschiedene präventiv-polizeiliche Massnahmen vor. Es trat am 1. Juni 2022 in Kraft. Das Gesetz ändert unter anderem das BÜPF. Insbesondere wird ein neuer Überwachungstyp zur Mobilfunklokalisierung im Rahmen der genannten Massnahmen eingeführt.

Juli

Erster Newsletter des Dienstes ÜPF für Strafbehörden
Der erste Newsletter für Benutzerinnen und Benutzer des Verarbeitungssystems des Dienstes ÜPF wurde im Juli 2022 erstellt und veröffentlicht. Er enthält praktische Informationen zur täglichen Arbeit im Rahmen der Fernmeldeüberwachung. Der Newsletter soll zukünftig zirka zweimal im Jahr erscheinen.

* Mehr dazu unter www.li.admin.ch > Themen > Programm FMÜ

September

Vorbereitung der Reorganisation des Dienstes ÜPF
Der Dienst ÜPF wurde beauftragt, eine Reorganisation durchzuführen. Diese soll zu einer Optimierung der Aufgabenerfüllung innerhalb des heutigen organisationsrechtlichen Rahmens führen. Dazu fand eine Reihe von Workshops in der zweiten Hälfte 2022 statt. Die neue Organisation wird per 1. Mai 2023 umgesetzt.

Oktober

Kundenzufriedenheitsumfrage 2022
Alle zwei Jahre führt der Dienst ÜPF eine Kundenzufriedenheitsumfrage bei seinen Leistungsbezügern durch. Gemäss der Umfrage bleibt die Zufriedenheit hoch. Auf einer Skala von 1 (sehr unzufrieden) bis 6 (sehr zufrieden) wurden die folgenden Werte erreicht:

- Gesamtzufriedenheit Auswertende Behörden: Steigerung von **4.7** auf **4.9**
- Gesamtzufriedenheit Anordnende Behörden: Steigerung von **4.6** auf **4.9**
- Gesamtzufriedenheit Genehmigende Behörden: Rückgang von **5.7** auf **5.5**

Dezember

Verordnung über die Finanzierung der Überwachung des Post- und Fernmeldeverkehrs (FV-ÜPF): Ämterkonsultation beendet
Die Vorlage der Verordnung sieht die Einführung von Pauschalen vor. Damit soll das heutige Finanzierungs- und Rechnungsstellungssystem vereinfacht werden. Gleichzeitig soll der Kostendeckungsgrad beim Dienst ÜPF angehoben werden. Die Ämterkonsultation wurde am 28. November 2022 beendet. Es wird in der ersten Hälfte 2023 eine Vernehmlassung folgen. Das Inkrafttreten ist auf den 01. 01. 2024 vorgesehen.

02

HINTERGRUND

Mobil, flexibel und kompetent

Ein Team für besondere Einsätze

Kleine Anbieterinnen von Telekommunikationsdienstleistungen, zum Beispiel lokale WLAN- oder Kabelnetzbetreiber, können sich von der gesetzlich vorgeschriebenen Überwachungsbereitschaft befreien lassen. Kommt es in ihren Netzen zu verdächtigen Aktionen und liegt ein richterlich genehmigter Überwachungsbeschluss vor, übernimmt das Special Case Team des Dienstes ÜPF.

Eichenweg 3 in Zollikofen, Campus der Bundesverwaltung. Zwei Mitglieder des Special Case Teams beladen eine Reihe von Cargokisten mit Werkzeugen, Kabeln, Steckern und Elektronikkomponenten. Per Warenlift bringen sie das Material in die Anlieferung.

Der Teamleiter erwartet sie bereits. Unterdessen steht ein Minivan bereit. Nach der Beladung wird die Klebefolie mit dem Logo der Schweizerischen Eidgenossenschaft von der Wagentür gezogen und losgeht's. «Es muss niemand von weitem erkennen, dass wir kommen», meint der Mann am Steuer.

Sein Chef nimmt auf dem Beifahrersitz Platz. Er ist ein international anerkannter Spezialist auf dem Gebiet der *Lawful Interception* (LI), der gesetzeskonformen Fernmeldeüberwachung. Der studierte Computerwissenschaftler arbeitete für international tätige Telekommunikationsanbieterinnen und Netzbetreiberinnen. Nach einigen Engagements als externer LI-Experte heuerte er 2012 fest beim Dienst ÜPF an. Seit 2017 leitet er das Team.

Sein Spezialgebiet ist die Datenkonversion und darum geht es im Kern auch bei den Einsätzen des Special Case Teams: Die Umwandlung der lokal erworbenen Daten in die einschlägigen Standards des Europäischen Instituts für Telekommunikationsnormen (ETSI).

Im vergangenen Jahr fanden in der Schweiz rund 10 000 Überwachungsmassnahmen statt; die überwiegende Zahl in den Netzen der grossen FDA. Marktführer wie Swisscom, aber auch Sunrise oder Salt müssen von Gesetzes wegen in der Lage sein, Daten aus ihren Netzen auszuleiten und sie in den vorgeschriebenen Formaten auf das Verarbeitungssystem des Dienstes ÜPF zu transferieren.

Das BÜPF sieht Mitwirkungspflichtige mit aktiven Überwachungspflichten und solche mit lediglich einer Duldungspflicht vor. Dabei geht es hauptsächlich um die Verhältnismässigkeit. Mittlere und kleine Unternehmen, die nicht von vielen Überwachungsmassnahmen betroffen sind, sollen auch nicht die dazu notwendigen Investitionen tätigen müssen. Sie sind nicht verpflichtet, eigene LI-Kompetenzen aufzubauen: Sie müssen nur dulden, dass Überwachungen stattfinden. «Die eigentliche Arbeit, die Erstellung der Überwachungsbereitschaft übernimmt dann unser Special Case Team», erklärt Alexandre Suter, Leiter des Providermanagements beim Dienst ÜPF.

Er schätzt, dass schweizweit über 1000 Unternehmen von Spezialfällen betroffen sein können. Die Palette reicht vom Hotel, das seinen Gästen ein kostenloses WLAN offeriert, über den Internet-Accessprovider bis zu den Anbieterinnen von Smartphone-Apps.

Sind die juristischen Umstände geklärt, beginnt die Diskussion der technischen Umsetzung.

Seit das revidierte BÜPF im März 2018 rechtskräftig wurde, hat das Providermanagement bei rund 40 Unternehmen Special Case Aufträge durchgeführt. Und jedes Jahr geraten fünf bis zehn weitere Provider, beziehungsweise einzelne ihrer Kunden, ins Visier der Strafbehörden.

«Unsere Arbeit beginnt mit einem Anruf beim LI-Verantwortlichen der Anbieterin», erklärt der Teamleiter. Wenn der Kontakt steht, tauschen die Beteiligten über verschlüsselte E-Mails die kritischen Informationen zu Zielanschlüssen- und Geräten aus.

Sind die juristischen Umstände geklärt, beginnt im Special Case Team die Diskussion über die technische Umsetzung. Sie kann kurz sein – wenn schon einmal eine Überwachung stattgefunden hat – oder eben länger, wenn der betroffene Provider zum ersten Mal in einen Special Case involviert ist.

Abklärungsbedarf schafft vor allem die extreme Heterogenität der Telekommunikationsinfrastrukturen. Jeder Provider vertraut auf andere Soft- und Hardwarelieferanten. Ausserdem laufen vielerorts mehrere Systemgenerationen parallel. Das Team muss auf zahllose Kombinationen von Anschlusstypen, Steckverbindern und Protokollen vorbereitet sein. Der Teamleiter erinnert sich: «Einmal war eine Netzwerkkomponente, die wir unbedingt benötigten, nur noch in Spanien verfügbar».

Der Minivan hat das Ziel, ein Datacenter im Grossraum Zürich, erreicht. Ein Mitarbeiter schliesst auf. Draussen scheint die Sonne, drinnen blinkt es aus den Serverracks. Zusätzliches

Licht kommt von ein paar Deckenleuchten. Die Serverfarmen summen und die Kühlsysteme rauschen.

«Der Telefon- und Datenverkehr wird seit einigen Jahren praktisch ausnahmslos in der Cloud abgewickelt», erklärt der Teamleiter. Wenn für eine verdächtige Person eindeutige Adressierungselemente vorliegen, finden die Einsätze des Special Case Teams daher vorwiegend in Datencentern wie diesem statt. Aufs Land hinaus – etwa zu den Räumlichkeiten eines lokalen Kabelnetzbetreibers – führt der Weg nur, wenn technische Gründe die Nähe zur Zielperson erforderlich machen.

Das Team sucht sich einen Platz zwischen den Serverschränken und richtet sich ein. Die Grundausrüstung für die eigentliche Überwachungstätigkeit bringt das Special Case Team mit. Sie wird bei Herstellern beschafft, die auch die Strafbehörden und Nachrichtendienste anderer

Staaten beliefern. Mitunter stossen die Standardwerkzeuge jedoch an ihre Grenzen. Dann läuft die Operation zweigleisig:

Während ein Teil des Teams vor Ort die Überwachung einrichtet, entwickeln die Kollegen im Büro eine fallspezifische Softwarelösung. Sobald der Server online ist, starten sogenannte Konnektivitätstests. So können allfällige Softwareänderungen bis zur letzten Minute hochgeladen werden.

Softwareänderungen können bis zur letzten Minute hochgeladen werden.

Im Hintergrund hält sich ein Spezialist des Providers zur Verfügung. Er beantwortet Fragen, die im Verlauf des Einsatzes auftauchen. «Im Normalfall ist die Zusammenarbeit gut», meint der Teamleiter. Ausnahmen bestätigen die Regel: So kann es vorkommen, dass ein Provider gewissermassen passiven Widerstand leistet und die Mitarbeitenden des Dienstes ÜPF erst nach Absprache mit einem Anwalt gewähren lassen will. In ganz seltenen Fällen – wenn der Provider den physischen Zutritt zu seiner Infrastruktur verhindern will – ist das Providermanagement des Dienstes ÜPF gezwungen, die Unterstützung von Polizeikräften anzufordern.

Die Motive der renitenten Provider sind oft unklar. Anbieter, welche die Strafbehörden im Verdacht haben, den Zielpersonen nahe zu stehen, werden gar nicht erst kontaktiert. «In solchen Fällen steuern wir das Ziel über einen Umweg an», erklärt der Leiter des Special Cases Team. Was konkret passiert, wenn sich ein direkter Zugriff auf die Infrastruktur eines Providers verbietet, verrät er nicht. «Nur eines ist sicher: wir finden immer einen Weg.»

Special Case Einsätze zielen in der Regel auf Echtzeitüberwachungen ab. Für das Team heisst das: Der Job ist erst erledigt, wenn aktuelle Kommunikationsdaten unverzüglich und störungsfrei ans Verarbeitungssystem des Dienstes ÜPF übermittelt werden können.

Gegen 15.00 Uhr ist es so weit. Das Team räumt seine Ausrüstung zusammen und bringt sie zurück in den Minivan. Was beim Provider zurückbleibt, ist eine unscheinbare Box. Es ist der Special Case Server, der den Daten- und Sprachverkehr der verdächtigen Person ausleitet.

Ab jetzt sind die involvierten Ermittler und die verantwortliche Staatsanwaltschaft am Zug.

Der grosse Umbau

Die Echtzeitüberwachungskomponente des Verarbeitungssystems FMÜ soll ersetzt werden. Im Sommer 2021 begannen die Realisierungsarbeiten am Federal Lawful Interception Core Component (FLICC).

Wenn der leitende Staatsanwalt Urs Hubmann die Abkürzung IOK verwendet, meint er nicht das Internationale Olympische Komitee, sondern die Italienische Organisierte Kriminalität. «Sie ist im Moment eine der grossen Bedrohungen unserer inneren Sicherheit».

Der 65-jährige Jurist führt seit 2011 die Staatsanwaltschaft II (STA II) des Kantons Zürich. Sie befasst sich insbesondere mit dem, was die Fachwelt Holkriminalität nennt. Es wird nicht auf eine Anzeige hin ermittelt, sondern bei bestehender Verdachtslage. Das Ziel ist es, mittels geheimer Zwangsmassnahmen ein Beweisfundament zu schaffen, das es erlaubt, Tatverdächtige vor Gericht zu bringen.

«Die Italienische Organisierte Kriminalität ist eine der grossen Bedrohungen unserer inneren Sicherheit.»

Urs Hubmann, Leitender Staatsanwalt Kanton Zürich

Schwerer Raub, Drogen- und Menschenhandel

Im Fokus stehen Fälle von organisierter und schwerer Bandenkriminalität. Die Palette der Delikte reicht vom schweren Raub über qualifizierten Drogenhandel, Menschenhandel, schwere Fälle von Geldwäscherei bis zur qualifizierten Cyberkriminalität.

Bei der Untersuchung dieser Straftaten steht der STA II ein gut bestückter Werkzeugkasten zur Verfügung. Neben dem Einsatz von verdeckten Fahndern, der Analyse von Finanztransaktionen, der Platzierung von Mikrophonen und Kameras, enthält er auch die Lawful interception (LI), die rechtskonforme Überwachung des Fernmeldeverkehrs; sei es rückwirkend oder in Echtzeit.

Die Echtzeitüberwachung erlaubt es den Ermittlern zu verfolgen, wo sich die Zielperson bewegt und was sie gerade mit ihrem Gegenüber zu besprechen hat. 2022 führte die STA II des Kantons Zürich über 200 Echtzeitüberwachungen durch; das entspricht rund 20 Prozent des gesamtschweizerischen Aufkommens.

Technisch werden die Überwachungen über das Interception System Schweiz (ISS) abgewickelt, die Echtzeitkomponente des Verarbeitungssystems FMÜ des Dienstes ÜPF. «Die Plattform wurde 2013 angeschafft und ist in die Jahre gekommen», erklärt Ernesto Ruggiano. Er ist Projektleiter beim Dienst ÜPF und verantwortlich für die Ablösung des ISS durch die neue Federal Lawful Interception Core Component (FLICC). Das Projekt wurde vor fünf Jahren lanciert. Die Realisierungsphase begann im Sommer 2021.

Die STA II würde FLICC lieber heute als morgen in Betrieb haben. Der Hauptgrund ist die technische Entwicklung in der Telekommunikationsindustrie. Für die Überwachung des Fernmeldeverkehrs auf dem heutigen Stand der Technik – Stichwort Mobilfunkstandart 5G – ist das ISS schlicht nicht ausgelegt. «Die Auswertung einer einzigen Überwachungssession – zum Beispiel eines kurzen Telefonats – ist deshalb aufwendig und dauert lange», erklärt Urs Hubmann.

Dazu kommt ein geändertes Kommunikationsverhalten. Auch Kriminelle tauschen sehr viel Belangloses aus. Die Datenflut, mit der die Ermittler konfrontiert sind, ist enorm.

Die Echtzeitüberwachung von Sprachkommunikationen und Textnachrichten soll ab Mitte 2023 verfügbar sein. In der Folgezeit soll die Überwachung von Internetdaten und E-Mails integriert werden und schliesslich steht an, was man als Innenausbau bezeichnen könnte: die Integration von neuen fortgeschrittenen Funktionalitäten.

Visualisierung und automatische Transkription

Zu dieser zählt zum Beispiel eine übersichtliche Visualisierung der Überwachungsergebnisse. Oder eine automatische Transkription von Sprachnachrichten mit Übersetzungsoption. Oder die Auswertung von genaueren Lokalisierungen von überwachten Geräten. «Mit FLICC etablieren wir die Echtzeitüberwachung als modernes, einfach zu handhabendes und effizientes Ermittlungsinstrument», sagt Ernesto Ruggiano.

Zwischen 2016 und 2022 ging die Zahl der Echtzeitüberwachungen schweizweit von 2800 auf etwas über 1200 zurück. Die Abnahme ist nicht zuletzt darauf zurückzuführen, dass Verfahren, in denen das Beweismittel Echtzeitüberwachung eine Rolle spielt, immer komplexer werden und vermehrt Spezialwissen erfordern. Das soll sich mit FLICC ändern.

«Wir etablieren die Echtzeitüberwachung als modernes und effizientes Ermittlungsinstrument.»

Ernesto Ruggiano, Projektleiter FLICC, Dienst ÜPF

Ein hoher Fahndungsdruck – darin sind sich die Experten einig – hält die organisierte und schwere Bandenkriminalität davon ab, sich in der Gesellschaft festzusetzen. Eine konsequente Verfolgung der einschlägigen Straftaten verhindert insbesondere, dass die Banden ihre internen Konflikte in der Öffentlichkeit austragen und bei gewalttätigen Auseinandersetzungen auch Unbeteiligte zu Schaden kommen.

«Gewaltexzesse auf offener Strasse kennen wir bisher vor allem aus dem Ausland», sagt Hubmann, «wir müssen unbedingt dafür sorgen, dass das so bleibt».

«Die Schweiz ist ein lohnendes Ziel.»

Auf der Spur von Spionen, Terroristen und Cyberangreifern: Jürg Bühler ist stellvertretender Direktor des Nachrichtendienstes des Bundes.*

Sind Sie ein eifriger Zeitungsleser, Herr Bühler?
Ich persönlich nicht unbedingt. Aber grundsätzlich können alle von in- und ausländischen Zeitungen publizierten Inhalte Informationen enthalten, die für einen Nachrichtendienst aufschlussreich sind. Wir sprechen von sogenannten Open-Source-Informationen, die der NDB systematisch beschafft und auswertet. So erhalte ich einen guten Überblick über die wichtigsten Meldungen.

Aus welchen anderen Quellen schöpft der Nachrichtendienst des Bundes (NDB) seine Informationen?
Es gibt viele. So haben wir grundsätzlich die Möglichkeit, bei allen Verwaltungsstellen von Bund und Kantonen relevante Informationen zu erheben. Das gilt über die Zusammenarbeit mit den Kantonen auch für die Gemeinden.

Klingt immer noch nicht sehr aufregend …
Weiter arbeiten wir mit human intelligence, das heisst mit menschlichen Quellen, die von unseren Quellenführern angeworben werden. Diese pflegen den Kontakt zu Personen, die Zugang zu Informationen haben, die für die Auftragserfüllung des NDB wichtig sind. Die Quellenführer entsprechen durchaus dem Bild, das sich die Öffentlichkeit von einem ‹Geheimagenten› macht. Weitere Informationsquellen sind schliesslich die internationalen Partnerdienste und die Nachrichtendienststellen in den Kantonen.

Wie viele Quellenführer beschäftigt der NDB?
Darüber geben wir nur unseren Aufsichtsorganen Auskunft.

Das Gegenstück zur human intelligence ist die signal intelligence. Was darf man sich darunter vorstellen?
Das ist die Aufklärung von technisch erzeugten Signalen, in der Regel von Kommunikationseinrichtungen. Dazu zählt beispielsweise die Funkaufklärung von Signalen aus dem Ausland oder von Satelliten im Weltraum. Hinzu kommt auch die Kabelaufklärung: Wir haben unter gewissen Bedingungen die Möglichkeit, grenzüberschreitende Datenströme abzuhören und sie nach zu unseren gesetzlichen Aufträgen gehörigen Suchbegriffen auszuwerten; etwa nach bestimmten Namen, Projekten, oder fernmeldetechnischen Adressierungselementen wie Telefonnummern.

* Das Interview mit Jürg Bühler wurde im Dezember 2021 vor Ausbruch des Krieges in der Ukraine geführt.

Das führt uns zum Thema lawful interception (LI), beziehungsweise Dienst ÜPF. Wie wichtig ist Fernmeldeüberwachung für die Arbeit des Nachrichtendienstes?
Sie liefert uns Informationen, die sonst nicht erhältlich sind. Im Kalenderjahr 2022 führte der NDB zwei Operationen mit Einsatz von solchen genehmigungspflichtigen Beschaffungsmassnahmen durch. Je eine in den Bereichen Terrorabwehr und verbotene nachrichtendienstliche Tätigkeit.

Insgesamt fanden 2022 in der Schweiz gut 10 250 Fernmeldeüberwachungen statt. Davon hat der NDB 95 angeordnet. Warum so wenig?
Die gesetzlichen Anforderungen für den Einsatz von Überwachungsmassnahmen sind für den NDB sehr streng. Für eine LI-Massnahme muss der NDB einen Antrag beim Bundesverwaltungsgericht stellen. Wenn dieses die Massnahme genehmigt, brauchen wir eine Freigabe der Vorsteherin VBS, die zuvor die Stellungnahmen der Vorstehenden des EDA und des EJPD einholen muss. Erst nach der Freigabe dürfen wir die Massnahme starten.

Einer der Gründerväter des Dienstes ÜPF

Jürg Bühler ist seit der Gründung des Nachrichtendienstes des Bundes (NDB) im Jahr 2010 Mitglied der Geschäftsleitung. Seine polizeiliche und nachrichtendienstliche Tätigkeit im Dienst der Eidgenossenschaft reicht indes bis in die 1990er-Jahre zurück. Er hat noch miterlebt, wie der Fernmeldeverkehr zu Zeiten des PTT-Monopols überwacht wurde; damals noch separat in den regionalen Fernmeldekreisdirektionen: «Das machten damals meist dafür spezialisierte Frauen, die mit Kopfhörern mithörten und die relevanten Gespräche protokollierten». Die Liberalisierung der Telekommunikationsindustrie stellte den Gesetzgeber vor eine doppelte Herausforderung: Erstens hatte er die Überwachungspflichten der nunmehr privaten Anbieter zu bestimmen, zweitens musste er für die hoheitliche Aufgabe der Fernmeldeüberwachung einen anbieterneutralen Dienst schaffen. Der heute 58-jährige Bühler war damals Leiter der gerichtspolizeilichen Ermittlungen bei der Bundespolizei: «In einer nationalen Arbeitsgruppe erarbeiteten wir zusammen mit dem Rechtsdienst der Telecom-PTT Vorschläge für einen vom Bund betriebenen Überwachungsdienst». Das Resultat war der Dienst für besondere Aufgaben (DBA), der am 1. Januar 1998 seine Arbeit aufnahm. Genau zehn Jahre später wechselte der DBA vom UVEK ins EJPD. Seitdem firmiert er unter dem heutigen Namen Dienst ÜPF.

«Qualifizierte Cyberangriffe erfolgen fast ausnahmslos grenzüberschreitend.»

Jürg Bühler, stellvertretender Direktor NDB

Selbst wenn der Verdacht besteht, dass die nationale Sicherheit der Schweiz gefährdet ist?
Das ist ohnehin eine Bedingung, die erfüllt sein muss, damit wir solche Massnahmen anwenden können. Im Zuge der Aufarbeitung des sogenannten Fichenskandals in den 1990er-Jahren beschränkte der Gesetzgeber den Handlungsspielraum des damaligen Nachrichtendienstes im Inland bewusst. Bis zum Inkrafttreten des Nachrichtendienstgesetzes im September 2017 war uns die Fernmeldeüberwachung im Inland untersagt. Seither nutzen wir diese Möglichkeit. Allerdings in weit geringerem Ausmass als damals die Gegner des Gesetzes befürchteten. Das belegen die Statistiken, die wir jährlich veröffentlichen.

Zu den zentralen Aufgaben des NDB gehört die Spionageabwehr. Wer spioniert in der Schweiz?
Wir schätzen die Zahl der ausländischen Geheimdienstmitarbeitenden, die sich dauerhaft in der Schweiz aufhalten, auf mehrere Tausend. In den diplomatischen Vertretungen gewisser Länder – Namen will ich keine nennen – ist rund ein Viertel der Mitarbeitenden mit nachrichtendienstlichen Aufgaben betraut.

Ist die Schweiz so wichtig für fremde Mächte?
Die Schweiz ist eine Hightech-Nation und insofern ein lohnendes Ziel für Wirtschaftsspionage. Dazu kommt, dass Genf eine Vielzahl von UN-Einrichtungen beherbergt. Wir tragen als Sitzstaat internationaler Organisationen eine Verantwortung, politische Spionageaktivitäten gegen Dritte auf unserem Staatsgebiet zu verhindern. Das heisst: Der NDB sammelt und bewertet auch Informationen, die darauf schliessen lassen, dass eine Regierung in der Schweiz gegen Nichtregierungsorganisationen, ethnische Minderheiten oder Oppositionsgruppen agiert.

Kommen wir zur Terrorabwehr, die im vergangenen Jahr drei von vier Massnahmen zur Fernmeldeüberwachung nötig machte. Wo liegt der Fokus des NDB?
Im Moment beim «Islamischen Staat».

Von welcher Personengruppe geht die Gefahr aus?
In der Schweiz geht die Bedrohung zum einen von hier radikalisierten Personen aus, die von der dschihadistischen Propaganda und durch Kontakte im persönlichen Umfeld inspiriert worden sind; zum anderen zunehmend auch von Personen, bei denen sich Radikalisierung und Gewaltorientierung mit persönlichen Krisen oder psychischen Problemen verbinden. Beide Gruppen können spontane Anschläge, vorwiegend auf

weiche Ziele, verüben. Gefährlicher sind aus dem Ausland einreisende Terroristen, die Aufträge für gezielte Anschläge haben. Wir sehen, dass diese beiden Gruppen teilweise kooperieren: Die Zugereisten rekrutieren die inländischen Laien und versuchen sie zu schulen.

Die in der Öffentlichkeit präsenteste Form der Bedrohung unserer nationalen Sicherheit sind wohl Cyberattacken auf öffentliche Einrichtungen wie die Spitäler oder die Stromversorgung. Decken sich Ihre Erkenntnisse mit dieser Einschätzung?
Die Zahl der computergestützten Angriffe auf militärische und zivile Ziele nimmt weltweit stetig zu. Sie stellen auch für die Schweiz mit ihrer hochgradig digitalisierten Infrastruktur eine erhebliche Bedrohung dar.

Ist der NDB auf diese Bedrohung aus dem Cyberspace vorbereitet?
Unser Bereich Cyber hat den Auftrag, Angriffe auf Computersysteme kritischer Infrastrukturen frühzeitig zu erkennen und zu verhindern. Man muss allerdings sehen, dass die gesetzliche Grundlage unserer Aktivitäten vor mehr als fünf Jahren in Kraft trat. In den parlamentarischen Beratungen im Vorfeld der Volksabstimmung vom Herbst 2016 schien die Gefahr aus dem Cyberspace noch überschaubar. Parlament und Volk räumten dem Schutz der Privatsphäre eine hohe Priorität ein. Deshalb müssen wir vor der Überwachung verdächtiger Aktivitäten – sei es mittels GovWare oder über den Dienst ÜPF – aufzeigen können, dass die nationale Sicherheit direkt und schwerwiegend bedroht ist. Genau das bereitet aber Schwierigkeiten.

Warum?
Weil qualifizierte Angriffe fast ausnahmslos grenzüberschreitend erfolgen. Die letzte Station eines Cyberangriffs liegt praktisch immer jenseits der Landesgrenzen. Das heisst: Cyberangriffe, für welche Infrastrukturen in der Schweiz missbraucht werden, sind gegen Einrichtungen im Ausland gerichtet. Damit stellen sie keine direkte Bedrohung der Schweiz im Sinne des Gesetzes dar. Ihre Aufklärung ist aus Sicht der Abwehr aber dennoch wichtig, um die Schweiz vor Angriffen schützen zu können.

Wie halten es die Nachrichtendienste unserer Nachbarländer mit grenzüberschreitenden Attacken?
Wir sind umgeben von Rechtsstaaten. Auch dort ist der Begriff der «nationalen Bedrohung» vergleichsweise eng gefasst. Das führt dazu, dass auch diese teilweise keine rechtlichen Grundlagen haben, allfällige Angriffsvorbereitungen auf Ziele in der Schweiz aufzuklären und zu vereiteln. Es handelt sich um ein strukturelles Problem, das Angreifer gezielt ausnützen können. Es muss daher sowohl auf nationaler als auch auf internationaler Ebene angegangen werden.

Hat die Schweiz schon entsprechende Schritte unternommen?
Das Nachrichtendienstgesetz wird zurzeit revidiert. Es ist vorgesehen, auch die Bedrohung von wichtigen internationalen Sicherheitsinteressen als Grund für den Einsatz von genehmigungspflichtigen Beschaffungsmassnahmen zuzulassen. Das würde auch die Möglichkeiten im Cyberbereich erweitern.

03

ZAHLEN UND FAKTEN

Gründe für Überwachungen

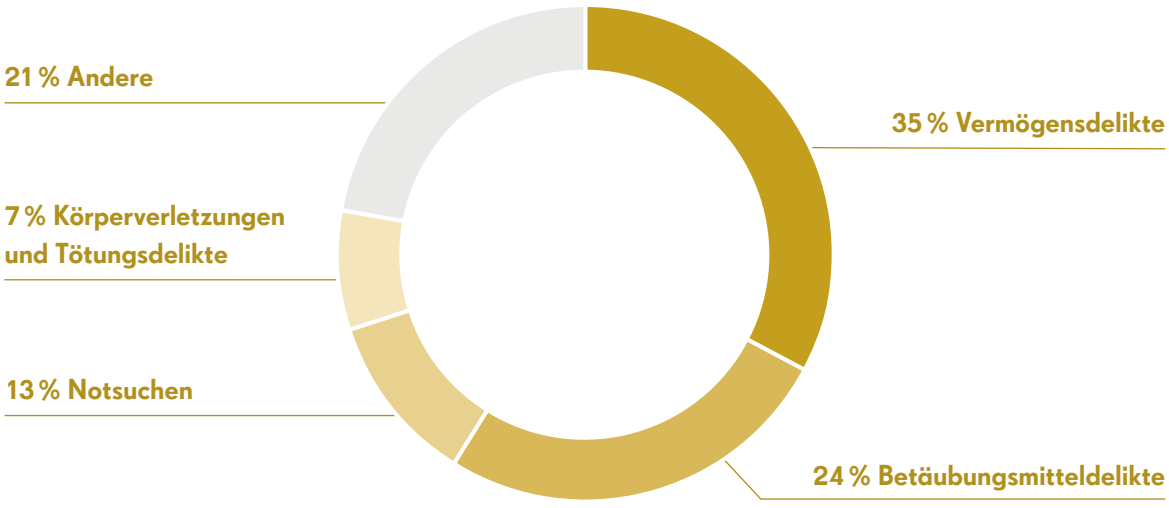
Gemäss polizeilicher Kriminalstatistik wurden 2022 in der Schweiz 549 404 Delikte gemeldet. Bei deren Verfolgung kam die Ermittlungsmassnahme Fernmeldeüberwachung mit 10 253 Überwachungen vergleichsweise selten zum Einsatz.

Es ist noch zu beachten, dass auf ein Delikt beziehungsweise eine genehmigungspflichtige Beschaffungsmassnahme mehrere Überwachungsanordnungen entfallen können. So können zum Beispiel sowohl der Festnetzanschluss als auch mehrere Mobiltelefone einer mutmasslichen Täterschaft überwacht werden. Weiter wird häufig dieselbe Mobiltelefonnummer bei verschiedenen Mitwirkungspflichten zur Überwachung in Auftrag gegeben, um sämtliche Roaming-Fälle abdecken zu können. Die Anzahl der von Überwachungsmassnahmen direkt betroffenen Personen liegt demnach merklich tiefer als die Anzahl der angeordneten Überwachungsmassnahmen.

Am häufigsten wurden Überwachungen in Verbindung mit Vermögensdelikten vorgenommen (35 Prozent). Mit 24 Prozent auf Platz zwei folgen die Verbrechen gegen das Betäubungsmittelgesetz. Auf dem vierten Rang (7 Prozent) liegen die Anordnungen wegen strafbarer Handlungen gegen Leib und Leben.

Eine Fernmeldeüberwachung kann auch bei der Suche nach vermissten Personen angeordnet werden. Die sogenannten Notsuchen stehen mit 13 Prozent auf Rang drei.

Weiterführende Informationen zu unseren Statistiken finden Sie unter:
www.li.admin.ch/stats



Definition und Anzahl an Überwachungsmassnahmen und Auskunftstypen

Echtzeitüberwachung (1)
Bei einer Echtzeitüberwachung werden die Post- oder Fernmeldeverkehrsdaten simultan, leicht verzögert oder wiederkehrend über das Verarbeitungssystem an die Strafverfolgungsbehörden übertragen.

Rückwirkende Überwachung (2)
Bei einer rückwirkenden Überwachung werden vor allem Verbindungsnachweise erhoben. Beantwortet wird zum Beispiel die Frage, wer mit wem, wann, wo und wie lange telefoniert hat.

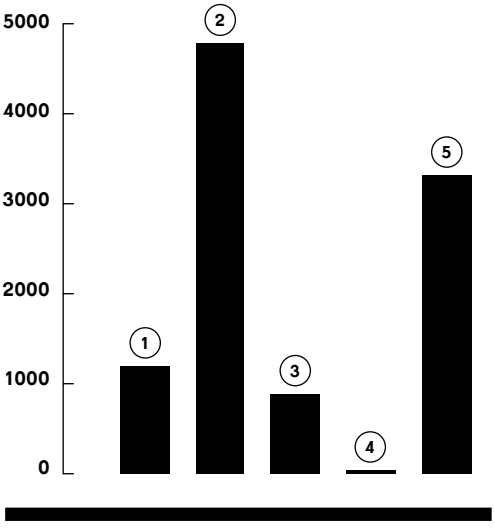
Notsuche (3)
Eine Notsuche wird etwa angeordnet, um verunfallte Wanderer oder verschwundene Kinder zu finden und zu retten.

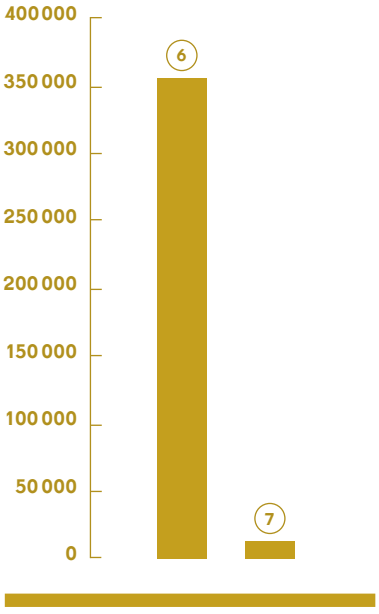
Fahndung (4)
Im Rahmen einer Fahndung können die Strafbehörden Personen aufspüren, gegen die in einem rechtskräftigen und vollstreckbaren Entscheid eine Freiheitsstrafe verhängt oder eine freiheitsentziehende Massnahme angeordnet wurde.

Antennensuchlauf (5)
Bei einem Antennensuchlauf interessiert eine Mobilfunkzelle beziehungsweise ein öffentlicher WLAN-Zugangspunkt. Erfasst werden alle angefallenen Kommunikationen, Kommunikationsversuche und Netzzugänge innerhalb einer bestimmten Periode.

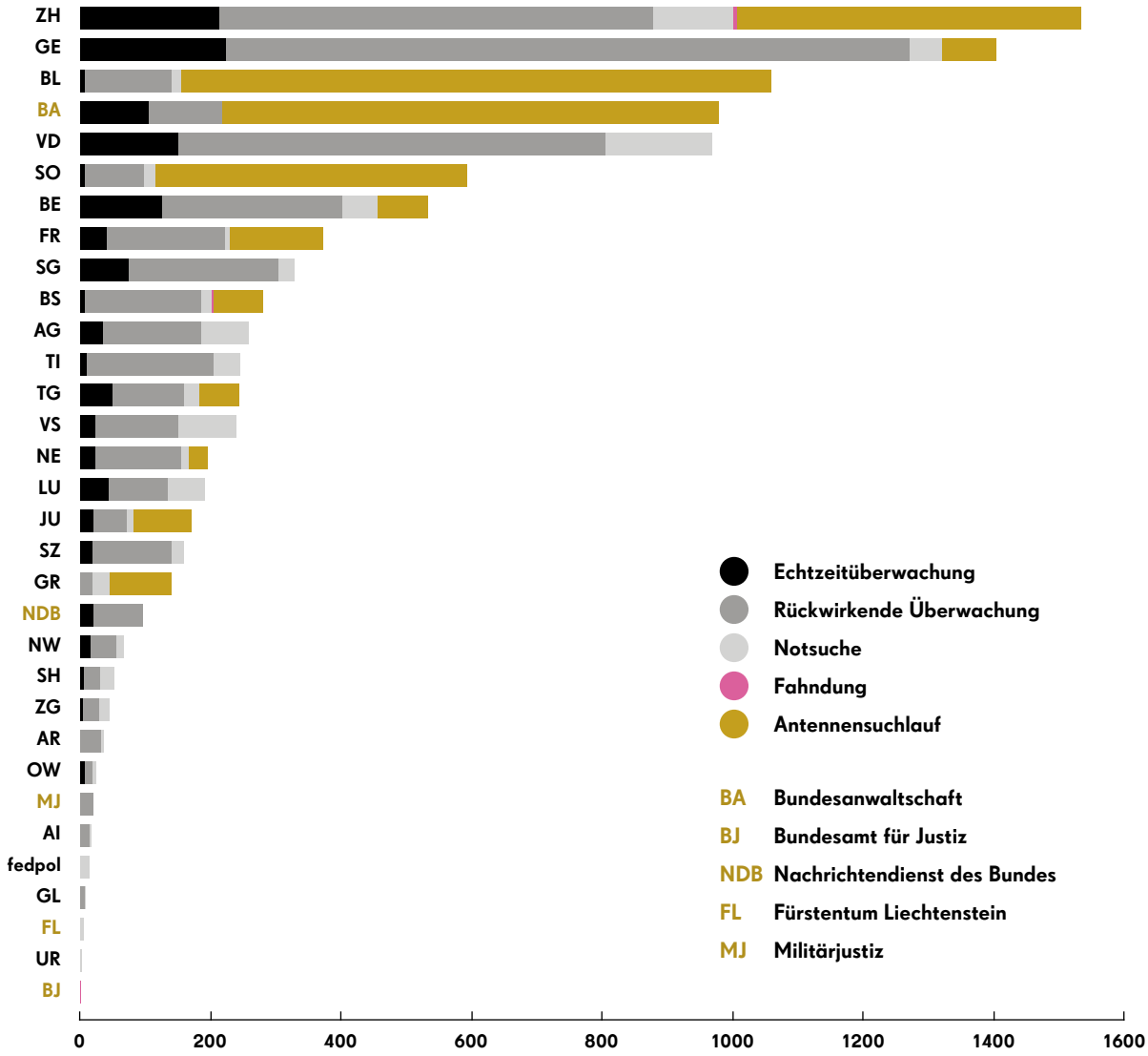
Einfache Auskünfte (6)
Einfache Auskünfte liefern die Grundinformationen zu Fernmeldeanschlüssen; insbesondere, welchem Abonnenten eine bestimmte Telefonnummer oder IP-Adresse zugeordnet ist.

Komplexe Auskünfte (7)
Komplexe Auskünfte liefern weitergehende Informationen zu Fernmeldeanschlüssen, zum Beispiel zugehörige Vertrags- oder Ausweiskopien.





Aufträge nach Bund, Kantonen und Liechtenstein

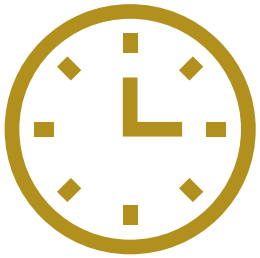


Überwachungsaufträge des Bundesamtes für Justiz
Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sieht Überwachungen nicht nur für Strafverfahren, die im Inland laufen, vor. Entsprechende Massnahmen können auch beim Vollzug eines von ausländischen Behörden eingereichten Rechtshilfeersuchens durchgeführt werden. In Auslieferungs- und anderen Rechtshilfefällen ist das Bundesamt für Justiz (BJ) zuständig.

Anzahl Bürgeranfragen

24

Geleistete Piketteinsätze



870

Registrierte Benutzer Verarbeitungssystem

WMC 2400
Warrant Management Component (Auftragsmanagement)

IRC 4300
Information Request Component (Auskünfte)

RDC 2200
Retained Data Component (rückwirkende Überwachungen)

ISS 2450
Interception System Schweiz (Echtzeitüberwachungen)

Anzahl Spezialfälle

83

(siehe S. 8 / 9, «Dienst ÜPF in Kürze», Providermanagement sowie S. 15 – 19, «Ein Team für besondere Einsätze»)

Anzahl Medienanfragen

21

Erfolgsrechnung Dienst ÜPF in Millionen CHF

Gesamtertrag
12,4

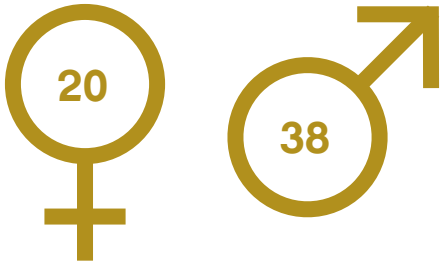
Gesamtaufwand
31,7

Deckungsbeitrag Bund
19,3

Anzahl Mitarbeitende

58

Frauen- und Männeranteil



Alter im Durchschnitt

46,5

Verteilung nach Sprachen

67 % Deutsch

6,4 % Italienisch

24,5 % Französisch

2,1 % Andere

Aufteilung nach Alter

20 bis 29 Jahre
10 %

30 bis 39 Jahre
19 %

40 bis 49 Jahre
26 %

50 bis 59 Jahre
40 %

60 bis 69 Jahre
5 %

«Die eigentliche Arbeit, die Erstellung der Überwachungs-bereitschaft, übernimmt unser Special Case Team.»

Alexandre Suter, Leiter des Bereichs Providermanagement des Dienstes ÜPF

Impressum

Redaktion: Dienst ÜPF
Mitarbeit: JNB Journalistenbüro, Luzern
Realisation: Schön & Berger, Zürich
Druck: Druckerei Ruch, Ittigen
Fotos: Lia Lüthi, Barbara Hesse, David Kelly
Schrift: Minion Pro, Drescher Grotesk
Papier: Z-Offset
Sprachversionen: Deutsch,
Französisch, Italienisch und Englisch

■

Der besseren Lesbarkeit und der allgemeinen Verständlichkeit zuliebe haben wir darauf verzichtet, zu detailliert in die Terminologie der Technologie und der Jurisprudenz abzutauchen. Wo immer möglich wurden geschlechtsneutrale Formen verwendet. Wo personenbezogene Bezeichnungen nur in männlicher oder weiblicher Form angeführt sind, beziehen sie sich auf Männer und Frauen in gleicher Weise.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Dienst Überwachung Post- und Fernmeldeverkehr ÜPF
3003 Bern