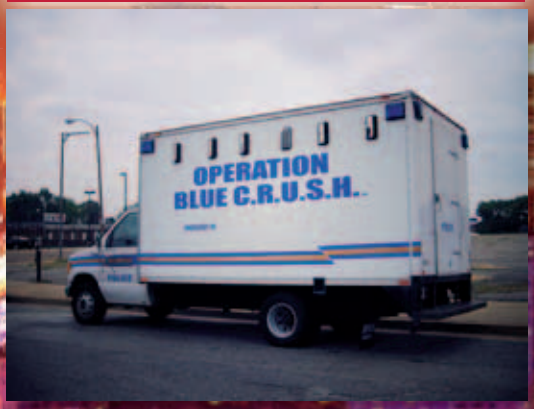
Das System „Blue Crush" überwacht seit 2005 die Stadt Memphis, Tennessee.



„Crime Eye" – das allgegenwärtige Auge des Gesetzes, heutzutage voll digitalisiert.

Die digitale Falle – für uns alle!

„Prädiktive Polizeiarbeit" und das Netzwerk privater Geheimdienste

Sebastian Frey

Smart City – die intelligente Stadt – überwacht und analysiert sich selbst und ihre Bewohner vollautomatisch

Ein sonniger Tag in San Francisco. Vor einem Straßencafé sitzen zwei Kriminalpolizisten in Zivil und schlürfen Kaffee aus den weltbekannten Pappbechern mit der Nixe. Eine kleine Ruhepause vor dem nächsten Einsatz? Weit gefehlt. Die Beamten befinden sich am Tatort eines Verbrechens. Genauer gesagt – eigentlich wird es erst ein Tatort sein. Kaffeetrinkend warten sie auf das Eintreffen des Täters, der in diesem Augenblick noch gar kein Verbrechen begangen hat.

Sind amerikanische Polizisten jetzt zu Hellsehern geworden? Was wie ein Szenario aus einem Zukunftsroman klingt, ist in unseren Tagen bereits Realität, und es ist das Resultat einer ausgeklügelten und flächendeckenden Überwachungstechnologie.

Vom Smartphone zur „Smart City"

„Smarter Cities" heißt ein automatisiertes Überwachungssystem, mit dem der US-Computergigant IBM Marktanteile zurückerobern will, und der Werbeslogan lautet „Predictive Policing", also „vorhersagende Polizeiarbeit".

Aus amerikanischen Krimiserien kennt man das Szenario, dass Polizeibeamte sich in hochtechnisierten Multimedia-Großraumbüros in verschiedene Überwachungskamerasysteme „einklinken", die von Hause aus eigentlich zu privaten oder zivilen Zwecken dienen – etwa zur Verkehrsüberwachung oder zur Sicherung des Einzelhandels. Umfangreiche Gesetzesverschärfungen seit Gründung der Homeland Security ermöglichen die Vernetzung privater Überwachungssysteme und Datenbanken mit denen der Justizbehörden, der Geheimdienste und des Militärs sowie mit Mobilfunk- und GPS-Satellitendaten. Auf diese Weise stand den Behörden praktisch fast augenblicklich ein Instrumentarium zur flächendeckenden und nahezu lückenlosen Überwachung von Großstädten zur Verfügung. Die gesamte Bevölkerung unter Generalverdacht.

Heutzutage läuft dies bereits weitgehend automatisiert. Die neuen digitalen Überwachungssysteme dienen vor allem dazu, durch computergesteuerte Auswertung einer Unzahl von Daten verbrechensgefährdete Regionen von weniger gefährlichen zu unterscheiden – auch im Hinblick auf die Zukunft – und an den so aufgefundenen Schwerpunkten die polizeiliche Präsenz zu verstärken. So jedenfalls funktioniert das System „Blue Crush", das bereits 2005 als Pilotprojekt in der Stadt Memphis, Tennessee, installiert wurde.

Grundlage der computergestützten Verbrechensvorhersage sind Polizeiberichte über frühere Verbrechen, die dem Programm von den Beamten eingegeben werden. Diese werden dann automatisch mit ganz alltäglichen Daten abgeglichen, die aus privaten Datenbanken über das Internet abgerufen werden können. Dazu gehören etwa Veranstaltungskalender, Gehaltszahltage, selbst Wetterberichte und noch vieles mehr. Nicht zu vergessen natürlich „verdächtige Aktivitäten" in sozialen Netzwerken wie Facebook oder Twitter. Man soll sich keine Illusionen darüber machen, wie genaue Persönlichkeitsprofile über jeden einzelnen von uns bereits existieren. Nicht nur aus dem Surfverhalten im Internet oder digital gespeicherten Kreditkartenabrechnungen. Auch die Gruppe der „unverbesserlichen" Barzahler opfert ihr letztes Stück Anonymität, wenn man an der Supermarktkasse für ein paar lausige Cents Rabatt seine Payback-Karte einscannen läßt. Aus einer derart modellierten digitalen Realität wirft prädiktive Software am Ende – so die Behauptung des Herstellers – Informationen darüber aus, wer wann und wo mit höchster Wahrscheinlichkeit ein Verbrechen begehen wird.

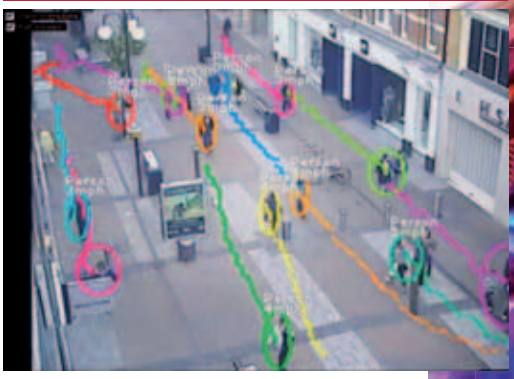
Digitale Propheten

Marktführer auf dem Gebiet der prädiktiven Kriminalitätssoftware ist die Firma SPSS, ein Dinosaurier der Statistik-Softwareentwicklung, mit dessen Produkten bereits in den sechziger und siebziger Jahren Sozialwissenschaftler ihre Statistikmodelle testeten – damals noch auf Lochkarten und mit kiloschweren Computerausdrucken. Inzwischen hat sich SPSS – einst ein Forschungsprojekt von Wissenschaftlern der Stanford-Universität für rein wissenschaftliche Zwecke – vom Statistikexperten zum digitalen Propheten entwickelt. Vor drei Jahren wurde die Firma zwecks großräumigerer Vermarktung von IBM aufgekauft.

In New York hat IBM der Polizei zeitgleich mit „Blue Crush" ein „Real Time Crime Center" installiert, also ein System zur Kriminalitätsüberwachung in Realzeit. Das System ist bei Bedarf durch Einbindung weiterer Kamerasysteme ausbaubar, und die Ergebnisse der Berechnungen werden unmittelbar an den nächstgelegenen Streifenwagen weitergeleitet. Dann klicken die Handschellen beim Täter, auch wenn er im Grunde noch gar keine Gelegenheit hatte, zum Täter zu werden. Eine juristisch bedenkliche Vorgehensweise, denn strafbare Handlungen liegen ja eigentlich erst vor, wenn ein Verbrechen tatsächlich begangen wurde. Oder schauen die Polizisten etwa zu, wie der Täter das Verbrechen begeht, damit sie dann etwas in der Hand haben?

Für die Geheimdienste geht's auch noch eine Nummer größer. Das „Analyst's Notebook" kann komplizierte Beziehungsdiagramme zwischen Personen, Orten und Gegenständen in Sekundenschnelle anschaulich visualisieren, auch für Agenten, die nicht zur Gruppe der Computer-Nerds gehören. Im Rahmen eines 9,6 Millio-

Aus Bewegungsprofilen von Passanten werden Realitätsmodelle simuliert und schließlich potentielle Verbrechensschwerpunkte prognostiziert.



nen-Dollar-Deals hat das US-Militär dieses System ebenfalls angeschafft, und zwar sowohl für das Heer als auch für die Marine. Deren hochtechnisierte kriminalistische Aktivitäten wurden ja weltbekannt durch die beliebte Fernsehserie „Navy CIS" (eine Einrichtung, die es wirklich gibt).

Die Schatten-CIA und das System TrapWire

Anfang 2012 veröffentlichte die Internet-Enthüllungsplattform Wikileaks eine Reihe von Emails der US-Firma Stratfor (Strategic Forecasting), eines in Texas ansässigen Unternehmens, das für private Auftraggeber geheimdienstähnliche Dienstleistungen anbietet und allgemein als so etwas wie

die „Schatten-CIA“ in Amerika angesehen wird (zumal sie auch im Inland aktiv werden kann, was der CIA zumindest offiziell verboten ist). Zur Kundschaft von Stratfor gehören u. a. große Rüstungsfirmen wie Lockheed Martin,

Wer benimmt sich verdächtig? Bei TrapWire berechnet das der Computer automatisch aus den Daten der Überwachungskameras

Northrop Grumman oder Raytheon, aber auch das Chemieunternehmen Dow Chemical, das für die Chemiekatastrophe von Bhopal 1984 verantwortlich war. Stratfor unterhält für seine Arbeit ein weltweites Netz von Informanten, die über Schweizer Bankkonten und Prepaid-Kreditkarten bezahlt werden. Um diese Informanten darüber hinaus bei der Stange zu halten, wendet Stratfor zum Teil recht rabiate Mittel an, wie aus einer der Emails hervorgeht: *„Du musst die Kontrolle über ihn übernehmen. Kontrolle bedeutet finanzielle, sexuelle und psychologische Kontrolle. Damit kommen wir zur Diskussion über Deine zweite Phase. …“*

Das umfangreiche Email-Archiv, das nunmehr veröffentlicht wurde, enthält nicht nur Korrespondenzen der Stratfor-Mitarbeiter untereinander, sondern auch mit ausgewählten Repräsentanten externer Firmen, deren Verbindungen zum FBI und anderen Ermittlungsbehörden offengelegt wird. Darunter scheinbar harmlose Vertreter des Einzelhandels, z. B. der Internet-Buchhändler Amazon oder die Kosmetikfirmen PETA und ELF. Ebenfalls offengelegt werden die Verflechtungen zwischen Stratfor und der Firma Abraxas, eines weiteren Privat-Geheimdienstes, der ein prädiktives Überwachungssystem namens *TrapWire* entwickelt hat. Diese futuristisch anmutende Technologie interagiert direkt mit einem Netzwerk von Überwachungskameras, um in Realzeit Gesichtserkennung zu betreiben. Bereits heute existiert unter dem Codenamen TW-CI (TrapWire Critical Infrastructure) ein landesweites Netzwerk von TrapWire-Hotspots, auf die das System mit Hilfe prä-operationaler Überwachungsaktivitäten sein spezielles Augenmerk richtet. Das System TW-CM (TrapWire Community Member) hingegen erstellt Online-Reports über verdächtige Aktivitäten bestimmter Personen. Derartige Systeme laufen in Los Angeles und Washington unter dem Namen „iWatch“ sowie in New York und Las Vegas unter dem Label „See Something Say Something“. Die dritte Ebene, TW-LE (TrapWire Law Enforcement) schließlich stellt diese Daten in den Zusammenhang mit Datenbanken aus der gesamten Region und darüber hinaus, erstellt Analysen und macht Vorschläge für logistische Aktivitäten. Die Firma Abraxas wird betrieben von einem Team ehemaliger Agenten der CIA, des FBI und der Homeland Security. Seit 2009 existiert ein Kooperationsabkommen mit Stratfor.

Einsatz nicht nur gegen Verbrecher

Für seine privaten Auftraggeber arbeitet das Stratfor/Abraxas-Netzwerk nicht nur zum Zwecke der Verbrechensbekämpfung, sondern man infiltriert auch unbequeme NGOs, so z. B. die Bhopal-Aktivisten, die bis heute um Entschädigungszahlungen von Dow Chemical für die Opfer der Chemiekatastrophe kämpfen. Auch Wikileaks selbst soll von Stratfor-Agenten unterwandert sein, und einige Tausende der nunmehr publizierten Emails zeugen davon, wie weit dieser vom Gesetzgeber weitgehend unkontrollierte Privat-Geheimdienst auch in die Aktionen gegen Wikileaks-Gründer *Julian Assange* verwickelt ist. Auch mit höchsten politischen Ebenen ist man verbandelt und nutzt diese Kontakte, um das Geschäft weiter zu expandieren. In den Stratfor-Emails wird darüber in einer Deutlichkeit geredet, die nichts zu wünschen übrig lässt. So heißt es über den texanischen Senator *John Carona*, man würde mehr TrapWire-Systeme verkaufen können, wenn er und einige andere Schlüsselfiguren *„ein paar Fettärsche im Capitol“* küssen würden.

Es stellt sich nunmehr die Frage, warum auf dem Gebiet der prädiktiven Software und Hardware eine derart babylonische Sprachverwirrung herrscht? Warum eine solche Vielfalt von Smart City über Blue Crush bis zu TrapWire? Weil in den USA überall und von Jedermann Überwachung betrieben wird. Und so haben FBI, Militär und lokale Polizeibehörden jeweils unabhängig voneinander ihre eigenen Systeme angeschafft, von privaten Auftraggebern ganz zu schweigen. Dass die unterschiedlichen Geheimdienste und Ermittlungsbehörden sich nicht gerade grün sind und oft eher gegen- als miteinander arbeiten, ist spätestens seit dem 11. September allgemein bekannt. Für die Entwickler prädiktiver Systeme ein nahezu unbegrenzter Markt und ein Milliardengeschäft. Weltweite Expansion nicht ausgeschlossen: Das „Analyst's Notebook“ wird mittlerweile auch schon vom Bundeskriminalamt eingesetzt. Von dort fanden die automatisierten Ermittlungsmethoden, wie inzwischen bekannt geworden, ihren Weg bis in Europas letzte Diktatur – Alexander Lukaschenkos Weißrussland. ■

Das „Analyst's Notebook“ erstellt komplizierte Beziehungsdiagramme zwischen Personen, Firmen, Staaten und was immer private oder staatliche Ermittler noch interessiert.