

Sie sind **durchschaut**

Neue Observationstechniken perfektionieren die **Überwachung durch Staat und Polizei**. Erste Geräte zur Gegenwehr gibt es auch schon.

VON ROMAN GOERGEN

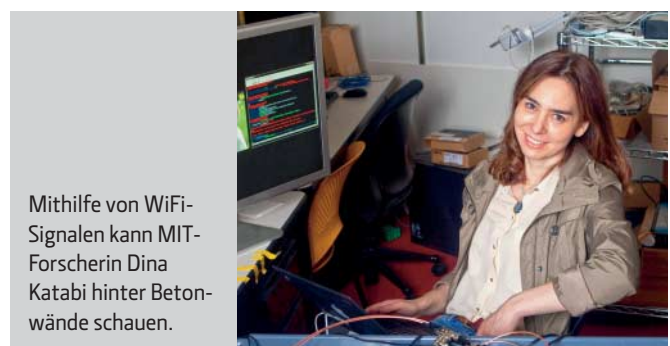
Im Kampf gegen Verbrechen und Terror sind moderne Observationstechnologien längst nicht mehr wegzudenken. Schon seit Jahrzehnten kommen etwa konventionelle Kameras überall auf der Welt in CCTV-Systemen (Closed Circuit Television) zur Beobachtung öffentlicher Plätze, Straßen und Bahnhöfe zum Einsatz. Doch sie können nur das Offensichtliche aufzeichnen. Sie enthüllen weder, was Menschen untereinander bereden, noch was sich in abgeschlossenen Räumen abspielt. Deshalb suchen Ermittler nach neuen Techniken, um diese Grenzen zu überwinden.

Je umfassender und ausgefeilter jedoch die technischen Möglichkeiten der Überwachung, desto größer auch die Sorge, dass die allgegenwärtige Observation Bürgerrechte zu sehr einschränkt, besonders das Recht auf Privatsphäre. Juristen kämpfen dagegen, Hacker bieten bereits erste Werkzeugkästen an, um der staatlichen Überwachung zu entgehen. Im 21. Jahrhundert zeichnet sich also ein neues Wettrüsten ab – zwischen Überwachern und Überwachten. Ein Überblick.

spielsweise Personen darin, entsteht ein Schattenbild ihrer Silhouette, das ein Algorithmus nach und nach rekonstruiert. Da Skelette und Bewegungsmuster sehr individuell sind, hoffen die MIT-Forscher, so eines Tages die Identität von Menschen feststellen zu können, „Silhouetten-Fingerabdruck“ nennen sie das.

Das Gerät soll in diesem Jahr auf den Markt kommen, zum Preis von 250 bis 300 US-Dollar. Zunächst ist die Technik vor allem für zivile Zwecke gedacht. So soll Emerald helfen, Alarm zu schlagen, wenn alte Menschen oder Babys in einem anderen Zimmer stürzen. Außerdem kann das Gerät die Funktionen eines Smart Homes erweitern, indem es feststellt, wo sich Hausbewohner aufhalten. Die App, die mit Emerald verbunden ist, kann dann das Licht ausschalten oder die Temperatur des Thermostaten ändern. Dass die Technik später auch im Sicherheitsbereich Verwendung finden wird, liegt für die Entwickler nahe. Bei Geiselnahmen könnte sie der Polizei zum Beispiel wertvolle Vorabinformationen liefern. „Niemand will ein Einsatzkommando in eine Situation schicken, in der keiner weiß, wo die Geiseln und wo die Geiselnnehmer sind“, sagt Katabi.

Durch Hausmauern sehen



Mithilfe von WiFi-Signalen kann MIT-Forscherin Dina Katabi hinter Betonwände schauen.

Foto: John D. & Catherine T. MacArthur Foundation

Die Ankündigung klingt nach Science-Fiction: „Wir demonstrieren hier, wie unser Gerät Personen hinter Hausmauern mithilfe von WiFi verfolgen kann“, sagt Dina Katabi, Leiterin des Projekts Emerald am Wireless Center des Massachusetts Institute of Technology (MIT) im amerikanischen Cambridge. Das Gerät sendet WiFi-Signale in einen Raum, der bis zu 18 Meter entfernt sein kann, dessen Betonwände aber nicht mehr als 20 Zentimeter dick sein dürfen. Die Wellen dringen durch die Wände und werden an Gegenständen und Körpern dahinter reflektiert. Aus den zurückgespiegelten Wellen lässt sich auf das Geschehen im Rauminneren schließen. Bewegen sich bei-

Scanner für Schiffscontainer



Speziallaster mit Röntgengerät an Bord durchleuchten Häuser und Autos.

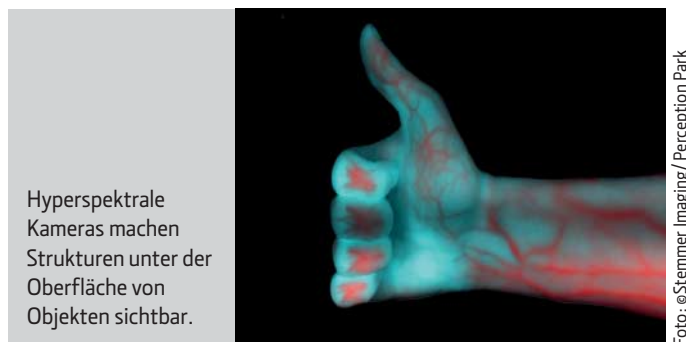
Foto: Visum

Das Fraunhofer-Entwicklungszentrum Röntgentechnik EZRT in Fürth besitzt den größten Computertomografen der Welt. Der XXL-CT kann selbst sperrige Objekte wie Schiffscontainer oder Fahrzeuge komplett durchleuchten. Mit einer Rotationsgeschwindigkeit von fünf Grad pro Sekunde wird das Objekt während des Scans um 360 Grad gedreht. So entsteht ein dreidimensionales Bild seines Inneren. Vorläufig dient der XXL-CT hauptsächlich dazu, archäologische Fundstücke zu durchleuchten und Materialschwächen an Windturbinen oder Autokarosserien ausfindig zu machen. Künftig aber kann der Detailreichtum der Bilder dem Zoll, der Polizei oder Anti-

terroreinheiten helfen, Waffen, Drogen und andere Schmuggelware zu finden.

In einer groben Variante sind solche Durchleuchtungssysteme sogar schon im Einsatz: Durch New York fährt seit einigen Jahren eine unbekannte Zahl von Röntgenlastern. Die nicht speziell gekennzeichneten Fahrzeuge sind mit einem Hochleistungs-Röntgengerät ausgestattet und kosten jeweils rund 800 000 US-Dollar. Ihre Strahlen können Wände durchdringen und somit in das Innere von Gebäuden oder in andere Wagen sehen. Kritiker fürchten allerdings Gesundheitsgefahren. Denn die Strahlenbelastung liegt rund 40 Prozent höher als etwa bei Röntgenscannern an Flughäfen. Um Polizisten zu schützen, die mit diesen Lastern arbeiten, können die Röntgengeräte aus bis zu 450 Metern Entfernung gesteuert werden. Das hilft unbeteiligten Passanten oder Verkehrsteilnehmern jedoch wenig. In Deutschland werden solche Laster nur genutzt, um unbemannte Fahrzeuge zu überprüfen, die zuvor aus dem Verkehr gezogen wurden.

Kameras schauen unter die Oberfläche



Hyperspektrale Kameras nutzen für ihre Aufnahmen das gesamte elektromagnetische Spektrum des Lichts, von Ultraviolett bis zum langwelligeren Infrarot. Bestimmte Materialien besitzen charakteristische Signaturen im elektromagnetischen Spektrum. Diese kann eine derartige Kamera auch dann noch aufspüren, wenn sie aus Bereichen unterhalb der Oberfläche des anvisierten Objekts stammen. So geben die Bilder Aufschluss darüber, was sich im Inneren eines Gegenstands befindet. Im Moment kommen solche Kameras vor allem bei Satellitenaufnahmen oder der Kontrolle von Lebensmitteln zum Einsatz. Hyperspektrale Kameras eignen sich aber auch für Antiterrormissionen: Das US-Einsatzkommando, das 2011 Osama bin Laden tötete, nutzte entsprechende Geräte, um den Angriff vorzubereiten.

Bisher waren solche Kameras groß und teuer. Nun jedoch kommt eine handlichere und günstigere Generation auf den Markt, darunter etwa die HyperCam, ein Gemeinschaftsprodukt von Microsoft und der University of Washington. Je nach Ausstattung soll sie nur zwischen 50 und 800 US-Dollar kosten. Die aufwendigere Version kann ein Bild in 17 verschiedenen Wellenlängen aufzeichnen. Sie ließe sich zum Beispiel in biometrische Sicherheitssysteme an Flughäfen integrieren. Mit ihrer Hilfe soll es dann möglich sein, nervöse Terroristen über ihre erhöhte Körpertemperatur zu entlarven. Auch das Einschleppen biologischer Erreger oder anderer verbotener Substanzen ließe sich anhand von elektromagnetischen Signaturen verhindern.

Handygespräche mitschneiden

Sogenannte IMSI-Catcher simulieren ein Mobilfunknetz und gaukeln einzelnen Handys vor, die nächstgelegene Funkzelle des eigenen Betreibers zu sein. Sie können dann die International Mobile Subscriber Identity (IMSI) auslesen, die Position des Handys eingrenzen und Telefonate mithören. Schon dies ist ein erheblicher Eingriff in die Privatsphäre. Hinzu kommt, dass die Technik sämtliche Handys anzapft, die sich gerade am Funkmast eingeloggt haben – die Ermittler könnten also auch Gespräche völlig Unbeteiligter mithören.

Das genaue Ausmaß des Einsatzes zu quantifizieren ist schwierig, denn die Behörden hüllen sich in Schweigen. Der Einsatz von IMSI-Catchern ist zwar grundsätzlich legal. Unter welchen Voraussetzungen Ermittler darauf zurückgreifen dürfen, ist allerdings hoch umstritten. Bürgerrechtler kritisieren, dass die Polizei oft einfach den Weg des geringsten Widerstandes wählt und den Einsatz nicht zugibt, statt eine rechtliche Prüfung zuzulassen. In den USA wurden Polizisten in der Vergangenheit sogar vom FBI angewiesen, IMSI-Catcher nicht zu erwähnen. In Großbritannien haben Polizisten Unterlagen vernichtet, welche die Anschaffung solcher Geräte bewiesen.

Hacker gegen Überwachung



Die Fälle zeigen, wie schwer sich schon Demokratien damit tun, Observationstechniken streng nach rechtsstaatlichen Regeln zu verwenden. Umso wichtiger sei es, Menschen in autoritären Regimen oder in Staaten, in denen Grundrechte in Gefahr sind, mit Gegenmitteln auszustatten, sagen Pedro Oliveira und Xuedi Chen. Die Designer vom Interactive Telecommunications Program an der New York University haben mehrere Gadgets entwickelt, mit denen sich Demonstranten oder Oppositionelle gegen die Polizei schützen können.

Zu ihrem Backlash Kit gehört zum Beispiel das Panikknopf-Armband. Es vibriert, wenn sich Demonstranten einer Zone nähern, in der andere eine akute Gefahr identifiziert haben. Die persönliche Black Box für die Hosentasche kreiert einen WiFi-Hotspot zum schnellen Hochladen von Fotos und Videos, falls Gefahr besteht, dass Kameras konfisziert werden. Außerdem kann ein mobiler Router ein Mesh-Netzwerk erzeugen, das den Aktivisten auch dann noch miteinander zu kommunizieren erlaubt, wenn Behörden den Zugang zum Internet behindern. Dabei sind alle Teilnehmer direkt miteinander verbunden. Ein Foto oder Video, das durch WiFi-Hotspot und Mesh-Router an alle weitergeleitet wurde, kann so in Sicherheit gebracht werden. ☞