Projekt INDECT -

Einblicke in das Europäische Sicherheitsforschungsprogramm

oder

Panopticon meets Orwell

D.N.J., Januar 2011

„EU finanziert Orwells künstlichen Intelligenz Plan zur Überwachung der Öffentlichkeit bei "abnormem" Verhalten“ lautete die Schlagzeile des britischen *Telegraph*[1], im aller ersten Bericht der Mainstream-Medien zu dem seit Anfang 2009 laufenden Sicherheits- und Überwachungs-Projekt der EU. *Die Zeit* nannte es in ihrer online-Ausgabe den *„Traum der EU vom Polizeistaat.*[2]*“* *„[Es] riecht nach einer abstrusen Verschwörungstheorie, könnte aber unsere nahe Zukunft sein*“, meinte *Der Freitag*[3] dazu, und die *TAZ* schrieb, dass das alles nach Science-Fiction klingen würde.[4]

Die Rede ist von einem von der Europäischen Union finanzierten Projekt mit der Bezeichnung INDECT (*„Intelligent information system supporting observation, searching and detection for security of citizens in urban environment“*, zu Deutsch: *„Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Entdeckung für die Sicherheit von Bürgern in städtischer Umgebung.“*). Doch was verbirgt sich nun hinter dem, was wie eine wilde Verschwörungstheorie, wie Orwells 1984 oder wie eine moderne Variante von Benthams *Panopticon*[5] klingt?

Um zu verstehen, um was es sich dabei konkret handelt bzw. in welchem größeren Kontext Projekte wie INDECT ins Leben gerufen wurden, wollen wir anfangs etwas weiter ausholen und kurz auf das Europäische Sicherheitsforschungsprogramm im Rahmen des „*Seventh Framework Programms*“[6] eingehen:

Im Februar 2004 initiierte die Europäische Kommission das Projekt PASR (“*Preparatory Action in the field of Security Research*”)[7] mit einem Budget von € 65 Millionen, verteilt auf den Zeitraum zwischen 2004 bis 2006[8]. Im Rahmen von PASR entstanden 39 Projekte mit folgenen Prioritätsbereichen: *1. Verbesserung von Situationserkennung, 2. Optimierung des Schutzes und der Sicherheit von Netzwerksystemen*, 3. *Schutz vor Terrorismus*, 4. *verbessertes Krisenmanagement* und 5. *die Herstellung von integrierten, kompatiblen Informations- und Kommunikationssysten*.

An PASR beteiligt waren vorwiegend Unternehmen aus der Verteidigungsindustrie. Unter anderem die britischen Firma *BAE Systems*, dem derzeit größten Rüstungskonzern der Welt. *BEA Systems* geriet in den letzten Jahren immer wieder wegen Korruptionsverdacht, Spionage, Betrugs und Menschenrechtsverletzungen in die Schlagzeilen. 2005 wurde etwa bekannt, dass das Unternehmen den chilenischen

1 The Telegraph: EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour" , Ian Johnston, 19 Sep 2009
2 Die Zeit, Indect – der Traum der EU vom Polizeistaat, Kai Biermann, 24.9.2009
3 Der Freitag, INDECT: War Orwell ein naiver Optimist? (08.11.2009)
4 TAZ: Die moderne Verbrecherjagd, Thomas Salter, 24.12.2009
5 Der Philosoph Jeremy Bentham entwickelte im 18. Jahrhundert ein Konzept zum Bau von Gefängnissen, Anstalten, Fabriken, Schulen und ähnlichem, welches er "Panoptikum" bzw. "Panoticon" nannte. Dabei handelt es sich um eine Gebäudekonstruktion die perfekt darauf ausgelegt ist, alle sich darin befindlichen Menschen effizient zu überwachen: In der Mitte des Gebäudes steht ein Beobachtungsturm von welchem aus offene Zelltrakte in der sogenannten Strahlenbauweise abgehen. So kann der Wärter in der Mitte in die Zellen einsehen, ohne dass die Insassen wiederum den Wärter sehen können. In einer, von Bentham vorgeschlagenen, erweiterten Form des Panoticon könnten mehrere Ringe von im Kreis angeordneten Zellen bewirken, dass Wärter wieder von Wärtern, die über ihnen stehen, kontrolliert werden, was potenziell über einige Ebenen weiter ausgebaut werden könnte. Damit werden die Gefangenen, wie auch die Wärter unter die permanente potenzielle Kontrolle eines allumfassenden Blickes gestellt. Jederzeit könnten sie beobachtet und für als falsch gewertete Handlungen bestraft werden, was bei ihnen zu einer neuen Konzeption von Verhalten führen würde, die gerade diesen potenziellen Blick der Überwacher einbezieht. Der Informationstheoretiker Branden Hookway führte 2000 auf der Grundlage von Benthams Idee das Konzept des "Panspectrons" ein, eine Weiterentwicklung des Panopticons dahingehend, dass es kein Objekt der Überwachung mehr definiert, sondern alle und alles überwacht wird. Das Objekt wird erst im Zusammenhang mit einer konkreten Fragestellung definiert.
6 European Commission: CORDIS: FP7
7 Vade-mecum, Preparatory Action in the field of Security Research, 31 March 2004
8 European Commission Decision 2004/213/EC of 3 February 2004 on the implementation of the Preparatory Action on the Enhancement of the European industrial potential in the field of security research.

Diktator *Pinochet* finanziell unterstützt hat,[9] und schon 2003 wurde *BAE* verdächtigt, Mitarbeiter der britischen NGO *Campaign Against Arms Trade auszuspionieren.*[10] Das englische *Serious Fraud Office* untersuchte Fälle vom Gebrauch politischer Korruption zur Erleichterung von Waffenverkäufen seitens BEA, an Länder wie Chile, die Tschechische Republik, Rumänien, Saudi Arabien, Südafrika, Tansania und Qatar[11]. *BAE* plädierte stets auf unschuldig und gab nie irgendwelche Verwicklungen in Korruption zu, sie wurden dennoch im Februar 2010 zu Geldstrafen in Höhe von knapp 300 Millionen Pfund verurteilt[12]. Nur einen Monat später verloren sie einen Prozess gegen die US Regierung wegen konspirativen Betrugs und wurden zu Geldstrafen in Höhe von $400 Millionen verklagt.[13]

In Saudi Arabien war *BAE* in den sogenannten *Al-Yamamah arms deal* verwickelt, die Untersuchungen wurden allerdings wieder eingestellt und die Untersuchungsergebnisse werden bis heute mit der Begründung zurückgehalten, dass die Veröffentlichung sowohl die internationalen Beziehungen als auch die kommerziellen Interessen Englands gefährden würde.[14]

Ein weiteres der Unternehmen, das an PASR beteiligt war, war die *European Aeronautic Defence and Space Company* (EADS). Auch sie gehört zu den weltweit größten Rüstungskonzern und auch sie waren und sind in diverse Fälle von Betrug bis Korruption involviert. EADS war beispielsweise, ebenso wie *BAE Systems*, in die *Eurofighter-Affäre* in Österreich verstrickt.[15] Dazu kommen dann noch weitere Rüstungskonzerne wie die französische *Thales Group* oder die italienische *Finmeccanica companies*. Allein diese vier Konzerne erzielten 2008 einen (offiziellen) Gesamtprofit von gut €150 Milliarden[16] durch den Verkauf von Waffen und Überwachungstechnik in die ganze Welt – an westeuropäisches Militär, private Sicherheitsagenturen auf der ganzen Welt, Diktatoren und diverse paramilitärische Organisationen – unterschiedslos. Solange nur der Gewinn stimmt. Diese Unternehmen leiteten das Sicherheitsforschungsprogramm der Europäischen Union während des PASR Projektes.

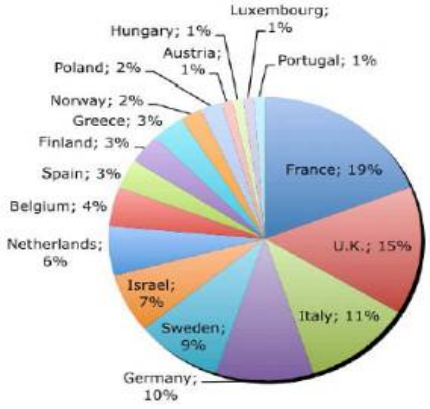
Ben Hayes schreibt diesbezüglich zu PASR[17]: „*Die wohl hervorstechenste Eigenschaft von PASR war das Ausmaß der Beteiligung der Verteidigungsindustrie. Von den 39 Sicherheitsforschungsprojekten im Rahmen von PASR, wurden 23 (60%) von Firmen geleitet welche primär im Verteidigungssektor tätig sind. Ein Drittel aller PASR Projekte (13) wurde von Thales (Frankreich), EADS (Niederlande), Finmeccanica companies (Italien), SAGEM Défense Sécurité (Teil der französichen SAFRAN Gruppe) und ADS („AeroSpace and Defence Industries Association of Europe" - Europas größte Lobby-Gruppe der Verteidigungsindustrie) geleitet. Zusammen mit BAE Systems (UK) beteiligten sich diese Firmen an 26 (67% oder zwei Drittel) der 39 Projekte."*

Zusätzlich zu diesen 39 PASR-Projekten finanzierte die EU zwischen 2002 und 2006 sicherheitsbezogene Forschungsprojekte im Rahmen des „*Sixth Framework Programme*" (FP6).[18] Aus einem Bericht für das EU Parlament von *Didier Bigo* und *Julien Jeandesboz* ging hervor, dass Ende 2006 insgesamt 170 Projekte von der EU im Rahmen von FP6 finanziert worden sind. Ein Großteil dieser Projekte befasste sich mit Forschung und Entwicklung in den Bereichen IT-Sicherheit, Raumfahrt, Weltraum- und Satelliten gestützte Beobachtung und Überwachung.[19] Zwischenzeitlich wurde im September 2004 die Einrichtung eines "*European Security Research Programme*" (ESRP) in die Wege geleitet welches über den Zeitraum von 2007 bis 2013 dann im Rahmen des FP6-Nachfolgeprogrammes FP7 („*7th Framework Programme*") mit einem Budget von 1.4 Mrd. € von der EU finanziert wird.

9 http://www.guardian.co.uk/world/2005/sep/15/bae.freedomofinformation
10 http://www.guardian.co.uk/world/2007/dec/04/bae.armstrade
11 Siehe dazu z.B.: http://www.guardian.co.uk/world/2009/oct/12/bae-bribery-case-brown-intervene, http://news.bbc.co.uk/2/hi/business/6339625.stm oder http://www.guardian.co.uk/world/interactive/2007/jun/07/bae.global.investigations
12 http://news.bbc.co.uk/2/hi/business/8500535.stm bzw. http://edition.cnn.com/2010/CRIME/03/02/bae.plea/index.html
13 http://www.justice.gov/opa/pr/2010/March/10-crm-209.html
14 http://www.guardian.co.uk/uk/2006/jul/25/houseofcommons.armstrade bzw. http://news.bbc.co.uk/2/hi/business/6181949.stm
15 http://diepresse.com/home/politik/innenpolitik/eurofighter/314181/Das-war-der-EurofighterUAusschuss?direct=314105&_vl_backlink=/home/index.do&selChannel=414 oder http://derstandard.at/2837275
16 http://books.sipri.org/files/FS/SIPRIFS1004.pdf
17 Ben Hayes - NeoConOpticon - The EU Security-Industrial Complex (2009), p. 12
18 Nähere Informationen zur Geschichte und Entwicklung des "European Security Research Programme" finden sich z.B. in Ben Hayes: Arming Big Brother - The EU's Security Research Programme, (2006) und Ben Hayes - NeoConOpticon - The EU Security-Industrial Complex (2009)
19 Bigo, D. & Jeandesboz, J. (2008) Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research.

Das "Europäische Sicherheitsforschungsprogramm" wurde unter FP7 erstmals als eigener Schwerpunkt ausgeschrieben und startete mit der europäischen Sicherheitsforschungskonferenz in Berlin unter deutscher EU-Ratspräsidentschaft. FP7 ist eine Art gemeinsames Dach unter welchem verschiedenste Forschungsprogramme der EU zum Thema Sicherheit und Kriminalitätsbekämpfung zusammengefasst werden. Das Gesamtbudget von FP7 beträgt ca. 50 Mrd. €[20] und umfasste ursprünglich 46, mittlerweile 91 Projekte. Auch hier beschäftigt sich ein Großteil der Projekt sich mit der Entwicklung von Technologien zur Überwachung. Jedes der FP7 Projekte ist um eine koordinierende Institution herum organisiert und wird von unterschiedlich vielen Partnern unterstützt. Finanziert werden die einzelnen Projekte zum Teil von der EU sowie von verschiedenen nationalen und privaten Organisationen und Firmen.

Von den ursprünglich 46 FP7 Forschungsprojekten werden 17 (37%) von Organisationen geleitet, die primär im Verteidigungssektor beschäftigt sind. Weitere fünf Projekte werden von Firmen aus der Sicherheitsindustrie geleitet. Doch der Anschein trügt, dass der Verteidigungssektor nun weniger dominant ist als noch während des PASR Programmes von 2004 bis 2006, denn im Großteil der FP7 Projekte sind mehr oder weniger "bekannte Persönlichkeiten" des Verteidigungssektors vertreten. Die Europäische Kommission bezeichnet ihre Sicherheitsforschung als einen "*public-private dialogue*". Beteiligt sind Schlüsselunternehmen aus der Verteidigungs- und Sicherheitsindustrie und „Endverbraucher" aus nationalen und europäischen Sicherheitsagenturen- und Diensten. Eigentlich steht die Beteiligung an FP7 allen Institutionen in EU-Mitgliedsstaaten und verbündeten Drittstaaten offen, doch ist die Beteiligung und Finanzierung ist sehr unregelmäßig verteilt: Organisationen aus sechs Staaten (Frankreich, U.K., Italien, Deutschland, Schweden und Israel) erhielten den Großteil der finanziellen Zuwendungen.[21]



QUELLE: Review of Security Measures in the Reasearch Framework Programme Study 2010. p. 20

„Seventh Framework Programme" (FP7) Projekte

Das Sicherheitsforschungsprogramm im Rahmen von FP7 befasst sich mit verschiedenen Bereichen rund um das Thema Sicherheit, wie etwa Kriminalitätsbekämpfung, Kriminalitätsprävention oder Kriesenmanagement. Die Schlüsselbereiche des später *FP7 Security Theme* (FP7-ST) genannten Programmes sind:[22]

- *Biometrie und Identifikation*
- *Erkennung und Überwachung*
- *Austausch von Informationen, Risiko-Analyse und Risiko-Vorausschätzung*
- *Schutz kritischer Infrastrukturen, Krisenmanagement und öffentliche Sicherheit*
- *Freiheit und Privatsphäre*

20 http://cordis.europa.eu/fp7/budget_en.html
21 Frankreich (19%), U.K. (15%), Italien (11%), Deutschland (10%), Schweden (9%) und Israel (7%) *Review of Security Measures in the Reasearch Framework Programme Study 2010*, p. 21; Genauere Details zur Finanzierung der Projekte sind zu finden auf den Seiten 20-25
22 Review of Security Measures in the Reasearch Framework Programme Study 2010, p. 25

Diese fünf Schlüsselbereiche sollen nun kurz etwas genauer betrachtet werden. Beginnen wir mit dem letzten Punkt „Freiheit und Privatsphäre“: Innerhalb der 45 Projekte die ursprünglich im Rahmen des FP7-ST Programmes verzeichnet waren, beschäftigen sich insgesamt nur drei davon mit der Untersuchung von gesetzlichen, politischen und sozialen Implikationen der technologischen Entwicklungen innerhalb von FP7-ST. Diese sind: DETECTER („*Detection technologies, terrorism, ethics and human rights*“)[23], INEX („*Converging and conflicting ethical values in the internal/external security continuum in Europe*“)[24] und dem sozialen Komponenten des Projektes GLOBE („*European Global Border Environment*“)[25]. DETECTER und INEX zusammen werden mit € 4.8 Mil., also mit knapp einem Prozent des Gesamtbudgets, finanziert. Im Vergleich dazu werden die Projekte welche sich mit „Erkennung und Überwachung“ befassen (insgesamt 26) mit einem Budget von € 177 Mil. (41.1% des Gesamtbudgets) unterstützt.[26]

Schutz kritischer Infrastrukturen, Krisenmanagement und öffentliche Sicherheit

Der Bereich „Sicherheit von kritischer Infrastruktur und der Öffentlichkeit“ umfasst die Entwicklung von Methoden und Werkzeugen für Krisenmanagement und ist mit einem Budget von € 194,3 Mil. (43.9% der FP7 Gesamtkosten) der größte Bereich von FP7-ST. Inkludiert sind u.a. Projekte wie PROTECTRAIL („*The Railway-Industry Partnership for Integrated Security of Rail Transport*“)[27], eines der größten Projekte von FP7-ST mit einem Budget von € 21,7 Mil., welches, wie der Name schon sagt, sich speziell mit dem Schutz von Bahninfrastrukturen befasst. E-SPONDER („*A holistic approach towards the development of the first responder of the future*“)[28] entwickelt Informations- sowie Command & Control Systeme zur Reaktion im Falle von Zwischenfällen bei kritischen Infrastrukturen. Ähnliche Projekte sind SECRICOM („*Seamless communication for crisis management*“)[29] oder SECUREAU CRISIS („*Security and decontamination of drinking water distribution systems following a deliberate contamination*“)[30]. SPIRIT („*Safety and Protection of built Infrastructure to Resist Integral Threats*“)[31], FRESP („*Advanced first response respiratory protection*“)[32] und DECOTESSC1[33] („*Demonstration of CounterTerrorism System-of-Systems against CBRNE phase 1*“) haben alle ihren Fokus auf CBRNE (chemische, biologische, radiologische und nukleare) Bedrohungen gerichtet.

Austausch von Informationen, Risiko-Analyse und Risiko-Vorausschätzung

16 Projekte finden sich in diesem Bereich, mit einem Gesamtbudget von € 39.4 Mil. (8.9% des Gesamtkosten). Dabei geht es vorrangig um die Entwicklung von Kommunikationsinfrastrukturen zwischen Regierungs- und Sicherheitsagenturen und Krisenmanagement. Hierzu gehören z.B. Projekte wie COMPOSITE („*Comparative Police Studies In The EU*“)[34], EMILI („*Emergency management in large infrastructures*“)[35] oder SCIIMS („*Strategic crime and immigration information management system*“)[36]. Weitere Projekte in diesem Bereich entwickeln unterschiedliche auf neuen Informationstechnologien basierende Werkzeuge. Das INDIGO („*Innovative Training & Decision Support for Emergency operations*“)[37] Projekt etwa hat seinen Fokus auf die Forschung und Entwicklung innovativer Systeme gerichtet, welche mit virtueller Realität, Simulationen und künstlicher Intelligenz arbeiten. Ein weiterer Typ von Projekten befasst sich mit Risiko-Management, wie z.B. EURACOM („*European Risk Assessment and Contingency planning Methodologies for interconnected energy networks*“).[38]

23 http://www.detecter.bham.ac.uk/
24 http://www.inexproject.eu/
25 CORDIS: European Global Border Environment
26 Review of security measures in the Research Framework Programme, European Parliament, Brussels, 2010 p.25, 26
27 CORDIS: The Railway-Industry Partnership for Integrated Security of Rail Transport
28 A holistic approach towards the development of the first responder of the future
29 http://www.secricom.eu/
30 CORDIS: Security and decontamination of drinking water distribution systems
31 CORDIS: Safety and Protection of built Infrastructure to Resist Integral Threats
32 Advanced first response respiratory protection
33 CORDIS: Demonstration of CounterTerrorism System-of-Systems against CBRNE phase 1
34 Comparative Police Studies In The EU
35 Emergency management in large infrastructures
36 Strategic crime and immigration information management system
37 Innovative Training & Decision Support for Emergency operations
38 European Risk Assessment and Contingency planning Methodologies for interconnected energy networks

Biometrie und Identifikation

Die Projekte in diesem Bereich haben insgesamt ein Budget von € 21 Mil. (also 4.76% des Gesamtbudgets der FP7-ST Projekte) und arbeiten an verschiedensten Methoden und Technologien im Bereich der biometrischen Identifikation[39]. Einige dieser Forschungsprojekte sind: EFFISEC („*Efficient integrated security checkpoints*“)[40], in dem man sich mit der Entwicklung effizienter biometrischer Checkpoints beschäftigt, MIDAS („*The Development and Validation of a Rapid Millifluidic DNA analysis system for forensic casework samples*“)[41], forscht im Bereich mobiler Werkzeuge zur Auswertung von DNA, MOBIO („*Mobile Biometry*“) entwickelt bio-modale Authentifikationssysteme für mobile Geräte wie Handys oder PDAs. ACTIBIO („*Unobtrusive authentication using activity related and soft biometrics*“)[42] arbeitet an einem völlig neuen Konzept der biometrischen Authentifikation durch "Extrahierung multi-modaler biometrischer Signaturen" welches, nach eigenen Angaben, völlig unauffällig funtkionieren soll. Das WABY Projekt („*Walk-By Biometric Identification System Based On Face Recognition System*“)[43] entwickelt Systeme zur Echtzeit-Gesichtserkennung in der Videoüberwachung und HIDE („*Homeland security, biometric identification and personal detection ethics*“)[44] zielt darauf ab, eine paneuropäische Dialog-Plattform zu erschaffen welche sich mit "*Ethics and Governance*" von Technologien zur Personenerkennung und Biometrie befassen soll.

Erkennung und Überwachung

Dieser Bereich umfasst 26 Einzelprojekte und macht somit einen sehr großen Teil (40%) des Gesamtumfangs von FP7-ST aus. Die Projekte haben ein Gesamtbudget von € 177 Millionen. In diesem Bereich finden sich einige der interessantesten Projekte (u.a. eben auch Projekt INDECT), deshalb wollen wir uns hier nun etwas detaillierter mit einigen dieser Projekte befassen. Neben INDECT fallen in diesen Bereich Projekte wie: IMSK[45] („*Integrated mobile security kit*“) welches an mobilen Security Kits, kombiniert mit Areal-Überwachung, Checkpoint-Control, CBRNE Aufspürung und VIP Schutz arbeitet. TALOS[46] („*Transportable autonomous patrol for land border surveillance*“) und SFLY („*Swarm of micro flying robots*“)[47] arbeiten beide an autonomen Mini-Hubschraubern und anderen Drohnen für Aufgaben wie Aufklärung, Suche und Rettung, Umweltüberwachung, Gefahrenabwehr, Personenüberwachung, Kontrolle und Rechtsdurchsetzung. Die Koordination für das SFLY Projekt unterliegt der ETH Zürich. Auf der Projektseite[48] von SFLY kann man sich beispielsweise über den aktuellen Stand der Entwicklung informieren. Es wird dort auch darauf hingewiesen, dass heutige Navigationssysteme, die auf GPS-Informationen basieren, für diese Zwecke nicht mehr ausreichend sind. Das von der EU und ESA ins Leben gerufene und mit 4,9 Milliarden € geförderte Projekt *Galileo*[49] wird diesen Mangel aber wohl ausgleichen.

Die EU hat bisher im Rahmen der verschiedenen *Framework* Forschungsprogramme auch mindestens ein Dutzend weitere Projekte finanziert die sich mit der Entwicklung von UVAs („*Unmanned Air Vehicles*“) befassen. Hierzu gehören u.a.: BSUAV („*Border Security Unmanned Aerial Vehicles*“), WIMA2S[50] („*Wide Maritime Area Airborne Surveillance*“) oder auch die mit € 5 Mil. finanzierte CAPECON Studie[51] zur Verwendung von sicheren und günstigen unbemannten Luftfahrzeugen, welche von der israelischen Luftfahrtindustrie geleitet wurde. Des weiteren gibt es das € 5.5 Mil. teure IFATS[52] („*Innovative Future Air Transport System*“) Projekt das sich mit innovativen Luftfahrtsystemen für die Zukunft beschäftigt und an dem ebenfalls die israelische Luftfahrtindustrie, sowie Thales und EADS beteiligt sind, oder auch das

39 Siehe dazu u.a.: Ben Hayes - NeoConOpticon - The EU Security-Industrial Complex (2009)
40 Efficient integrated security checkpoints
41 The Development and Validation of a Rapid Millifluidic DNA analysis system
42 http://www.hideproject.org/references/fp7_projects/ACTIBIO
43 ftp://ftp.cordis.europa.eu/pub/itt/docs/itt99-5_en.pdf
44 http://www.hideproject.org/
45 Integrated mobile security kit
46 http://www.talos-border.eu/
47 http://www.hideproject.org/references/fp7_projects/SFLY
48 http://projects.asl.ethz.ch/sfly/doku.php
49 http://www.esa.int/esaNA/galileo.html
50 http://www.wimaas.eu/pdf/WIMAAS_Description_of_Work.pdf
51 Civil uav application and economic effectiveness of potential configuration solutions (CAPECON)
52 http://www.dlr.de/fl/desktopdefault.aspx/tabid-1149/1737_read-5084/

µDRONES[53] Projekt das u.a. mit Firmen wie Thales UAVs zur Überwachung in urbaner Umgebung entwickelt.

SeaBILLA[54] („*Sea Border Surveillance*“) entwickelt neue Technologien und Werkzeuge zur maritimen Überwachung und iDetecT 4ALL[55] („*Novel intruder detection & authentication optical sensing technology*“) beschäftigt sich mit Überwachungssystemen, Warnvorrichtungen und der Detektion von Eindringlingen in und um kritische Infrastrukturen. SUBITO („*Surveillance of Unattended Baggage and the Identification and Tracking of the Owner*“)[56] forscht und entwickelt an automatisierter Erkennung von verlassenen Gepäckstücken, der schnellen Identifikation der Besitzer und deren Verfolgung.

Sehr interessantest im Bereich „Erkennung und Überwachung“ sind auch Projekte wie ADABTS, ANASID, LOTUS, PROMETHEUS oder SAMURAI – denn sie alle befassen sich auf die eine oder andere Weise mit der Entwicklung von Frühwarnsystemen zur Erkennung von Verbrechen und Bedrohungsszenarien ("*Predictive Analytics*"). Wir wollen diese fünf Projekte nun etwas genauer betrachten:

ADABTS - Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces[57] (Automatische Erkennung von abnormen Verhaltensweisen und Bedrohungen in überfüllten Räumen)

ADABTS soll den Schutz der Bürger, von Eigentum und Infrastrukturen vor einer Bedrohung durch Terrorismus, Kriminalität und Unruhen ermöglichen. ADABTS nutzt dazu die automatische Erkennung „abnormalen“ Verhaltens bei Menschen. Die Unterscheidung zwischen normalem und abnormalem Verhalten wird nach eigenen Angaben zuerst durch erfahrene Bediener von Überwachungskameras getroffen. Aus den so gewonnenen Daten lassen sich dann Algorithmen entwickeln, die selbstständig abnormales Verhalten erkennen können sollen. Für eine genaue Erkennung werden Daten von Audio- und Video-Sensoren mit Kontext-Informationen kombiniert. Die Entwicklung der nötigen Hardware wird u.a. durch die Videospiel-Industrie voran getrieben. Sie bietet ein enormes Potenzial für High-Performance Low-Cost-Überwachungs-systeme. Koordinator von Projekt ADABTS ist das Totalforsvarets Forskningsinstitut (*Schwedisches Verteidigungsforschungsinstitut*). Partner sind das Bulgarische Innenministerium, Detec As (Norwegen), BAE Systems LTD (UK), Stiftelsen Sintef (Norwegen), Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (Niederlande), die Universität von Amsterdam und das Home Office (UK). Die Gesamtkosten des Projektes belaufen sich auf € 4,478,990.

ANASID - Analysing Social Interactions at a Distance[58] (Analyse Sozialer Interaktionen aus der Entfernung)

Ziel der Forschung dieses Projektes ist die automatische Analyse sozialen Verhaltens aus der Distanz als Werkzeug zur Überwachung und zum besseren Verständnis der Benutzung öffentlicher Räume. Koordiniert wird das Projekt von der Universität Amsterdam. Mit einem Budget von € 161,248 gehört dies jedoch eindeutig zu den kleineren Projekten.

LOTUS - Localisation of threat substances in urban society[59] (Lokalisierung von bedrohlichen Substanzen in städtischer Gesellschaft)

Projekt LOTUS erforscht und entwickelt Methoden zur Aufspürung von Produktionsstätten von Bomben und Drogen noch während deren Herstellungsprozessen. Die Hauptaufgabe des Projektes ist die Messung der Ausbreitung von chemischen Ausgangsstoffen bei der Produktion von illegalen bzw. gefährlichen Substanzen und entsprechende Erkennungs- und Überwachungssysteme. Durch die Verwendung vorhandener globaler Infrastrukturen zur Positionierung (GPS) und Netzwerken (GSM) kann das LOTUS

53 Offizielle µDRONES Website
54 Sea Border Surveillance
55 http://www.idetect4all.com/
56 http://www.hideproject.org/references/fp7_projects/SUBITO
57 http://www.hideproject.org/references/fp7_projects/ADABTS
58 http://www.hideproject.org/references/fp7_projects/ANASID
59 http://www.foi.se/FOI/Templates/ProjectPageDesign____7715.aspx

System mehr oder weniger überall auf der Welt mit nur geringen Kosten verwendet werden. Das LOTUS Konsortium besteht aus drei Forschungsinstituten: FOI (Schwedisches Verteidigungsforschungsinstitut), TNO (Niederländische Organisation für Angewandte Naturwissenschaftliche Forschung) und AIT (Österreichisches Technologie-Institut)), zwei Industrieunternehmen (SAAB, Bruker), drei Konzernen (Portendo, Ramem, Bruhn NewTech), der Universität von Barcelona und einer Gruppe nicht näher definierten „Endverbraucher". Gesamtbudget des Projektes: € 4,298,593.

Neben dem LOUS Projekt gibt es auch noch diverse andere Projekte mit dem selben Fokus, u.a.: OPTIX („*Optical technologies for the identification of explosives*")[60], DIRAC („*rapid screening and identification of illegal Drugs by IR Absorption spectroscopy and gas Chromatography*")[61] und PREVAIL („*PRecursors of ExplosiVes: Additives to Inhibit their use including Liquids*").[62]

PROMETHEUS - Prediction and interpretation of human behaviour based on probabilistic structures and heterogeneous sensors[63] (Voraussage und Interpretation von menschlichem Verhalten basierend auf Wahrscheinlichkeitsstrukturen und verschiedenartigen Sensoren)

Dabei handelt es sich um Forschungen im Bereich automatisierter Erkennungsprozesse zur Kurzzeit-Prognose menschlichen Verhaltens, sowie komplexer menschlicher Interaktionen in nicht-begrenzten Umgebungen und simultaner Lokalisierung/Verfolgung mehrerer Menschen, wie auch die Erkennung ihrer Aktivitäten. Koordiniert wird das Projekt vom Totalförsvarets forskningsinstitut, Department of Sensor Informatics (Stockholm, Schweden). Weitere Beteiligte sind: Faculdade Ciencias e Tecnologia, Universität Coimbra (Portugal), Technische Universität München (Deutschland), Universität Patras (Griechenland), Marac Electronics S.A. (Griechenland), Technisches Institut Kreta (Griechenland) und Probayes SAS (Frankreich).

SAMURAI - Suspicious and abnormal behaviour monitoring using a network of cameras & sensors for situation awareness enhancement[64] (Beobachtung von auffälligem und abnormalem Verhalten durch Verwendung eines Kamera-Netzwerkes und Sensoren zur verbesserten Situationserkennung)

Das Ziel von SAMURAI besteht darin, intelligente Überwachungssysteme zur stabilen Beobachtung innerhalb sowie in der Umgebung kritischer öffentlicher Infrastrukturen zu entwickeln und zu integrieren. Im Vergleich zu anderen, ähnlichen Projekten, welche derzeit in der EU und anderswo erprobt werden, kann das Projekt SAMURAI laut eigenen Angaben mit drei bedeutenden Neuerungen aufwarten:

- SAMURAI verwendet verschiedenartige vernetzte Sensoren, anstatt nur der CCTV Kameras[65], sodass multiple ergänzende Informationsquellen integriert werden können um Visualisationen zu erzeugen welche ein vollständigeres Bild belebter öffentlicher Plätze bieten sollen.
- bereits existierende Systeme sind auf die Analyse aufgezeichneter Videodaten fokussiert und verwenden dazu vordefinierte Regeln, was häufig inakzeptable Fehlalarme zur Folge hat. SAMURAI entwickelt ein lernfähiges Verhaltens-Profiling in Echtzeit, ein Erkennungssystem für abnormales Verhalten sowie ein Prognosesystem mit angeblich weitaus weniger Fehlalarmen.
- zusätzlich zu fix positionierten CCTV Kameras kann das SAMURAI System auch Input von Steuerungszentralen und von mobilen Sensoren verarbeiten um ein hybrides, kontextbezogenes Erkennen von abnormalem Verhalten zu gewährleisten.

Weitere Zielsetzungen von SAMURAI sind:

- Entwicklung innovativer Werkzeuge und Systeme um innerhalb eines Netzwerkes von Kameras unter realen Bedingungen Menschen, Fahrzeuge und Gepäckstücke zu erkennen, zu verfolgen und

60 CORDIS: Optical technologies for the identification of explosives
61 CORDIS: rapid screening and identification of illegal Drugs
62 CORDIS: Precursors of Explosives
63 http://www.hideproject.org/references/fp7_projects/PROMETHEUS
64 http://www.samurai-eu.org/
65 Closed Circuit Television (CCTV)

zu kategorisieren.

- Entwicklung eines Systems zu Erkennung abnormalen Verhaltens basierend auf verschiedenartigen Sensor-Netzwerken, bestehend aus aus fix-positionierten CCTV Kameras und mobilen, tragbaren Kameras mit Audio- und Positionssensoren.
- Entwicklung von Werkzeugen unter Verwendung von multimodaler Datenverschmelzung und Visualisation von verschiedenartigen Sensoren-Inputs zur effizienteren Bearbeitung von Anfragen durch Steuerungszentralen.

Die Projektkoordination von SAMURAI erfolgt durch das Queen Mary and Westfield College an der Universität London (UK). Weitere Beteiligte sind: Borthwick-Pignon Ou (Estonia), Elsag Datamat S.p.A. (Italien), BAA Limited (UK), Syndicat Mixte des Transports pour le Rhone et l'Agglomeration Lyonnaise (Frankreich), Waterfall Solutions Ltd. (UK), Universität Verona (Italien), Esaprojekt SP. Z.O.O (Polen). Die Gesamtkosten des Projektes belaufen sich auf € 3,638,131.

Die EU finanziert darüber hinaus auch diverse Projekte die auf "*Data-minin*g" in verschiedensten Formen abzielen, wie etwa das ADMIRE[66] („*Advanced Data Mining and Integration Research for Europe*“) Projekt, das konsistente und benutzerfreundliche Technologien zur Extrahierung von Information und Wissen aus verschiedensten Quellen entwickelt.

Wir haben hier also Projekte zur automatischen Erkennung von abnormen und auffälligen Verhaltensweisen und Bedrohungen, selbst in überfüllten Räumen, durch Verwendung von Kamera-Netzwerken und anderen, nicht weiter definierter Sensoren. Projekte zur Analyse sozialer Interaktionen aus der Entfernung, zur Voraussage und Interpretation von menschlichem Verhalten basierend auf Wahrscheinlichkeitsstrukturen und verschiedenartigen anderen Sensoren. Projekte zur Lokalisierung von bedrohlichen Substanzen in urbaner Umgebung, Projekte die an Drohnen in verschiedenster Form forschen und Projekte, die an innovativen Technologien zur Datensammlung aus allen nur verfügbaren Quellen arbeiten. Und dies sind nur ein paar wenige der insgesamt 91 Projekte von FP7-ST. Kurz gesagt: es wird an allen nur erdenklichen Methoden und Technologien zur Kontrolle und Überwachung gearbeitet.

Als Anmerkung am Rande: Ein ähnliches, beinahe noch mehr nach Science Fiction klingendes Projekt, wird derzeit von den USA erprobt – es nennt sich *Future Attribute Screening Technology (FAST) Project.* Das Projekt ist Teil des *Homeland Security Advanced Research Project Agency (HSARPA)* Programms bzw. der *Human Factors/Behavioral Sciences Division (HFD)* und ist eine Initiative zur Entwicklung von „nicht in die Privatsphäre eingreifenden“ („*non-invasive*“) Technologien zur Überprüfung von Menschen an Sicherheits-Checkpoints. FAST basiert angeblich auf Forschungen zu menschlichem Verhalten und Psychophysiologie, mit dem Ziel, Menschen mit „*malintent*“ (also mit „schädlichen“) Absichten anhand ihrer Herzschlagfrequenz, Hauttemperatur und Mimik zu identifizieren.[67] Laut dem Magazin *NewScientist* liegt die Genauigkeit dieses FAST-Verfahrens mittlerweile bei 78% hinsichtlich der „*malintent*“ Erkennung, und bei 80% bei Täuschungsversuchen.[68] Falls Sie also kurz vor Ihrer nächsten Einreise in die USA mit Ihrem Partner gestritten haben, von Ihren Kindern genervt worden sind oder auch nur etwas schlechtes gegessen haben, dann sollten Sie sich vor Security-Checkpoints vorsehen...

Nach diesem kurzen Überblick über einige der gegenwärtig im Rahmen des europäischen Sicherheits-forschungsprogrammes laufenden Projekte stellt man sich vielleicht die Frage: Wie soll man die riesige Datenflut überhaupt bewältigen, wenn all diese Technologien irgendwann wirklich eingesetzt werden? In London beispielsweise gibt es mittlerweile so viele Überwachungskameras, das sich all die Aufzeichnungen gar keiner mehr anschauen kann. Und den ganzen Tag lang in zwanzig Monitore gleichzeitig zu starren um etwaige Verbrechen oder Gefahren zu identifizieren ist wohl auch keine sonderlich angenehme Tätigkeit.

Die riesigen Mengen an Daten aus dem Internet, der Telekommunikation, von Videokameras usw. ist mit den gegenwärtigen Verfahren unmöglich zu bearbeiten. Doch genau hier kommt INDECT ins Spiel. INDECT soll all diese Daten vollautomatisch analysieren und interpretieren – und das in Echtzeit.

66 http://www.admire-project.eu
67 Siehe dazu: http://www.dhs.gov/files/programs/gc_1218480185439.shtm#9 und Implementing Privacy Protections in Government Data Mining
68 http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html

Das INDECT Projekt

INDECT[69] ist ein Akronym das auf Deutsch soviel bedeutet wie „*Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Entdeckung für die Sicherheit von Bürgern in städtischer Umgebung.*“ Die Gesamtkosten für dieses Projekt belaufen sich auf ca. €15 Mil.[70], somit gehört es ganz klar zu den größeren Projekten im Rahmen des FP7. Das Projekt läuft seit Januar 2009 bis voraussichtlich 31.12.2013 und es hat sich zum Ziel gesetzt, eine Sicherheitsarchitektur zu entwerfen, die sämtliche bestehende Technologien – Videoüberwachung, Vorratsdatenspeicherung, Telekommunikation, Gesichtserkennung, Websites, Diskussionsforen, Usenet-Gruppen, Datenserver, P2P-Netzwerke sowie individuelle Computersysteme und alle vorhandenen Datenbanken wie Namen, Adressen, biometrische Daten, Interneteinträge, polizeiliche, geheimdienstliche, militärische, forensische und zivile Datenbanken, Daten von luft- und seegestützte Plattformen und Satelliten (und letztendlich dann auch wohl die Daten der oben erwähnten FP7-ST Projekte) – logisch miteinander verknüpft, in Echtzeit auswertet und verwaltet. Aus den zusammengefassten Daten sollen dann mittels intelligenter Computeranalyse von Verhalten und Sprache kriminelle und „abnormale“ Aktivitäten und Bedrohungen automatisch frühzeitig erkannt und gemeldet werden. So soll sich dann beispielsweise die Identität einer Person, die sich etwa durch extremistische Postings in einem Forum verdächtig macht, mit Hilfe von Verbindungsdaten ermitteln lassen die im Zuge einer Vorratsdatenspeicherung angefallen sind. Ist der Verdächtige identifiziert, könnte er von Überwachungskameras bzw. von Drohnen weiter observiert werden. Und dies ist nur eines von vielen möglichen Szenarien.

Erich Moechel von *Futurezone.at* meint dazu: *„Der Gesamtverbund aus Backbone, Funkkommunikations-knoten, vernetzten statischen oder mobilen Sensoren und Kameras, GSM/GPS-Trackern, unbemannten Flugkörpern sowie Servern, Datenbanken und Client-Workstations unterscheidet sich praktisch nicht von militärischen Gefechtsfeldzentralen. Bei INDECT handelt es sich demnach schlicht um eine verkleinerte Ausgabe der in der vernetzten Kriegsführung seit mehr als einem Jahrzehnt eingesetzten und ständig weiterentwickelten militärischen Kommando- und Kontrollsysteme (C4).“*[71]

Die Betreiber von INDECT, allen voran die "Polnische Plattform für Heimatschutz", betonen stereotyp, INDECT sei ein rein wissenschaftliches Projekt. Auf der Website heißt es dann auch "*INDECT ist ein Forschungsprojekt. Die Liste der Projektziele enthält definitiv KEINE Form der globalen Überwachung IRGENDEINER Gesellschaft."* Direkt darunter sind die eigentlichen Ziele aufgezählt: *"Eine Versuchsinstallation des Kontroll- und Überwachungssystems im urbanen Raum"* ist ebenso dabei wie *"ein System zur mobilen Objektverfolgung" oder "kontinuierliches und automatisches Monitoring öffentlicher Ressourcen wie Websites, Diskussionsgruppen, Usenet-Gruppen, Fileservern, P2P-Netzwerken wie auch privaten Computersystemen.*"

INDECT wird von der AGH Univeristy of Science and Technology in Polen koordiniert und steht unter der Leitung von *Andrzej Dziech*.[72] Insgesamt sind neun Ländern, zehn Universitäten, fünf Privatunternehmen und zwei Polizeibehörden an dem Projekt beteiligt[73]. Außerdem ist das deutsche Bundeskriminalamt (BKA) in einer beratenden Funktion im Projekt involviert[74], was allerdings nur selten Erwähnung findet und weder vom deutschen Innenministerium noch auf der offiziellen Projektseite bestätigt wird[75]. Das BKA hatte allerdings auch schon 2005 im "*European Security Research Advisory Board*" (ESRAB) mitgearbeitet, das wesentliche Grundlagen für das aktuelle Europäische Sicherheitsforschungsprogramm lieferte.

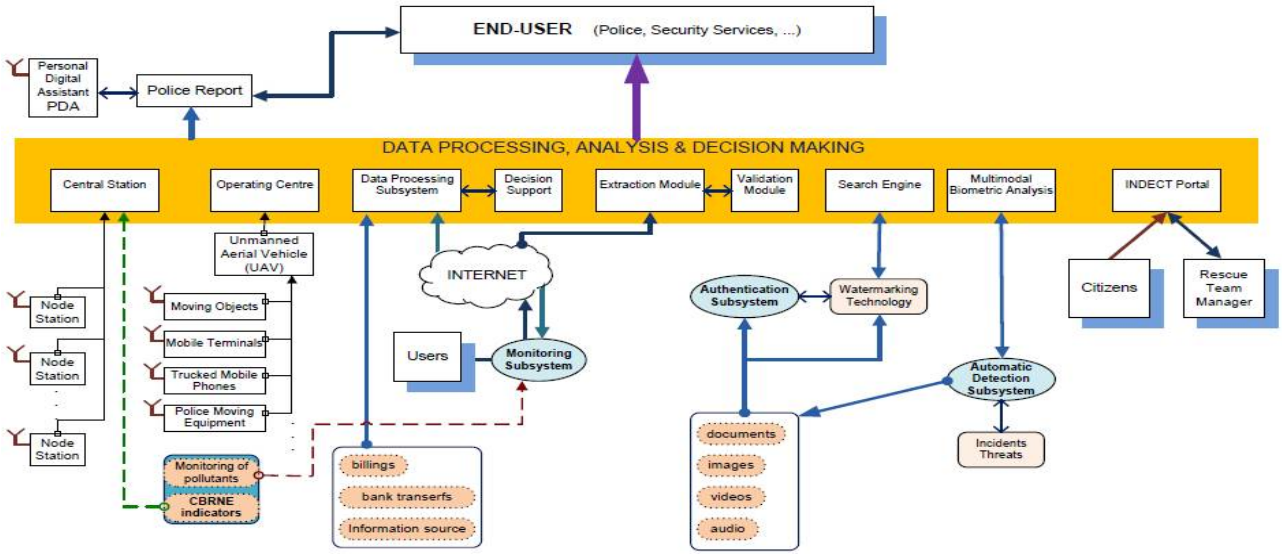
69 http://www.indect-project.eu/
70 ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf
71 http://www.futurezone.at/stories/1660457/
72 Intelligent information system supporting observation, searching and detection for security of citizens in urban environment
73 AGH - University of Science and Technology (Polen), Gdanst University of Technology (Polen), InnoTec DATA G.m.b.H. & Co. KG (Deutschland), Grenoble INP (Frankreich), General Headquarters of Police (Polen), Moviquity (Spanien), PSI Transcom GmbH (Deutschland), Police Service of Northern Ireland (UK), Poznan University of Technology (Polen), Universidad Carlos III de Madrid (Spanien), Technical University of Sofia (Bulgarien), University of Wuppertal (Deutschland), University of York (UK), Technical University of Kosice (Slovakei), X-Art Pro Division G.m.b.H. (Österreich) und Fachhochschule Technikum Wien (Österreich), genauere Information zu den einzelen Tätigkeisbereichen der verschiedenen beteiligen Partner sind auf der offiziellen Webseite zu finden: http://www.indect-project.eu/indect-partners
74 http://www.if.pw.edu.pl/~krab/INDECT-PREZENT.pdf und Präsentation zu INDECT von Tomasz Ruść vom 18.2.2010
75 Zeit Online: Der Rechner als Polizist, Anna Sauerbrey, 27.10.2010

Hauptziel des INDECT Projektes ist:

- Die Entwicklung einer Plattform für die Registrierung und den Austausch von Einsatzdaten, die Erfassung von Multimedia-Inhalten, sowie intelligentes Verarbeiten aller Informationen und automatische Erkennung von Bedrohungen, abnormem Verhalten oder Gewalt.
- Entwicklung eines Prototyps eines integrierten, vernetzten Systems zum Unterstützen der Einsatzaktivitäten von Polizeibeamten mithilfe von Techniken u. Werkzeugen für die Observierung verschiedener mobiler Objekte.
- Entwicklung einer neuen Art von Suchmaschine, in der die direkte Suche von Bildern und Videos basierend auf Wasserzeichengeschützten Inhalten mit der Speicherung von Metadaten in Form von digitalen Wasserzeichen kombiniert wird.
- Entwicklung einer Reihe von Techniken zum Unterstützen der Überwachung des Internets, der Analyse der gesammelten Informationen, des Erkennens von kriminellen Aktivitäten und Bedrohungen.

Das Kernstück der Forschungsarbeit ist die Integration von Sicherheitssystemen mit den immer weiter verbreiteten drahtlosen Kommunikationssystemen sowie selbstorganisierenden Computernetzwerken, um die Erfassung, Auswertung, Verteilung und Unterstützung von Sicherheitsinformation über Bürger zu ermöglichen. INDECT plant die Forschung in mehrere Richtungen durchzuführen:

- Beobachtung verschiedener Menschenansammlungen und Erkennung von abnormalem Verhalten sowie gefährlicher Situationen.
- Entwicklung und Evaluierung von komplexen, mehrschichtigen biometrischen Verfahren und Systemen zur Authentifizierung (in Schulen, Spitälern, Büros, etc.), sowie zur Identifizierung (um z.B. die Schuldigen in gefährlichen Situationen auszumachen).
- Daten aus dem Internet sammeln, sowie die Beobachtung verdächtiger Aktivitäten im Internet.
- Entwicklung automatischer Benachrichtigungsdienste basierend auf den immer weiter verbreiteten drahtlosen Kommunikationssystemen, sowie selbstorganisierenden Computernetzwerken.
- Entwicklung neuer Methoden und Suchmaschinen basierend auf digitalen Wasserzeichen.



QUELLE: INDECT Präsentation von Andrzej Dziech, Security R&D Innovation for the Citizens Stockholm, 29-30 September 2009[76]

76 http://www.src09.se/upload/Presentations/Day_1/Sessions-1100-1245/Session-1-Hall-B/Dziech.pdf

Erwartete Resultate aus dem Projekt sind:[77]

Eine Pilotinstallation des Beobachtungs- und Überwachungssystems in verschiedenen städtischen Ballungszentren, und

- die Demonstration dieses Prototyps in einem System mit 15 Knotenpunkten (= Überwachungs-stationen).
- Implementierung eines verteilten Computersystems, welches in der Lage ist alle Daten zu Erfassen, zu Speichern und nach Bedarf effektiv zur Verfügung zu stellen, sowie diese "intelligent zu verarbeiten".
- Die Erzeugung einer Familie von Geräten zur mobilen Zielverfolgung.
- Realisierung der Suchmaschine für das schnelle Aufspüren von Personen und Dokumenten, unter Verwendung der Wasserzeichen-Technik. Dabei sollen bisherige Forschungsergebnisse für die semantische Suche, basierend auf Wasserzeichen, einfließen.
- Realisierung von sog. „Agenten“ zur fortwährenden und automatischen Beobachtung von öffentlichen Ressourcen wie: Webseiten, Diskussionsforen, UseNet Gruppen, Fileserver, p2p Netzwerken, sowie individuellen (privaten) Computersystemen.
- Ausführliche Vorführung dieses internetbasierten Datensammel- und Überwachungssystems, sowohl aktiv als auch passiv, und Demonstration seiner Effizienz in einer messbaren Art und Weise.

Das Projekt INDECT wurde in 10 Arbeitspakete (*Work Packages*) gegliedert.[78] In Analogie zu Schichtenmodellen[79] aus der Netzwerktechnik sind die Technik-orientierten Arbeitspakete in 3 Schichten (*Layer*) unterteilt: 1) *Intelligente Analyse und Entscheidungsunterstützung*, 2) *Datenverarbeitung und -analyse,* und 3) *Physische Schicht*. Schauen wir uns die verschiedenen Work Packages – wie in „*Deliverable 9.4: Evaluation of Components*“ beschrieben – nun etwas genauer an:[80]

Work Package 1

Das Hauptziel dieses Arbeitspaketes besteht darin, öffentliche Räume zu beobachten und Menschen und Bedrohungen zu erkennen. Quellen für die Erkennung und Überwachung sind Video, Audio, Roh- und alphanumerische Daten. Zudem sieht WP1 vor, Algorithmen für eine “Event-Detection” in Video und Audiodaten zu entwickeln.

77 http://euro-police.noblogs.org/gallery/3874/Expectations_of_end_users.pdf
78 http://www.src09.se/upload/Presentations/Day_1/Sessions-1100-1245/Session-1-Hall-B/Dziech.pdf
79 Siehe dazu: http://en.wikipedia.org/wiki/OSI_model
80 Siehe: Deliverable 9.4 - Evaluation of Components

Im Rahmen von WP1 sollen so genannte „*Node Stations"* - kleine, tragbare Computereinheiten - entwickelt werden, die die gesammelten Daten vorverarbeiten und die gewonnenen Informationen an einen entfernten Server schicken. *Node Stations* sollen mit Mikrophonen, Kameras (fix oder mobil) und Sensoren kommunizieren können. Die Systeme sollen mit hochauflösenden Videos und mit hohen Frameraten umgehen können und schicken ihre Daten, versehen mit Metadaten (Beschreibung, GPS-Position, Ort, Zeit, etc.), an eine Zentrale oder auch an verschiedene mobile Stellen. Video und Audiostreams können in den *Node Stations* codiert und an Endgeräte verschickt werden. Sie sollen miteinander kommunizieren können und somit eine Überwachung von z.B. Personen oder Fahrzeugen über mehrere Bereiche, überwacht von verschiedenen *Node Stations*, hinweg verfolgen zu können.

Es soll also ein dezentrales System entstehen, an dessen Endpunkten die *Node Stations* stehen. Die erkannten "gefährlichen" Ereignisse werden an eine „*Central Station"* weitergeleitet. An dieser können viele, sogar einige hundert *Node Stations* angeschlossen sein. In der *Central Station* kommen also keine Livestreams von Videokameras an, sondern nur die erkannten Ereignisse („*Event-Detection*") in dem überwachten Bereich. Video- und Audiobeweise dieser gefährlichen Ereignisse können auch an mobile Endgeräte verschickt werden. Damit kann ein Überwacher auch mobil sein: *"Designed Mobile Terminal is based on PDA preferably operating Windows Mobile"*.

Work Package 2

Haupziel von WP2 ist die Entwicklung von Technologien zur Überwachung jeglicher beweglicher Objekte. In WP2 sollen Geräte entwickelt werden, die in permanenter kabelloser Verbindung zum zentralen Element dieses System stehen sollen. Darüber sollen Polizeibeamte dann detaillierte Informationen über das überwachte Objekt abrufen können. Ein zentrales Element ist die Entwicklung von UAVs („*Unmanned aerial vehicles*" - also Quadrocopter und andere Drohnen) für die lückenlose und flexible Überwachung von mobilen Objekten. Die entwickelten Algorithmen sollen auch die wahrscheinlichste zukünftige Position des Überwachten voraussagen und eine effiziente Navigation der Polizeibeamten bieten. Die entwickelten UAVs sollen "intelligent und autonom" vernetzt sein und so verdächtige Objekte auch im städtischen Raum verfolgen können.

Work Package 3

In WP 3 geht es in erster Linie um die Entwicklung von Technologien die bei der Überwachung des Internets, bei der Analyse von erlangten Informationen und bei der Erkennung von illegalen Aktivitäten helfen sollen, sowie um die Entwicklung entsprechender Softwarelösungen. Es sollen Technologien entwickelt werden, die zur Erkennung von kriminellen Aktivitäten im Internet dienen. Dazu müssen Informationen aus dem Internet gesammelt werden (automatisch und regelmäßig): von Webseiten, Foren, UseNet-Gruppen, Fileservern, P2P-Netzwerken und privaten Computersystemen. Es sollen Inhalte und Verkehrsdaten überwacht werden. Die Projektpartner nennen diese Überwachungskomponenten "Agenten".

Work Package 4

WP 4 beschäftigt sich mit der Entwicklung von Systemen zur Informationssammlung im Internet indem jeder beliebige Text (auch in natürlicher Sprache) erfasst werden kann. Eines der Planziele des WP4 ist es, dass durch Informationen auf Webseiten und sozialen Netzwerken Beziehungen erkannt werden. In diesem System sollen auch Graphen erstellt werden können, indem Knoten Personen und Kanten zwischen zwei Knoten eine Beziehung widerspiegeln. Ein weiteres Planziel ist es, dass das System durch bekannte Kiminelle und deren Verhalten lernt und so zukünftige illegale Aktivitäten von anderen Personen erkennt. Verdächtige Webseiten sollen, als weiteres Planziel, automatisch erkannt werden und verschiedenste Datenbanken (öffentlich, polizeiliche,…) sollen problemlos eingebunden und durchsucht werden können. *(Stichwort: Vorratsdatenspeicherung, SWIFT, Passenger Name Record, u.v.m).*

Work Package 5 & 6

In diesen zwei Arbeitspaketen geht es darum, ein System zum durchsuchen und speichern von Multimedia-daten zu entwickeln und eine Plattform für INDECT inklusive Suchmaschine einzurichten.

Work Package 7

Dieses Arbeitspacket beschäftigt sich mit Algorithmen zur Erschaffung „künstlicher Intelligenzen“ zur Erkennung von Personen (über biometrische Daten) und von kriminellem Verhalten (Emotionen, Gesichtszüge, etc.)

Work Package 0, 8 & 9

Die Arbeitspakete 0, 8 und 9 haben organisatorischen Charakter und sind daher schichtenübergreifend: In WP0 geht es um Projektmanagement, WP8 behandelt das Management der Datensicherheit und den Schutz der Privatsphäre und WP9 beschäftigt sich mit Qualitätssicherung.

INDECT und die Medien

Im Rahmen einer Präsentation auf der jährlich stattfindenden Konferenz "*Future Security*" erklärte der polnische Projektkoordinator *Andrzej Dziech* 2008 (also noch vor offiziellem Projektbeginn) gegenüber Journalisten, dass INDECT zur Fußball-EM 2012 in Polen getestet werden soll.[81] Verdächtige Personen und auffälliges Verhalten während der EM würden demnach automatisiert analysiert und im Ereignisfall ein Alarm an einen Operator ausgegeben. Mittels Audio-Sensoren könnten zudem Fan-Gesänge ausgewertet werden und im Falle „bedrohlicher Gesänge“ Sicherheitspersonal bzw. Polizisten auf den Plan gerufen werden.

Laut Informationen eines Projektpartners[82] ist auch eine der involvierten Universitäten als Testlandschaft für 2012 im Gespräch. Die Testinstallation soll 15 der weiter oben erwähnten "*Node Stations*" umfassen. Sie würden mit folgenden Komponenten ausgestattet: Kamera, Mikrofon, biometrische Sensoren, GPS, Mikro-Sender und RFID-Tag.

Im Herbst 2009 (als neun Monate nach Beginn des Projektes) berichtete der *Telegraph* als erstes Mainstream-Medium über INDECT unter dem Titel: "*EU-finanziert Orwells künstlichen Intelligenz Plan zur Überwachung der Öffentlichkeit bei "abnormem Verhalten*". Der *Telegraph* zitierte dort *Stephen Booth*, einen Wissenschaftler des Think Tanks "*Open Europe*": *„Das ist nach meiner Meinung alles ziemlich beängstigendes Zeug. Diese Projekte würden eine riesige Invasion der Privatsphäre bedeuten und die Bürger müssen sich fragen, ob die EU wirklich ihre Steuergelder für so etwas ausgeben sollte."*[83]

Einige europäische Medien zogen nach und berichten ebenfalls über INDECT. Unter ihnen *Die Zeit*, die *taz*, *futurezone*, *der Standard* und *El País*. Insgesamt hielt sich die Berichterstattung allerdings sehr in Grenzen und interessanterweise berichteten hauptsächlich deutschsprachige Medien über das Thema. So hieß es in der *taz*[84]: *„Die EU stellt die Weichen für zukünftige Sicherheitspolitik, ohne dass die Medien sich groß dafür interessieren.“* In einem Artikel der *Zeit Online* vom September 2009 hieß es u.a.:[85]

„Wird das Projekt umgesetzt, wäre es der Albtraum jeder Bürgerrechtsbewegung. Verbindet es doch alle einzelnen Überwachungsinstrumente, die bereits jetzt installiert sind wie Videokameras, Vorrats-datenspeicherung, Handyortung, Gesichtserkennung oder Telefonüberwachung zu einem einzigen Spähprogramm.“

81 http://www.heise.de/tp/r4/artikel/33/33282/1.html bzw. http://futurezone.orf.at/stories/1631510
Die http://www.indect-project.eu URL wurde ebenfalls bereits am 26. Februar 2008 registriert
82 http://www.psitrans.de/de/ptr-applications/forschungsprojekte/indect/
83 http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung bzw. Telegraph, *Ian Johnston,* 19 Sep 2009
84 http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/die-moderne-verbrecherjagd/
85 http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

Die durchwegs negative Berichterstattung der Medien hatte zur Folge, dass die Geheimhaltungsvorschriften des Projektes verschärft wurden, und so wurde es auch in den Medien wieder recht still um dieses Thema – bis Ende 2010. Seit November 2010 setzen sich nun auch studentische Gremien der Universität Wuppertal kritisch mit dem Projekt auseinander und in Polen trafen sich Studenten mit beteiligten Professoren. Auch die Medien berichten nun wieder gelegentlich. So hieß es auf *Telepolis* im Oktober 2010:[86]

„Das EU-Sicherheitsforschungsprojekt INDECT geht zur Geheimniskrämerei über. Gleichzeitig werden erstmals Testreihen im öffentlichen Raum vorbereitet. In einem kürzlich auf der Projektseite online gestellten Arbeitsbericht gehen die INDECT-Macher auf Konfrontationskurs mit der kritischen Öffentlichkeit. Weil sich die Projektbeteiligten von Journalisten und Datenschützern "missverstanden" fühlen, sollen Informationen nur noch gefiltert nach außen gelangen. Zuständig ist hierfür ein "Ethics Board", das sich aus Polizisten, Überwachungsforschern und Professoren zusammensetzt. Die meisten Mitglieder des Ethikrats sind selbst an der INDECT-Forschung beteiligt.“

Der Ethik-Rat und die Geheimhaltung

Die bisherige Kritik der Geheimniskrämerei hatte einen Versuch zur Stärkung des Ethik-Rats des Projektes zur Folge gehabt, jedoch ist dieser nun selbst Ziel heftiger Kritik geworden – was allerdings vor allem die Schuld des Ethik-Rates selbst ist. So kommt er unter anderem zur fragwürdigen Einschätzung, Daten aus Videoüberwachung seien "weniger sensibel" als jene aus der Telefon-Überwachung.[87] Außerdem besteht dieses INDECT *Ethics Board* aus zehn Mitgliedern von denen die meisten Polizeibeamte[88], und fast alle auch anderweitig in das Projekt involviert sind. Als Ethik-Beauftragter von INDECT wurde mit *Assistant Chief Constable Drew Harris*[89] ausgerechnet ein britischer Polizist benannt, Vorsitzender des Ressorts "*Hate Crimes*" in der britischen *Association of Chief Police Officers* (ACPO). Insgesamt sind nur drei der Mitglieder unabhängige Experten, wie z.B. der Ethikprofessor *Tom Sorrell* von der Universität Birmingham, welcher zu den ethischen Bedenken der Kritiker des Projektes lapidar meinte: *„Nicht nur die Projektpartner müssen sich viel mehr mit den ethischen Aspekten auseinandersetzen, sondern auch die Kunden.“*[90]

Auch ein internes Demonstrationsvideo[91] des Projektes welches erstmals auf der jährlichen Sicherheitsforschungskonferenz unter schwedischer Ratspräsidentschaft in Stockholm gezeigt wurde und anschließend an die Öffentlichkeit gelangte, hatte nicht sonderlich positive Auswirkungen auf das Image des Projektes. Denn das Demonstrationsvideo illustriert bestens den technokratischen Machbarkeitswahn der beteiligten Forscher. Das Video wirkt wie ein schlecht gemachter Krimi. Darin stiehlt ein Mann Unterlagen des Forschungsprojektes aus dem Büro von *Andrzej Dziech*. Beim Verlassen des Gebäudes wird er sofort von einer Videokamera erfasst. Dank allgegenwärtigen Überwachungskameras, automatischer Gesichts- und Autonummernschilderkennung und Ortung wird der Täter in Kürze von einer schwerbewaffneten Sondereinheit der Polizei geschnappt und die Aktenmappe sichergestellt.

Ein weiterer Grund für die Kritik an dem Ethik-Rat liegt an einem von ihm veröffentlichen Dokument aus dem hervorgeht, dass die Behandlung ethischer Aspekte Zeit beanspruchen würde, die im Rahmen des Projekts nicht zur Verfügung steht. Es wird daher empfohlen, einfach die Veröffentlichung jeglicher Projektinhalte, die eine negative Auswirkung auf die "organisatorische Reputation" haben könnten, sowie anderer sensibler Themen einzustellen. In dem Papier heißt es, dass man *„Themen, die sich negativ auf die Strafverfolgungsbehörden, die nationale und öffentliche Sicherheit oder das Ansehen der Beteiligten auswirken könnten, nicht mehr der Öffentlichkeit zur Verfügung stellen zu wolle“*[92]. Der Ethik-Rat scheint sich demnach ganz offensichtlich mehr um die PR des Projektes als um etwaige ethische Bedenken zu kümmern.

Abgeordnete des Europäischen Parlaments richteten bereits 2009 eine Anfrage zum INDECT Projekt und seinen Datenschutzaspekten an die Europäische Kommission. Eine der Antworten der Kommission war:

86 http://www.heise.de/tp/r4/artikel/33/33282/1.html
87 http://www.heise.de/tp/r4/artikel/31/31802/1.html
88 http://www.indect-project.eu/ethics-board-members
89 Assistant Chief Constable Drew Harris OBE - Crime Operations Department
90 http://www.zeit.de/2010/31/A-Ueberwachung
91 http://en.wikinews.org/wiki/File:INDECT-400px.ogv
92 Deliverable 0.5: Ethical Issues - 2009, p. 10

"Die Kommission wird die Aufnahme eines zusätzlichen, unabhängigen Experten in den Ethik-Rat des Projektes anregen, um die Rolle des Ethik-Rates weiter zu stärken. Dieser Experte soll nachweisliche Expertise in Fragen der Ethik und des Datenschutzes mitbringen".[93] Der Ethik-Rat ist aber weiterhin von Polizeioffizieren und nicht von Datenschutz-Experten dominiert.[94]

„Abnormales Verhalten“

Ein wesentlicher Kritikpunkt an dem ganzen Unternehmen INDECT besteht darin, es „intelligenten“ Computersystemen zu überlassen, „abnormales“ von „normalem“ Verhalten zu unterscheiden. Zwar beruft sich der Ethik-Rat von INDECT darauf, dass die Verhaltensmuster erst später von den Endanwendern definiert werden, allerdings ging man dann doch so weit, typische äußerliche Erkennungsmerkmale von Dieben oder Dealern definieren zu wollen.

Um mittels Computer-Algorithmen aber erkennen zu können, welche Verhaltensweisen in das Raster von „abnormal“ bzw. „verdächtig“ fallen, benötigt man natürlich Definitionen davon. Verhaltensbiologen würden vom klassischen Ethogramm[95] sprechen. Da Ethogramme von Verbrechern aber nicht so einfach zu bekommen sind, hat man sich im INDECT-Programm für den guten, alten Fragebogen-Ansatz entschieden. Dabei hat man mehreren hundert polnischen Polizisten Fragebögen vorgelegt, bei denen sie ausfüllen sollten was generell oder auch ortsspezifisch für sie verdächtiges Verhalten ist. Antworten auf diese Frage waren häufig "Herumlungern", "sich umsehen", "zu lange an einem Ort sitzen", "rennen" oder einen "längeren Aufenthalt in Türbereichen." Einige weitere dieser Fragen waren: *"Wie würden sie eine bestimmte Person des folgenden Typs erkennen, an der Kleidung, am Verhalten: Räuber, Taschendieb, Drogendealer, Drogenabhängiger, verlorenes Kind, Pädophiler, Terrorist, Hooligan." „Woran erkennt man Autodiebstähle, Vandalismus, Bedrohung mit Waffengewalt etc.?“ „Woran erkennt man Personen, die Hilfe benötigen?“ „Welche Bewegungsarten zeichnen gefährliche Situationen in Massenveranstaltungen aus?“* Aus den Fragebögen-Ergebnissen wird abgeleitet, welche Verhaltensweisen automatisiert erkannt werden sollen: 1) Bewegung in die "falsche" Richtung, 2) Herumlungern, 3) Treffen von mehr als X Personen, 4) Autodiebstahl, 5) Laufen, 6) fallende Personen, 7) Gepäck vergessen, 8) Herumsitzen, 9) länger als Dauer X, 10) Hilfeschreie, 11) Schüsse, Explosionen, Schreie, fluchende Personen.[96]

Die Polizisten die an der Umfrage teilgenommen haben sind zum Großteil nicht definiert, über deren Expertise liegt in den meisten Fällen keine Information vor, und so ist die gesamte Stichprobe der Befragten nichts weiter als ein schwammiges, unwissenschaftliches Etwas.

Das man es in diesem Projekt mit der Wissenschaftlichkeit des öfteren nicht so genau nimmt zeigt schon eine oberflächliche Suche nach Belegen für manche in den veröffentlichten Texten aufgestellte Behauptungen. So findet man etwa folgende Aussage: *„Das rasante Anwachsen des Aufkommens an Videodaten [...] zeigt sich deutlich im Vereinigten Königreich. London wird als die Stadt mit der höchsten Dichte an Überwachungskameras weltweit angesehen. Zugleich ist die öffentliche Akzeptanz hoch, da die Einwohner darüber informiert sind und die erhöhte Sicherheit in den überwachten Gebieten schätzen.“* Die Quelle für diese Behauptung ist ein technischer Bericht aus dem Police Department des britischen Innenministeriums aus dem Jahr 1992 (sic!). Die zugehörige Fußnote "[48]" befindet sich im Anhang des Dokuments.[97]

Schweigen auf der einen, heftige Kritik auf der anderen Seite

Im Europäischen Parlament regt sich mittlerweile ein wenig Protest gegen das Sicherheitsforschungsprojekt. Mehrere EU-Abgeordnete haben im Juli 2010 in Brüssel eine Initiative für eine schriftliche Erklärung[98] der Volksvertreter zu dem umstrittenen Überwachungsprojekt vorgestellt, das ihrer Ansicht nach tief in die Grundrechte der EU-Bürger einschneiden könnte. *Hannes Tretter* vom Ludwig Boltzmann Institut für

93 Parlamentarische Anfragen, 30. August 2010 und Answer given by Mr Tajani on behalf of the Commission, 4 May 2010
94 Digital Civil Rights in Europe: INDECT - Privacy ethics in a secret project, 8. September 2010
95 Ein Ethogramm (auch: Verhaltensinventar, Aktionskatalog) ist ein schriftliches oder graphisches Verzeichnis aller beobachtbaren, diskreten Verhaltensweisen und der Verhaltensmuster einer Tierart oder des Menschen.
96 Siehe dazu: Deliverable 1.1 public version, p. 10-29
97 http://www.indect-project.eu/public-deliverables Deliverable 5.1, p. 45
98 http://www.alexander-alvaro.de/wp-content/uploads/2010/10/indect-written-declaration.pdf

Menschenrechte bezeichnet dieses wahllose Sammeln von personenbezogenen Daten als *»europäischen Bevölkerungsscanner«* mit dem nicht nur die Daten potenzieller Terroristen, sondern auch die von völlig harmlosen Personen erfasst würden. *»Damit werden wir alle verdächtig, was eine Abkehr von der Unschuldsvermutung bedeutet.«*[99]

Alexander Alvaro, innenpolitischer Sprecher der FDP im EU-Parlament, sagte dazu, dass die Kommission *"die totale Überwachung in europäischen Städten"* zu finanzieren scheine.[100] Der SPÖ-Abgeordnete *Johann Maier* richtete im März 2010 eine parlamentarische Anfrage an die Innenministerin. Die knappe Antwort: Gegenwärtig sei keine Kooperation geplant. Über eine künftige Beteiligung schwieg die Ressortchefin jedoch viel sagend.[101] *Roland Albert*, der eigens für INDECT abgestellte Sprecher der Piratenpartei meint: *"Wir halten das Projekt für sehr gefährlich und ethisch nicht vertretbar [...] Damit entsteht ein automatischer Bevölkerungsscanner."*[102] Auch die verschiedenen Anfragen an das EU-Parlament blieben meist unbeantwortet[103] und die deutsche Bundesregierung gibt sich in der Antwort auf eine Kleine Anfrage[104] des Bundestagsabgeordneten *Andrej Hunko*[105] ziemlich ahnungslos und uninteressiert. Bezüglich dieser Kleinen Anfrage berichtete *Telepolis*:[106]

„Die Kleine Anfrage [bringt jedoch] endlich Licht ins Dunkel über die Beteiligung des Bundeskriminalamtes an INDECT. Demnach hat das Amt die Ergebnisse von dessen Projekt Foto-Fahndung[107] *vorgestellt. 200 Pendler hatten hierfür von Oktober 2006 bis Ende Januar 2007 in einem "Feldtest" die biometrische Gesichtserkennung als neues "Fahndungshilfsmittel für die Polizei" getestet. Die Probanden hatten zuvor in ihre Teilnahme eingewilligt. Die deutsche Bundesregierung fördert im Programm "Forschung für die zivile Sicherheit" im Rahmen ihrer "High-Tech-Strategie" weitere Projekte zur Videoerkennung*[108]*, darunter "CaminSens", "APFEL", "ASEV", "MUVIT" und "SINOVE".“*

Laut EU-Kommission ist INDECT *"eher ein Prototyp/Prüfstand zur Technologiedemonstration als ein serienreifes Produkt"*.[109] Demgegenüber wird auf der INDECT-Webseite erklärt, dass 2013 "Industriepartner" eingeladen und "Marktstudien" zur Einführung der entwickelten Technik in den Polizeialltag eingeleitet werden. Ein ebenfalls angekündigter Workshop für die "*intelligence community*" kann so verstanden werden, dass auch europäische Nachrichtendienste als Endnutzer anvisiert werden. In einer Projekt-Verlautbarung heißt es, INDECT entwickle primär Anwendungen für „*Homeland Security Services*“, doch wird auch explizit erwähnt, dass als zweite Zielgruppe „Industriepartner“ und Forschungsinstitute in Frage komme würden.[110] Die konkreten Ziele von INDECT bleiben somit vorerst aufgrund der oft sehr konträren Aussagen von offiziellen Stellen und Mitarbeitern unklar.

Einige Europa-Parlamentarier haben sich nun allerdings mit einer fraktionsübergreifenden Initiative zu Wort gemeldet. *Alexander Alvaro, Carlos Coelho, Stavros Lambrinidis, Judith Sargentini* und *Rui Tavares* rufen zur Unterzeichnung einer Erklärung[111] auf, in der die Offenlegung aller Dokumente sowie ein endlich klar definiertes Forschungsziel gefordert werden. Wieviel Erfolg sie damit haben werden bleibt aber zweifelhaft.

INDECT betont indes weiterhin, dass es ein harmloses Forschungsprojekt wäre – was im Moment wohl auch noch zutreffend ist. Denn selbst wenn INDECT planmäßig bis 2013 einsatzbereit sein würde, wäre es noch ein weiter Weg, die übrige von INDECT benötigte Technologie „*up-to-date*“ zu bringen um INDECT wirklich effizient einsetzen zu können.

Ein Beispiel: In London gibt es derzeit ca. 4,5 Millionen Videokameras. Eine automatische Suche von Personen auf Kameraaufnahmen ist aber nur möglich, wenn die Kameras vernetzt sind und 15 bis 20 Bilder pro Sekunde liefern. Die meisten Kameras, die europaweit im Einsatz sind, schaffen jedoch gerade einmal

99 http://www.zeit.de/2010/31/A-Ueberwachung
100 http://www.alexander-alvaro.de/archives/1308/alvaro-menschensuchmaschine%20-indect
101 http://www.zeit.de/2010/31/A-Ueberwachung
102 ZEIT ONLINE, *Anna Sauerbrey*, 27.10.2010
103 European Parliament: Parliamentary questions
104 Kleine Anfrage vom 08. 11. 2010
105 http://www.andrej-hunko.de/start/downloads/doc_download/39-forschung-am-eu-projekt-indect
106 http://www.heise.de/tp/r4/artikel/33/33755/1.html
107 http://www.bka.de/kriminalwissenschaften/fotofahndung/
108 http://dipbt.bundestag.de/dip21/btd/17/027/1702750.pdf
109 http://www.heise.de/tp/r4/artikel/33/33755/1.html
110 http://www.heise.de/tp/r4/artikel/33/33282/1.html
111 http://www.euractiv.de/fileadmin/images/INDECT_Written_Declaration.pdf

zwei, drei Bilder pro Sekunde und vernetzt ist der Großteil davon ebenfalls (noch) nicht. Es gibt also nicht nur bei INDECT selbst, sondern auch bei den meisten anderen FP7 Projekten noch große technische Hürden zu bewältigen. Doch auch hier, im Bereich der Bild/Videoerkennung- und Verarbeitung ist man im Rahmen von FP7 mit Projekten wie 4DVIDEO („*4D spatio-temporal modelling of real-world events from video streams*“)[112], COPE („*Common Operation Picture Exploitation*“)[113] oder RTD („*Real-Time Delivery for Sensor Networks in Unpredictable Environments*“)[114] darum bemüht, möglichst bald verwendungsbereite Technologien zur Verfügung zu haben.

In Anbetracht des gesamten Ausmaßes des *7th Framework Programmes* (wie etwa den weiter oben beschriebenen Projekten), und angesichts der Vielzahl an beteiligten Organisationen, Unternehmen und Universitäten, ganz zu schweigen von den bereits investierten Kosten, ist es dennoch durchaus vorstellbar, dass die derzeit im Rahmen von FP7 erforschten Technologien in nicht allzu ferner Zukunft einsatzbereit sein und dann auch zum Einsatz kommen werden. Und nachdem wir uns nun einige der der FP7-ST Projekte etwas näher betrachtet haben, wird es auch etwas verständlicher, weshalb der *Telegraph* oder der Bericht des *OpenEurope* Think-Tanks[115] von „Orwell'schen Sicherheitstechnologien“ sprechen, welche durch die EU finanziert werden. Einzeln genommen zeugen die meisten dieser Projekte „nur“ von dem Versuch, alles was mit dem derzeitigen Stand der Technik möglich ist, dahingehend zu verwenden, um modernste Überwachungstechnologien zu entwickeln. *Die Zeit* schrieb dazu: „*Was auf den ersten Blick wie eine ambitionierte Bastelei von Hightech-Spezialisten aussieht, wollen die Brüsseler Überwachungsstrategen später einmal den Innenministerien der Mitgliedsstaaten zur Verfügung stellen.*“[116]

Sobald die Technologien und Werkzeuge aus Projekten wie ADABTS, ANASID, HIDE, LOTUS, PROMETHEUS, SAMURAI oder TALOS funktionsbereit sind, wird es nur noch eine Frage der Zeit sein, bis sie auch eingesetzt werden. Und werden sie erst einmal im kleinen Rahmen Verwendung finden, so ist es ebenfalls nur eine Frage der Zeit, bis sie auch im großen Rahmen Verwendung finden werden. Das die Resultate dieser Projekte schlussendlich kommerzialisiert werden, steht wohl außer Frage. Die andere Option wäre jene, dass Projekte wie INDECT einfach wieder eingestampft werden, weil sie sich nicht als funktionstüchtig erweisen. Diese Möglichkeit besteht natürlich durchaus auch. In Anbetracht der hohen Kosten dieser Projekte für die EU und die anderen involvierten Unternehmen und Organisationen scheint dies allerdings eher unwahrscheinlich zu sein. Und selbst wenn, müsste man sich dann doch fragen, wie die EU einfach so viele Steuergelder in nutzlose Projekte investieren kann.

Betrachtet man die FP7-ST Projekte in ihrer Gesamtheit, so kann man jedenfalls durchaus sehr deutliche Zeichen dafür erkennen, worauf die offensichtlich von unendlichem Kontrollwahn getriebenen Sicherheitsbestrebungen der EU in letzter Instanz abzielen: Permanente, flächendeckende Überwachung aller Bürger mit Technologien welche automatisch „abnormales“ Verhalten erkennen und bereits dann eingreifen können, wenn auch nur der bloße Verdacht besteht, dass jemand eine strafbare Handlung planen oder ausführen könnte. Alles in allem erinnert das Sicherheitsforschungsprogramm im Rahmen von FP7 stark an das *Information Awareness Office (IAO)* welches Anfang 2002 von Präsident Bush unter dem Namen *Total Information Awareness* ins Leben gerufen wurde und ebenfalls – wie auch INDECT – von Anfang an starker Kritik ausgesetzt war.[117]

Die europäischen Sicherheitsforschungsprojekte sind jedoch, im Vergleich zu US-Äquivalenten wie dem IAO, weitaus weniger geheim. FP7-ST ist – jedenfalls bis zu einem bestimmten Grad – sehr gut dokumentiert und eine Vielzahl von Daten und Dokumenten sind auch öffentlich zugänglich. Viele der einzelnen Projekte haben sogar eigene Webseiten. Die EU scheint hier einen entgegengesetzten Weg zu gehen. Sie veröffentlicht von verschiedenen offiziellen Stellen so viele Informationen, dass man schnell den Überblick verlieren kann. Vielleicht ist auch dies ein Grund dafür, weshalb man weder in den Mainstream-Medien noch in sogenannten alternativen Medien so wenig zu diesem Thema liest und hört. Wie schon in einem *Standard* Artikel zum Thema INDECT vom August 2010 geschrieben stand: *„Man muss es nur öffentlich machen, damit die Ungeheuerlichkeit eines Vorhabens nicht auffällt.“*[118]

112 http://www.hideproject.org/references/fp7_projects/4DVIDEO
113 http://cope.vtt.fi/
114 http://www.hideproject.org/references/fp7_projects/RTD
115 How the EU is watching you: the rise of Europe's surveillance state, 26 October 2009, p. 7
116 Die Zeit Online: Stunde der Späher, Marion Bacher, 29.7.2010
117 http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html
118 Helmut Spudich, DER STANDARD/Printausgabe, 25.8.2010

Angesichts der Tatsache, dass so viele dieser Forschungsarbeiten publik sind, könnte jedoch auch die Frage aufkommen, woran denn derzeit eigentlich im geheimen in der EU geforscht wird. Es gibt unzählige Theorien über Technologien zur Wettermanipulation, zur Erzeugung von Erdbeben, zur Manipulation und Kontrolle der menschlichen Psyche und viele mehr. Allerhand Theorien kursieren über Forschungseinrichtungen wie HAARP[119] oder *Pine Gap*[120], oder über den gegenwärtigen Entwicklungsstand von ECHELON und wofür es heutzutage Verwendung findet. Was und wie viel von all diesen Theorien der Wirklichkeit entspricht, ist nur schwer zu beantworten da es meist weitaus mehr Gerüchte als Indizien gibt, und noch weniger handfeste Belege.

Nach all den bekannten und belegten Technologien wie etwa jenen, an denen im Rahmen von FP7 geforscht wird, zu urteilen, kann man zumindest davon ausgehen, dass Filme wie beispielsweise „*Der Staatsfeind Nr. 1*“ gar nicht so weit her geholt sind, wie manch einer vielleicht denken mag und wie manche vielleicht versuchen, einem weiszumachen. In der Dokumentation „*The Spy Factory*“[121], erklärte *Eric Haseltine*[122]: „*Für uns, in der Intelligence Community, sind Filme wie Staatsfeind Nr.1 recht amüsant, denn sie vermitteln den Eindruck, wir wären allwissend ... Man sammelt vielleicht viel Zeug, doch weiß man nicht was man hat. Die größte technologische Herausforderung war, wie man mit Massen an Informationen umgehen soll, wie man die Puzzlestücke findet, sie verknüpft und versteht. Darin besteht das Problem.*“ Und er meint, dass der nächste Schritt der sei, dem Computer konkrete Fragen stellen zu können - ihn etwa in einem bestimmten Zusammenhang nach Bedrohungen fragen zu können oder sich zu erkundigen, ob man in einer bestimmten Angelegenheit vielleicht irgendwelche ungewöhnlichen Verbindungen übersehen hat. Wie jedoch ein Blick auf Programme wie FP7, und insbesondere Projekte wie INDECT zeigt, scheint dieser nächste Schritt schon in absehbarer Zeit machbar zu sein.

Cui bono ? - Wem zum Vorteil ?

Abschließend stellt sich die Frage, wer welchen Nutzen aus diesen Projekten hat. Einerseits geht es natürlich um Sicherheit. Die Frage stellt sich allerdings, um welche Art von Sicherheit es sich dabei handelt: „Bürgersicherheit“ oder „Staatssicherheit“, denn diese beiden müssen nicht zwangsläufig identisch miteinander sein. Wenn die Menschen in einem Staat von Geburt an als potenzielle Kriminelle angesehen werden, was nicht nur in der EU immer häufiger der Fall zu sein scheint, und wenn dann auch noch intensiv an Technologien zur Überwachung dieser Menschen geforscht wird, dann ist es äußerst fraglich, inwieweit all diese Maßnahmen schlussendlich wirklich der Sicherheit der Bürger dienen werden. Man könnte auch auf die Idee kommen, dass der Staat immer mehr Schutz vor seinen Staatsbürgern haben zu wollen scheint.

Ein weiterer wichtiger Aspekt an der Forschung an all diesen sicherheitsbezogenen Projekten ist natürlich aber auch Geld bzw. Wirtschaftlichkeit. Der Bundesverband Deutscher Wach- und Sicherheitsunternehmen geht etwa von einem Umsatzpotenzial für Sicherheitstechnologien und Sicherheitsdienstleistungen allein in Deutschland in Höhe von 31 Milliarden € bis 2015 aus. Der globale Markt für "*Homeland Defense*" wird sich nach Schätzungen des Hamburger Weltwirtschaftsinstituts von 2005 bis 2015 auf 178 Milliarden US-Dollar vervierfachen. Rund 20% davon würden vom Sektor "Geheimdienstliche Aufklärung" abgeschöpft:[123]

„Unter diesen Punkt fällt eine Vielzahl von Aktivitäten. Die Kerntätigkeiten dieser Dienste bestehen unter dem Aspekt der Inneren Sicherheit im Sammeln, in der Auswertung und der Überwachung sensibler Daten insbesondere aus der Nutzung moderner Kommunikationsmittel. Dazu bedarf es des Ausbaus einer bislang nur rudimentär bestehenden Koordination von Auslands- und Inlandsdiensten mit Polizei- und Regierungsstellen in den betreffenden Staaten. Zusätzlich müssen Verbindungen zu den Kontrollpunkten in Häfen, an Grenzen und kritischen Infrastrukturobjekten hergestellt werden. Über gemeinsame

119 „*High Frequency Active Auroral Research Program*“ US-amerikanisches ziviles und militärisches Forschungsprogramm in Alaska bei dem angeblich hochfrequente elektromagnetische Wellen zur Untersuchung der oberen Atmosphäre (insbesondere Ionosphäre) eingesetzt werden.

120 Pine Gap ist eine Militärbasis in Australien welche von der CIA während des Kalten Krieges gebaut wurde und es wird vermutet, dass es es sich dabei um eine der größten Bodenstationen von ECHELON handelt.

121 PBS Nova episode "Spy Factory" (February 3, 2009)

122 Dr. Eric Haseltine arbeitete 13 Jahre lang bei *Hughes Aircraft*, danach für *Walt Disney Imagineering* wo er in der Forschungs- und Entwicklungs-abteilung für "*large-scale virtual-reality*" Projekte tätig war und dort 2000 zum *Executive Vice President* ernannt wurde. 2002 wechselte er zur *National Security Agency* als Forschungsdirektor und zwischen 2005-2007 war er *Associate Director for Science and Technology* im *Office of the Director of National Intelligence* (ODNI), eine Position, die er 2006 in einem *US News and World Report* Interview wie folg bezeichnete: "*Sie können sich mich vorstellen als den CTO [chief technology officer] der "intelligence community".*

123 Strategie 2030 - Vermögen und Leben in der nächsten Generation, HWWI und Berenberg Bank

Beschaffungsstellen sollten einheitliche Hard- und Softwarelösungen angestrebt werden. Letztendlich wird ein starker Personalaufbau unabdingbar sein.“

Da Sicherheit und Katastrophenschutz nicht gerade zu den Themen gehören, die in den meisten europäischen Ländern auf ein wohlwollendes Interesse in der Öffentlichkeit und der Politik treffen, hat jede Warnung vor "erhöhter Terrorgefahr" den Beigeschmack einer kostenlosen Werbung für die Sicherheitsindustrie und die Förderung von Projekten der Industrie lassen sich ohne Frage als Subvention bezeichnen. Es geht also nicht allein um das Offensichtliche – Kontrolle und Überwachung der Menschen – sondern ebenso, vielleicht sogar noch mehr, um ökonomische Belange. Oder anders ausgedrückt: das ganze ist ein Milliardengeschäft das sich keiner entgehen lassen will.

Und es ist ja auch ein wahrhaft gutes Geschäft mit glänzenden Profitaussichten und geringem Risiko: Erst beteiligen sich die Steuerzahler in der EU großzügig an der Finanzierung von diesen neuen Überwachungstechnologien, und wenn diese dann erst ausgereift und einsatzbereit sind, werden sie an verschiedene Behörden und Sicherheitsagenturen innerhalb der EU-Staaten – wiederum durch Steuergelder finanziert – weiterverkauft, um dann anschließend zur Kontrolle und Überwachung jener eingesetzt zu werden, die diese Technologien von Anfang an mitfinanziert haben: eben wieder die Steuerzahler. Die Anschaffung dieser Technologien und Werkzeuge wird den EU-Bürgern von den Regierungen als unerlässlich zur Wahrung ihrer eigenen Sicherheit verkauf werden und so wird ihnen dann weisgemacht, sie würden durch Projekte wie INDECT in Form von mehr und höherer Sicherheit profitieren, während die Sicherheitsindustrie in Form von Milliardengewinnen daran profitieren wird.

> *„Mit der Zeit wirst du bemerken, dass viele Sicherheitssysteme nicht das tun, was sie behaupten, und dass ein Großteil unserer inneren Sicherheit Geldverschwendung ist. Du wirst Privatsphäre als Vorbedingung für Sicherheit, nicht als ihr Gegenteil begreifen. Du wirst dir keine Sorgen mehr über Dinge machen, um die sich andere sorgen, und anfangen, dich um Dinge zu sorgen, an die andere Menschen nicht einmal denken. Privatsphäre gegen Sicherheit einzutauschen ist dumm genug; dabei nicht einmal wirkliche Sicherheit zu erhalten, ist noch dümmer.“*
>
> – Bruce Schneier

> *„Wer die Freiheit aufgibt um Sicherheit zu gewinnen, der wird am Ende beides verlieren.“*
>
> – Benjamin Franklin

> *„Wer Sicherheit der Freiheit vorzieht, ist zu Recht ein Sklave.“*
>
> – Aristoteles zugeschrieben