SIE KÖNNEN DICH SEHEN

ADRIAN RYNT,
34 J., LEDIG,
ENTWICKLER,
GEB. IN BONN

GEMELDET: EBD.
AKTUELL IN: HH
VORSTRAFEN: 0
KONTOSTAND:
2435 EURO
SMARTPHONE-
KONTAKTE: 687

Der G20-Gipfel Anfang Juli in Hamburg wird mehr als Weltpolitik, umlagert von Groß-Demos und bedroht von gewaltsamen Randalen. Er wird vor allem: eine BIG-BROTHER-LEISTUNGSSCHAU *modernster Überwachungs- und Fahndungstechnik aus aller Welt. Ein Albtraum für Datenschützer – und ein Lehrstück für die deutsche Polizei*

SIE WERDEN DICH KRIEGEN

text **JAY TUCK**

In Hamburg brennt die Luft. Schon Monate vor dem G20-Gipfel, zu dem Anfang Juli die Staats- und Regierungschefs der wichtigsten Industrienationen und Schwellenländer anreisen werden, gab es Brandanschläge auf den Tagungsort, die Hamburg Messe. Auch Polizeiwagen brannten. Einige militante G20-Gegner betreiben regelrechte Trainingslager. Im Internet besprechen sie Routen und Ausrüstung, Angriffstaktik und Verteidigung gegen die Staatsmacht, versichern sich der Unterstützung politisch motivierter Gewalttouristen aus dem Ausland. Und auch der Staat rüstet massiv auf.

Seit Wochen sieht man in Hamburg groß angelegte Übungen mit Polizeihelikoptern, Hafentauchern und Straßensperren. Beamte trainieren an vermummten Statisten den Umgang mit Gewalttätern und haben ein weitläufiges Areal mit Nato-Stacheldraht gesichert, wo Festgenommene von Richtern in Schnellverfahren abgeurteilt werden können. Das mag beängstigend wirken, doch die stärksten staatlichen Waffen – gegen gewaltbereite G20-Gegner und womöglich auch radikale Islamisten – sind dieses Mal unsichtbar: Technologien, die die Grenzen gewöhnlicher deutscher Polizeiarbeit sprengen. Menschenmassenbeobachtung aus der Luft gehört dazu, die computergestützte Identifikation einzelner Personen in der Menge sowie der sekundenschnelle Datenabgleich mit Fahndungsprofilen aus anderen Ländern. Die internationale Kooperation der Sicherheitskräfte aus aller Welt, vermuten Insider, wird auch für die deutsche Polizei einige Lehrstunden bereithalten.

TRUMPS TRUPPE

Allein die Augen und Ohren, die der Secret Service mitbringt, die Leibgarde von US-Präsident Donald Trump, ist ein Arsenal an modernsten Überwachungsinstrumenten, gekoppelt an gigantische Archive der Identitäten potenzieller Gefährder. Insider erwarten, dass auch die Spionage-Drohne Predator dabei sein wird. Hoch über den Köpfen der Demonstranten sollen demnach unbemannte Aufklärer mit einem geheimen Spionage-Paket namens Argus-IS kreisen, ursprünglich für das US-Militär entwickelt. Aus einer Flughöhe von 5,5 Kilometern können ihre Hochleistungskameras halb Hamburg erfassen. Und Hunderttausende von Menschen. Einzeln und in Echtzeit. Mit Argusaugen, die mit einer Bildschärfe von 1,8 Milliarden Pixel durch 65 aktive Fenster zugleich schauen.

Technisch besonders erstaunlich ist dabei die Fähigkeit, solche riesigen Bilddatenmengen auch tatsächlich zu verarbeiten und zu analysieren: Sind gesuchte Gefährder in der Menge? Selbst Heerscharen von Menschen vor Bildschirmen könnten Fragen wie diese nicht beantworten. Das kann nur künstliche Intelligenz – unter anderem mit Hilfe einer Hochleistungssoftware namens RIOT. Die „Rapid Information Overlay Technology" vom US-Rüstungsunternehmen Raytheon, das auch Spionage-Sensoren für Drohnen und Exoskelette für Soldaten entwickelt, ist eine Suchmaschine der Superlative. RIOT wird ausschließlich an Militärs, Nachrichtendienste und Strafverfolgungsbehörden verkauft. Ihre Leistung stellt sogar Google in den Schatten.

DIGITALE SUPER-COPS

RIOTS Algorithmen sind für enorme Informationsmengen ausgelegt, in der Fachsprache Extreme-Scale Analytics, und ihre Geschwindigkeit ist atemberaubend. Ist eine Zielperson ausgemacht, spuckt die Software umfangreiche Eckdaten aus: Telefonate und Kontakte, SMS-Texte und E-Mails sowie GPS-Standorte. Bei jeder Aktivität eines ins Visier genommenen Verdächtigen zeigt RIOT dessen Bewegung auf einer Landkarte. Wie Brotkrümel im Märchenwald ist die Route ablesbar – in Echtzeit, aber auch für zurückliegende Tage, Monate oder Jahre.

Zudem errechnet RIOT komplexe Ereignisketten. Geht Person A in ein Café mit Person B, die sich mit Person C im Chat austauscht, die wiederum Bargeld an Person D überweist, werden alle beteiligten Menschen und ihre Verbindungen erfasst. Sie werden per Gesichtserkennung identifiziert, ihre Besucher fotografisch festgehalten und in einer übersichtlichen Tortengrafik abgebildet. Komplizierte Knäuel solcher Ketten kann RIOT zu Hunderten entzerren und analysieren. Binnen weniger Minuten. Und die Ergebnisse landen in den ewigen Archiven der Behörden.

DEUTSCHE LANDESPOLIZEI

Solche künstlichen Superhirne sind für deutsche Fahnder allenfalls eine Traumvorstellung von perfekter Verbrecherjagd – und für viele Bürger ein Albtraum. Deutschland kennt Big Brothers modernste Kinder noch nicht. Im internationalen Vergleich gelten die technischen Möglichkeiten hiesiger Sicherheitsbehörden als altbacken, ihre Fahndung und Forensik als veraltet. „Es gibt ernsthafte Lücken in der Ausbildung unserer Polizei, vor allem was Hightech angeht", sagt André Schulz, Vorsitzender des Bundes Deutscher Kriminalbeamter. Seit Jahren fordert er Modernisierung – wenigstens in grundlegenden Bereichen. „In den USA hat jeder Streifenpolizist ein Terminal im Auto, an dem er gestohlene Wagen oder ausstehende Haftbefehle abrufen kann. In Deutschland haben wir 16 Landespolizeien und nicht einmal eine einheitliche Software."

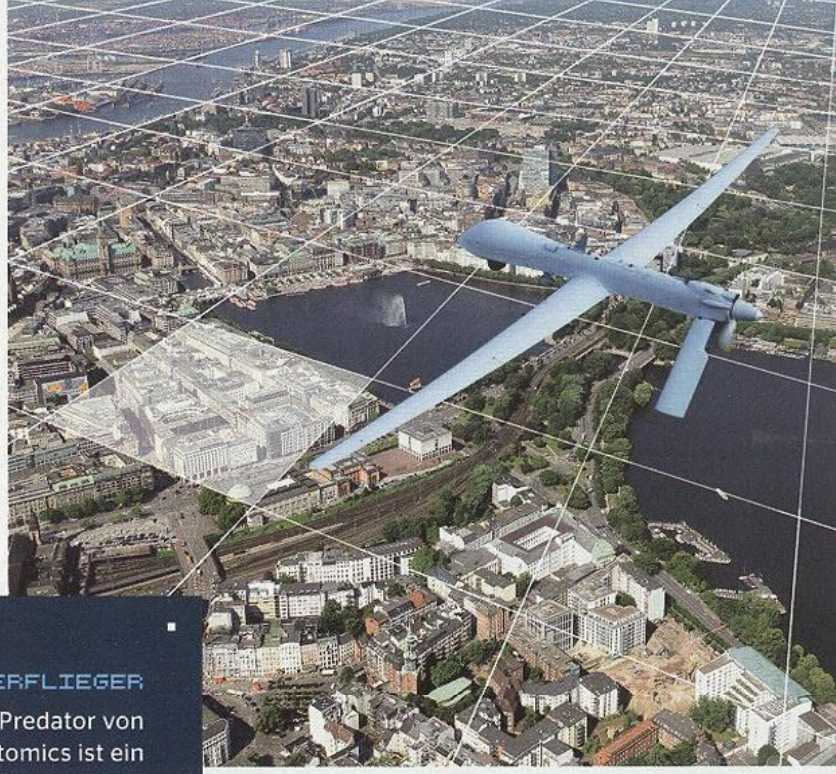
G20 soll daher ein lehrreicher Kulturaustausch werden. Besonders mit den USA, wo Landespolizei und FBI, CIA und Homeland Security viel freizügiger Informationen miteinander teilen als deutsche Dienste. Und wesentlich schneller. Die wichtigste Ursache dafür liegt in den antiquierten IT-Systemen der deutschen Landespolizeibehörden. Bestes Beispiel: die

FOTOS: DPA, LAIF, JAY TUCK

bundesweite Gemeinsame Ermittlungsdatei, die im Jahr 2012 eingeführt wurde – für 2,3 Millionen Euro. Die Software ist mit den unterschiedlichen Landessystemen nicht kompatibel. Will ein Ermittler Daten aus einem anderen Bundesland verwenden, muss er sie manuell aus dem einen System herausnehmen und per Hand in das andere eintragen. Eine Schnittstelle existiert nicht. Heißt: Ein flüchtiger Krimineller aus Bayern muss nur über die Grenze nach Thüringen gelangen, schon ist er in relativer Sicherheit.

„Unter solchen Umständen ist länderübergreifende Zusammenarbeit unmöglich", sagt Schulz. Aus den Ermittlungen gegen den Berliner Weihnachtsmarkt-Attentäter Anis Amri 2016 und schon vor Jahren aus dem Fall der rechten Terrorgruppe NSU ließ sich ersehen, wie leicht entscheidende Hinweise in der Konfusion und im Kompetenzgerangel der Länderdienste verloren gehen.

Hinzu kommt der deutsche Datenschutz, der die technischen Möglichkeiten unserer Fahnder beschneidet. Unmittelbar nach dem Berliner Attentat vom 19. Dezember 2016 bat das Bundeskriminalamt (BKA) die Berliner Polizei, ein Foto des flüchtigen Attentäters Amri zu veröffentlichen. Doch die Behörde verpixelte das Bild zunächst, bevor es für die Öffentlichkeit freigegeben wurde. In Hamburg wurde es sogar tagelang zurückgehalten – gegen die dringende Bitte des BKA. Das ist in der Hansestadt nicht ungewöhnlich, kritisieren Kripo-Beamte. Grund ist der – im Norden besonders ausgeprägte – politische Wille, persönliche Daten zu schützen. Er verlangt, dass erst alle anderen Ermittlungsmöglichkeiten ausgeschöpft werden, bevor mit einem öffentlichen Fahndungsfoto das Persönlichkeitsrecht eines Verdächtigen verletzt wird. Ironie des Schicksals, dass nun ausgerechnet Argus-IS über Hamburg kreist und Informationen über deutsche Staatsbürger sammelt – ohne Kontrolle deutscher Behörden.



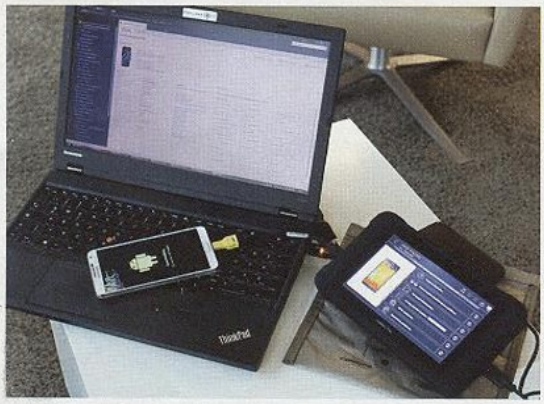
UEBERFLIEGER

Die MQ-1 Predator von General Atomics ist ein unbemanntes Fluggerät, das per Joystick aus großer Entfernung gesteuert wird. Typischerweise mit Hellfire-Raketen unter den Flügeln, ist die Drohne in Kriegsgebieten wie Afghanistan oder Syrien unterwegs, via Satellit verbunden mit ihren fernlenkenden Piloten in geheimen US-Militärstützpunkten (rechts). Die Drohne kann aber auch mit Aufklärungselektronik wie Argus-IS ausgestattet werden. Insider erwarten, dass sie mit solcher Überwachungstechnik während des G20-Gipfels über Hamburg zum Einsatz kommt (Bildmontage oben).

PRIVATE DETEKTIVE

Eine groß angelegte Video-Beobachtung der Bürger im öffentlichen Raum, etwa durch Verkehrsüberwachungssysteme: In Deutschland wäre sie undenkbar. Protokollieren in den USA vielerorts fest installierte Kamerasysteme zur automatischen Kennzeichenerfassung die Vorbeifahrt Tausender Autos pro Stunde, inklusive Uhrzeit, Fahrzeughalter, Geschwindigkeit und Fahrverhalten, dürfte der deutsche Staat nicht einmal Mautstellen auf diese Weise überwachen. Wenn hiesige Fahnder Überwachungskamerabilder wollen, sind sie meist auf Privatfirmen angewiesen, auf Kaufhäuser, Casinos oder Banken und Verkehrsbetriebe, die den eigenen Geschäftsbereich im Blick behalten.

Genauso benötigen deutsche Ermittler oft private Unterstützung, wenn sie digitale Spuren verfolgen sollen, die Verdächtige auf Festplatten oder in Smartphones hinterlassen. Eines frühen Morgens im Frühling 2017 steht diese geballte Expertise in Gestalt eines Mannes mit eckiger Brille und Strubbelhaaren vor einem Haus in der hessischen Provinz: Marko Rogge,



LEBENS-LESER

IT-Forensiker wie Marko Rogge, 44, können beim Auslesen eines Smartphones ein komplettes Leben offenlegen. Dazu nutzt Rogge ebenso wie Strafverfolger vom Bundeskriminalamt und Geheimdienste oder Militärs in aller Welt das Universal Forensic Extraction Device (UFED) der israelischen Firma Cellebrite. Es kopiert den gesamten Inhalt eines sichergestellten Smartphones innerhalb von Minuten, darunter auch gelöschte, verschlüsselte oder versteckte Daten. Es extrahiert und dekodiert Dateisysteme und Passwörter - verschafft sich so Zugang zu sämtlichen Inhalten. Und hinterlässt dabei selbst keine Spuren.

44, IT-Forensiker einer Firma aus Heilbronn. Es ist sieben Uhr, nicht seine Lieblingszeit, aber die bevorzugte Stunde für den unangemeldeten Besuch der Staatsmacht. An diesem Tag handelt es sich um Betrugsverdacht. „Ich muss erst warten, bis die Beamten die Wohnung öffnen, den Durchsuchungsbefehl vorzeigen und die Räumlichkeiten sichern", erklärt Rogge, während er mit einem Kaffeebecher am Mannschaftsbus lehnt. Dann aber müsse es schnell gehen.

MODERNES SPIONAGEGERÄT

Rogges Job ist es, PINs und Passwörter zu knacken, gelöschte Dateien wiederherzustellen und chiffrierte Texte zu entziffern. „Wenn ich reingehe, sichere ich zuallererst einmal die Geräte", erklärt er. Und zwar in Behältnissen, die nach Art Faraday'scher Käfige den Inhalt abschirmen: Kein Funksignal geht mehr rein, keines mehr raus. Warum er sich dabei beeilen muss? Weil viele Verbrecher technisch versiert sind. „Ein Komplize könnte verräterische Daten noch in letzter Sekunde per Fernbedienung löschen", sagt Rogge. Würden die Ermittler Smartphones und Festplatten ungesichert abtransportieren, könnten solche Daten sogar automatisch verschwinden: „Es gibt Software, die bei verändertem GPS-Standort eine Festplatte formatiert. Man nennt das GEO-Fencing", erklärt Rogge. Mancher Kriminelle ist heute technisch versierter, als ihre Ausbildung es der Polizei erlaubt.

Rogge ebenfalls. Hat er die beschlagnahmten Geräte erst mal auf der sicheren Seite, rückt er ihnen mit UFED (siehe Kasten links) zu Leibe. So heißt sein Hauptwerkzeug. Nach Angaben des israelischen Herstellers Cellebrite knackt es Codes und umgeht alle Sperren, mit denen Smartphones gesichert sind. Dann liefert es Protokolle von Chats, Apps, Telefonverbindungen, WLAN-Standorten, SMS-Texten, Fotos und GPS-Standorten. Über Social Media kann UFED sogar den Zugriff auf Festplatten in fernen Ländern ermöglichen und Cloud-Daten runterladen.

Solche Cellebrite-Geräte sind in mehr als 100 Ländern im Einsatz. Per Online-Verbindung können sie eine firmeneigene Superhirn-Software nutzen, eine künstliche Intelligenz, die komplexe Beziehungen zwischen dem verdächtigen Smartphone-Besitzer und seinen Kontakten analysiert. Personen und Standorte werden auf einer Karte im Verhältnis zueinander dargestellt. Unter den Cellebrite-Kunden ist auch das Bundeskriminalamt. Die deutsche Strafverfolgung darf allerdings nur auf deutsche Daten zugreifen. Stehen die Cloud-Server im Ausland, braucht sie Amtshilfe.

Die internationalen Spione und Kriminalisten, die zum G20-Gipfel anreisen, haben außer UFED noch ganz andere Hightech-Tools im Köcher. Zur Palette gehören auch Systeme wie Stingray von Harris Corporation – ein Gerät, das Sendemasten simuliert. Als sogenannter IMSI-Catcher lockt er Handys aus der Umgebung zum Andocken an. Dann kann Stingray Gespräche mitschneiden, SMS-Texte speichern und womöglich den gesamten Speicherinhalt eines Smartphones ohne Wissen des Inhabers downloaden. Ein leistungsfähiger IMSI-Catcher ist in der Lage, Tausende Mobiltelefone gleichzeitig anzuzapfen. Mit

FOTOS: MARKUS KIRCHGESSNER FÜR PLAYBOY (2), PRIVAT

dem Gerät könne der Staat, so warnen Bürgerrechtler, Signale durch Wände und Kleidungsstücke empfangen. Oder auch der Watchhound von Berkeley Varitronic: Er spürt drahtlose Aktivitäten in Echtzeit auf. Ortet Stimmen, SMS-Texte oder sogar Handys im Stand-by-Modus und protokolliert alles samt Mobil-Nummern und Uhrzeit. All solche Gerätschaften führt der Secret Service im Gepäck, wenn er zum Schutz des US-Präsidenten unterwegs ist.

BIG BROTHERS SCHLAUE BRÜDER

Die Königsdisziplin der staatlichen Späher aber bleibt die Video-Überwachung großer Menschenmassen. Dass dabei die Kameras meist oben – an Hausfassaden, an der Decke von U-Bahn-Waggons oder am Bauch von Drohnen – angebracht sind, erschwert zwar die Identifikation gesuchter Personen. Denn mit den Frontal-Fotos aus den amtlichen Gefährder-Archiven stimmen die Video-Aufnahmen bisweilen kaum überein. Doch zusätzliche Späh-Techniken ziehen weitere Merkmale zu Rate als das Gesicht: den Ohrenabstand, den Haaransatz, die Muster des Bewegungsablaufs beim Gehen – auch solche Daten sammeln manche westlichen Geheimdienste. Telefoniert ein Verdächtiger, wird sein Stimmabdruck gecheckt. Haben Fahnder ihn erst mal vor sich, können auch seine Venenstruktur oder das Profil seines Schweißgeruchs helfen, ihn zu identifizieren.

Als die Besten im Westen, wenn es um die Erkennung aus der Luft geht, gelten die Drohnen- und Satelliten-Betreiber der amerikanischen National Geospacial-Intelligence Agency (NGA) – einer US-Behörde mit Sitz auf einem geheimen militärischen Gelände rund 20 Kilometer südlich von Washington, größer als das CIA-Hauptquartier, unbekannter als die NSA. Über Deutschland, so vermuten Experten, wird die NGA während des G20-Gipfels ihre Künste ebenso anwenden wie über Nordkorea oder den Konfliktgebieten in Nahost. Nur im eigenen Land ist es den Auslandsgeheimdiensten CIA, NSA und NGA gesetzlich verboten, US-Staatsbürger auszuspionieren. In Hamburg Anfang Juli aber – so sagt zumindest das US-Gesetz – dürfen sie.

DER AUTOR
Im Januar dieses Jahres ließ sich der Bund Deutscher Kriminalbeamter von **US-Sicherheitsexperte Jay Tuck** den neuesten Stand der Hightech in Fahndung und Forensik erklären. Aus Anlass des G20-Gipfels, findet der frühere „Tagesthemen"-Redakteur und Kriegsreporter, hätten jetzt auch die Bürger ein Anrecht darauf. Allen voran: die freiheitsliebenden Playboy-Leser