Staatliche Überwachungsmethoden - Honeypots und andere Tricks

5. Dezember 2013

Von Heiner Busch, WOZ

Wie kommen Polizei und Geheimdienste zu ihren Informationen? Ein unvollständiger Überblick über die heutige Praxis und geplante Gesetzesänderungen.

In den neunziger Jahren begann für Polizei und Staatsschutz in der Schweiz das Zeitalter der Datenbanken. Diese erleichtern das Auswerten und Zusammenführen von Informationen; Onlineverbindungen erlauben den schnellen Abruf von Daten aus Registern anderer Verwaltungen. Möglich ist auch der Abgleich grösserer Datenmengen. Schon Ende der siebziger Jahre entwickelte die deutsche Polizei auf der Suche nach konspirativen Wohnungen der Rote-Armee-Fraktion (RAF) die Methode der Rasterfahndung. Dabei werden Datenbestände anhand eines Profils so lange gegeneinander abgeglichen, bis ein «Bodensatz» von Personen übrig bleibt, die zwar unverdächtig sind, aber dem Merkmalsraster entsprechen und dann nach herkömmlichen Methoden überprüft werden. Bei der letzten grossen Rasterfahndung, die im Herbst 2001 begann, suchte die deutsche Polizei nach Schläfern von al-Kaida. Sie glich dabei Millionen von Daten aus Ausländer- und Melderegistern, von Hochschulen, Fluggesellschaften und technischen Instituten miteinander ab - erfolglos.

Denunzieren und spitzeln

Zu den traditionellen Ressourcen von Geheimdiensten und Polizeien (vor allem den politischen) gehört seit je das Spitzelwesen: Da ist zunächst der (gelegentliche) Informant, im angelsächsischen Jargon manchmal auch «walk-in» genannt, weil er in die Dienststelle hineinläuft und seine Informationen anbietet. Der Übergang vom Informanten zum V-Mann (oder zur V-Frau) ist fliessend. Auch V-Leute sind Privatpersonen, ihre Zusammenarbeit mit der Polizei ist allerdings fester: Sie liefern nicht nur hier und da Informationen, sondern erhalten Aufträge zur Informationsbeschaffung und gleichzeitig die Zusage, dass man ihre Identität nach aussen, auch gegenüber Gerichten, geheim hält. Sie haben einen festen Ansprechpartner in der Behörde. Rekrutiert werden sie in der Szene, die sie ausforschen sollen. V steht zwar für «Vertrauen». «Vorsicht» wäre besser, denn V-Leute verfolgen in der Regel eigene Interessen. Einigen geht es darum, selbst von der Strafverfolgung verschont zu werden, anderen schlicht ums Geld. Das deutsche Bundesamt für Verfassungsschutz zahlte 2010 insgesamt rund 2,5 Millionen Euro Honorar an seine V-Leute.

Wie viel der schweizerische Nachrichtendienst des Bundes (NDB) seinen V-Leuten zahlt, ist nicht bekannt. Das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, das Staatsschutzgesetz also, erlaubt dem NDB seit Ende 2011 den Einsatz privater Spitzel und die Ausstellung von «Tarnidentitäten» für sie. Eine gesetzliche Grundlage für den Einsatz von V-Leuten im Strafverfahren gibt es bisher nicht. Das Bundesgericht hat aber 1998 ihre Behandlung als anonyme ZeugInnen für rechtens erklärt. Die hauptamtlichen Spitzel des NDB werden im Gesetz einfach als «Mitarbeiter» bezeichnet, bei der Polizei spricht man von

verdeckten Ermittlern. Sie nehmen unter einer Legende, also mit amtlich gefälschten Papieren, am Rechtsverkehr teil. Auch für deren grenzüberschreitenden Einsatz gibt es vertragliche Regelungen. Wenn V-Leute oder verdeckte Ermittler zu Straftaten anstiften, spricht man von Agents Provocateurs.

Spähen und lauschen

Die Videoüberwachung im öffentlichen Raum hat in den vergangenen Jahren stark zugenommen. Sie ist, insbesondere bei Veranstaltungen und Demonstrationen, mittlerweile in vielen kantonalen Polizeigesetzen verankert. Wenn Kameras ein ganzes Gebiet abdecken und die durchgehende Beobachtung einer Person erlauben, spricht man von Closed Circuit Television (CCTV). Eine solche Anlage ist derzeit im Genfer Quartier Pâquis geplant. Der Staatsschutz ist gemäss Art. 14 BWIS ebenfalls zum «Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen» ermächtigt.

Observationen sind langfristig angelegte, verdeckte und gezielte Beobachtungen einer Person im öffentlich zugänglichen Raum, wozu auch Geschäfts-, Betriebs- und Arbeitsräume gehören können. Es operieren meist spezielle Teams, zu deren Repertoire auch der Einsatz technischer Mittel - Peilgeräte, Videokameras, Richtmikrofone - gehört.

Bei strafrechtlichen Ermittlungsverfahren sind Lausch- und Spähangriffe in Privatwohnungen in der Schweiz seit Ende der siebziger Jahre erlaubt. Der NDB soll diese Befugnis nun mit dem Nachrichtendienstgesetz erhalten, für das der Bundesrat demnächst die Botschaft vorlegen wird.

Abhören, mitlesen und orten

Parallel zur Entwicklung der Kommunikationstechnik hat sich auch deren Überwachung fortentwickelt. Die Postüberwachung kommt heute nur noch selten vor. Noch Anfang der neunziger Jahre klagten Polizeibehörden, dass Mobiltelefone nicht abhörbar seien. Heute machen Handyüberwachungen den Löwenanteil der Telekommunikationsüberwachungen aus. Die E-Mail-Überwachung wird in der Schweiz seit etwa zehn Jahren praktiziert, ihr Anteil an der Gesamtzahl der Überwachungen ist aber noch vergleichsweise niedrig.

Seit 1998 sind neben der aus der PTT hervorgegangenen Swisscom auch die neuen privaten Anbieter, einschliesslich der Internetprovider, verpflichtet, auf Anordnung der Strafverfolgungsbehörden die Überwachung zu ermöglichen. Ein Zwangsmassnahmengericht muss die Anordnung genehmigen.

Gemäss der Strafprozessordnung bedarf es dafür eines dringenden Verdachts, dass der oder die Beschuldigte eine Straftat aus einem Katalog von rund hundert Delikten begangen hat. Die Überwachung der Telekommunikation ist bisher nur im Rahmen strafrechtlicher Ermittlungen erlaubt, mit dem Nachrichtendienstgesetz soll diese auch präventiv möglich werden. Den praktischen Ablauf regeln das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) sowie technische Richtlinien.

Überwacht werden aber nicht nur die Inhalte der Kommunikation. Das polizeiliche Interesse gilt zunehmend den Randdaten - auch Verkehrs- und Verbindungsdaten genannt -, die bei der Telekommunikation automatisch anfallen. Wer hat mit wem telefoniert? Wer hat wem eine SMS oder eine E-Mail geschickt? Die Auswertung solcher Daten gibt Aufschluss über Beziehungsnetze. Da jedes Handy sich automatisch bei der nächstgelegenen Funkzelle

einloggt, liefert die mobile Kommunikation auch Daten über den Standort, von dem aus telefoniert wurde, und erlaubt damit auch die Erstellung von Bewegungsprofilen. Die Provider sind verpflichtet, diese Daten ein halbes Jahr lang zu speichern und auf Anordnung an die Strafverfolgungsbehörden herauszurücken (Vorratsdatenspeicherung). Mit der Revision des Büpf soll die Speicherungsdauer auf ein Jahr verlängert werden.

Die Mobilfunktechnik hat auch eine ganze Reihe neuer Überwachungsmethoden eröffnet - hier ein paar Beispiele: Bei der Funkzellenabfrage - auch Antennensuchlauf genannt - wird festgestellt, welche Handys zu einem bestimmten Zeitpunkt im Bereich einer Funkzelle eingeschaltet waren. 2011 wurde diese Methode in der Schweiz 218-mal angewandt.

Der IMSI-Catcher ist ein Gerät, das problemlos in einem Personenwagen verstaut werden kann und eine Funkzelle simuliert. Die im Umkreis befindlichen (eingeschalteten) Mobiltelefone loggen sich hier ein und «verraten» damit die International Mobile Subscriber Identity (IMSI), eine Nummer, die auf der SIM-Karte gespeichert ist. Da seit 2004 auch Prepaidhandys registriert werden müssen, ist damit in der Regel auch die Identität des oder der TelefoninhaberIn bekannt. Parallel zur Revision des Büpf will das Eidgenössische Justiz- und Polizeidepartement in der Strafprozessordnung eine gesetzliche Grundlage für den Einsatz dieses Geräts schaffen.

Eine stille SMS ist eine Form der Handyortung. Anders als eine normale SMS wird sie aber nicht auf dem Display des Handys angezeigt und produziert auch beim Eingang kein akustisches Signal, dafür aber Verbindungs- und natürlich Standortdaten des/der EmpfängerIn, die die Polizei bei den Providern abgreift.

Surfen und Fallen stellen

Schwierigkeiten hat die Polizei heute noch bei der Überwachung von verschlüsselten E-Mails oder von Internettelefoniediensten wie Skype. In beiden Fällen findet nämlich die Verschlüsselung auf dem sendenden und die Entschlüsselung erst auf dem empfangenden Computer statt. Beim Provider fällt nur ein Wust unlesbarer Zeichen an. Mittels Trojanern, also Schadsoftware, kann auf den zu überwachenden Computer zugegriffen und die Kommunikation vor der Verschlüsselung angezapft werden. Die Rechtsgrundlage hierfür will das Eidgenössische Justiz- und Polizeidepartement in der Strafprozessordnung festschreiben. Mit Trojanern kann aber nicht nur verschlüsselte Kommunikation angezapft, sondern der gesamte Computer ausspioniert werden. Diese Lizenz möchte der Bundesrat dem NDB im neuen Nachrichtendienstgesetz geben.

Nur naive Menschen halten das Internet für einen Raum der freien Kommunikation. Tatsächlich haben sich die Möglichkeiten der Überwachung durch das weltweite Netz potenziert. Das beginnt bei der Auswertung offener Quellen, die nur scheinbar ungefährlich ist: Schon mit gewöhnlichen Suchmaschinen lassen sich detaillierte Informationen über Personen sammeln. Behörden und zunehmend auch private Sicherheitsfirmen verwenden spezielle Suchmaschinen und durchkämmen auch Chaträume, Foren, soziale Netzwerke, Filesharing-Dienste und das Usenet.

Polizei und Geheimdienste betreiben aber nicht nur eine passive Beobachtung, sondern auch verdeckte Ermittlungen im Netz: Die Polizei verschweigt nicht nur einfach, dass sie die Polizei ist, sie präsentiert sich als Interessent einer verbotenen Ware, als Erwachsener, der sexuellen Kontakt mit Minderjährigen sucht, oder als Mitglied einer politischen Szene. Weil die 2011 in Kraft getretene schweizerische Strafprozessordnung solche verdeckten Ermittlungen ohne vorherigen konkreten Verdacht nicht mehr zuliess, haben die meisten Kantone nun

entsprechende Bestimmungen in ihren Polizeigesetzen erlassen. Dabei geht es keineswegs nur um die Suche nach Pädophilen, die in der öffentlichen Diskussion in den Vordergrund gerückt wurde.

Nicht bekannt ist, ob schweizerische Polizeibehörden dabei auch Honeypots auslegen, das heisst Leute auf eine Website locken, die die IP-Adressen der zugreifenden Computer speichert. Wie das funktioniert, demonstrierte das deutsche Bundeskriminalamt (BKA) im Zuge seiner Ermittlungen gegen die «Militante Gruppe» (MG): Zwei BKA-Beamte beteiligten sich 2004 als «die zwei von der Muppet Show» an der Militanzdebatte des Berliner Szeneblatts «Interim». Die LeserInnen wurden aufgefordert, die Spezialseite zum MG-Verfahren auf der BKA-Website zu besuchen. Über 400 IP-Adressen wurden erfasst, in 210 Fällen lieferte die Deutsche Telekom die Daten der NutzerInnen.

Elektronisch staubsaugen

Nicht nur die US-amerikanische NSA und ihr britisches Pendant GCHQ bedienen sich grosser Parabolantennen, um die über Satelliten vermittelte internationale Telekommunikation abzufangen und nach Suchwörtern zu durchkämmen. Auch der NDB befleissigt sich dieser hierzulande Funkaufklärung genannten Methode. Die grossen Ohren stehen in Leuk VS und Heimenschwand BE, die Zentrale des Onyx-Systems in Zimmerwald BE.

Die Bedeutung der satellitengestützten Kommunikation hat in den letzten fünfzehn Jahren abgenommen. Vor allem der Internetverkehr verläuft heute über ein weltumspannendes Netz von Glasfaserkabeln. Mit dem neuen Nachrichtendienstgesetz soll auch der NDB das Recht zur «Kabelaufklärung» erhalten.