# Siemens und Telekom im Sumpf der Sicherheitsindustrie

*von Christoph Marischka*

Eine vernichtende Bilanz legte die US-amerikanische Kanzlei Debevoise & Plimpton über die Geschäftspraktiken des Siemens-Konzerns zwischen 1999 und 2005 vor: „in fast allen untersuchten Geschäftsbereichen und zahlreichen Ländern" wurden Belege für Korruptionsverstöße gefunden. „Insgesamt sollen mindestens 1,3 Milliarden Euro an Schmiergeldern zur Erlangung von Aufträgen an diverse Behörden und Entscheidungsträger geflossen sein", berichtet die österreichische Zeitung Kurier.

Im untersuchten Zeitraum erhielt „Siemens Business Services", heute „Siemens IT Solutions und Services", mit einem gemeinsam mit IBM gebildeten Konsortium den Zuschlag für das laut Financial Times Deutschland größte Public-Private-Partnership-Projekt in ganz Europa. Im Rahmen des Herkules-Projekts soll die Bundeswehr bis 2015 flächendeckend mit neuen Computerarbeitsplätzen und Telefonanlagen ausgestattet werden. Hierzu gründete das Konsortium gemeinsam mit der Bundesrepublik Deutschland die Gesellschaft „BWI Informationstechnik", an der Siemens mit 50.5% beteiligt ist. „Diese strategische Partnerschaft ist ein wichtiger Baustein der Bundeswehrreform", schreibt die Gesellschaft in ihrer Selbstdarstellung. Die ursprünglichen Plankosten für das Herkules-Projekt beliefen sich auf 7.2 Mrd. Euro, verteilt auf die 10 Jahre, während derer das Projekt durchgeführt werden soll, bereits damals der nach eigenen Angaben größte Auftrag in der Firmengeschichte der Siemens AG. Die Gesellschaft hat sich hierfür ein eigenes Firmengebäude bauen lassen und ist längst an längerfristigen Projekten beteiligt. Das Fernmeldebataillon 384 in der General-Fahnert-Kaserne in Karlsruhe wurde bereits am 14.3.2008 von seinen Aufgaben entbunden, darunter der Betrieb des Automatische Führungsfernmeldenetz (AutoFüFmN) und des taktischen Richtfunknetzes der Flotte (TRF), die zukünftig die BWI Informationstechnik übernimmt. Auch am nach Bundesinnenminister Schäuble „größten technologischen Modernisierungsprogramm in Deutschland", das die so genannten „Behörden und Organisationen mit Sicherheitsaufgaben" (BOS) per einheitlichem Digitalfunk miteinander vernetzt, ist Siemens gemeinsam mit Nokia und dem Rüstungsunternehmen EADS beteiligt.

**Siemens: Top-Anbieter in Sachen Sicherheit**

42% seines Umsatzes erwirtschaftet Siemens IT Solutions and Services in Deutschland, weitere 42% im restlichen Europa. Unter den Auftraggebern befinden sich neben der Bundeswehr zahlreiche weitere öffentliche Stellen: Vom südafrikanischen und italienischen Innenministerium über die Finanzministerien in Frankreich und der Türkei, die Europäische Kommission bis hin zu den italienischen Carabinieri, dem schweizerischen Departement für Justiz und Polizei sowie zum Rüstungskonzern EADS und der internationalen EUROCONTROL-Behörde in Belgien, welche zukünftig die gemeinsame Flugsicherheit der zivilen und militärischen Luftfahrt in Europa regeln soll.

Einem Monitor-Bericht vom 16.3.2006 zu Folge lieferte Siemens auch an das usbekische Karimov-Regime „ein hochmodernes digitales Telekommunikationssystem, integraler Bestandteil laut Produktbeschreibung eine Technik, mit der Gespräche aller Art landesweit abgehört werden können." Zwar verpflichte der usbekische Gesetzgeber „… jeden Telekomanbieter, den Behörden Abhörtechnik zur Verfügung zu stellen", doch Siemens selbst warb in einem Prospekt von sich aus für entsprechende Standards: „Gesetzgebung und Standardisierung der Telekommunikation verlangen überall in der Welt von den Netzwerk-Betreibern die Mittel bereitzustellen, alle Formen der Telekommunikation zu überwachen und aufzuzeichnen".

Unter den privaten und halbstaatlichen Kunden allein des Zweiges IT Solutions and Services befinden sich v.a. internationale Flughäfen, Telekommunikations-Anbieter, Energieversorger, Banken, Versicherungen und Logistikunternehmen, also mehr oder weniger all das, was als „kritische Infrastruktur" betrachtet wird.

In Kroatien hat Siemens IT Solutions and Services wesentlich an der Gesamtkonzeption des Border-Managements mitgewirkt und liefert die entsprechende Technik. Innerhalb von 14 Monaten hat das Unternehmen im Auftrag der Europäischen Kommission gemeinsam mit dem kroatischen Innenministerium das so genannte „National Border Management Information System" (NBMIS) implementiert, eine „streng nach EU-Vorgaben konzipierte Lösung zur Personenidentifikation über Reisedokumente und Fingerprint...". Der Leiter Public Security bei Siemens IT Solutions and Services, Jörg Sauerbrey, schreibt dazu in der Zeitschrift „Homeland Security" (1/2008): „Bei der Identifikation per RFID liest ein mobiler Dokumentenscanner automatisch die Daten der biometrischen Ausweispapiere ein und vergleicht diese mit den zentral geführten Einträgen zu dieser Person ... An kroatischen Grenzübergängen werden zudem Fahrzeuge und deren Nummernschilder automatisch per Videokamera erfasst und in einer zentralen Datenbank, auf die auch das Innenministerium Zugriff hat, gespeichert. Durch die Schengen-kompatible Ausrichtung von NBMIS können die erfassten Kfz-Nummern und -Typen schon heute mit zahlreichen internationalen Datenbanken abgeglichen werden. Dies ermöglicht einerseits eine rasche Aufklärung bei Delikten bei Grenzübertritt. Andererseits sind die erfassten Fahrzeugbewegungen für nationale und internationale Verkehrsstatistiken nützlich."

Mittelfristig, so Sauerbrey, sollen die Systeme der Mitgliedsstaaten standardisiert werden, denn: „In den kommenden Jahren wird zudem das biometrische EU-Visum spruchreif, das den Grenz- und Zollbeamten auch die Kontrolle der Identität von Einreisenden aus Drittländern ermöglicht." Erst Mitte Februar hatte EU-Kommissar Frattini das so genannte Border Package der Öffentlichkeit vorgestellt, eine Sammlung von Evaluationen und Folgenabschätzungen, welche vorsehen, dass zukünftig alle, die in die EU ein- oder ausreisen, biometrisch erfasst werden sollten. Daneben sah das Papier eine Stärkung der EU-Grenzagentur Frontex sowie ein umfassendes System zur Überwachung der Außengrenze namens EUROSUR vor. Bei diesem sollen nicht nur Drohnen und Satelliten zum Einsatz kommen, sondern auch bestehende Techniken wie Wärmebildkameras und Radaranlagen aufgerüstet und vernetzt werden.

**Vernetzte Sicherheit**

Auch hierüber schien die Rüstungsindustrie bereits vorab informiert. Bereits im Juni hatten Finmeccanica und Thales ein Green Paper verfasst, in dem sie ihre Fähigkeiten

für die Umsetzung des EUROSUR-Projektes anpriesen und sich später mit einem entsprechenden Projekt um Fördermittel beim 7. Forschungsrahmenprogramm der EU bewarben. Im Border Package sprach sich wiederum die Kommission dafür aus, „[d]as 7. Rahmenprogramm für Forschung und Entwicklung (Themenbereiche Sicherheit und Weltraum) [heran zu ziehen], um die Leistungsfähigkeit und den Einsatz von Überwachungsinstrumenten zu verbessern, damit das erfasste Gebiet ausgeweitet werden kann, mehr verdächtige Aktivitäten aufgedeckt, potenziell verdächtige Zielobjekte leichter identifiziert werden können und der Zugriff auf Daten hochauflösender Beobachtungssatelliten erleichtert wird." Die ursprünglichen Vorschläge, die beiden Dokumenten, dem „Green Paper" und dem „Border Package" zu Grunde liegen, entstammen Studien der EU-Grenzbehörde Frontex.

Die Kommission, die ja normalerweise sehr viel Wert auf freien Wettbewerb legt, sollten solch enge Kooperationen zwischen öffentlichen Auftraggebern und privatwirtschaftlichen Anbietern bereits in der Konzeptionsphase eigentlich ein Dorn im Auge sein, schaffen sie doch letztlich wesentlich größere Wettbewerbsverzerrungen als einfache Schmiergeldzahlungen. Im Falle der Sicherheitsindustrie scheint jedoch eine andere Logik vorzuherrschen. So wurde im Herbst 2007 auf Initiative der Kommission das Europäische Forum für Sicherheitsforschung und Innovation (ESRIF) gegründet, nach Angaben der Kommission „eine informelle, beratende Plattform, an der die Interessengruppen aus dem öffentlichen und dem privaten Sektor auf freiwilliger Basis teilnehmen. Diese Interessengruppen sind die Industrie, Forschungseinrichtungen, öffentliche und private Endnutzer, Organisationen der Zivilgesellschaft, EU-Institutionen (insbesondere das Europäische Parlament) und europäische Organisationen... Ein öffentlich-privater Dialog im Bereich der Sicherheitsforschung ist von zentraler Bedeutung für eine höhere Sicherheit der Infrastrukturen, den Kampf gegen das organisierte Verbrechen und den Terrorismus, für die Wiederherstellung der Sicherheit in Krisenzeiten sowie für eine Verbesserung der Grenzüberwachung und -kontrolle. Bis Ende 2009 soll das ESRIF eine gemeinsame Agenda für Sicherheitsforschung aufstellen, die gegebenenfalls Empfehlungen an die Behörden enthalten wird."

Trotz seines informellen Charakters hat die Kommission Büros für das ESRIF eingerichtet, den Vorsitz führt der ehemalige EU-Koordinator für Terrorismusbekämpfung, Gijs de Vries. Stellvertretende Vorsitzende sind BKA-Vizepräsident Jürgen Stock und Giancarlo Grasso von der italienischen Rüstungsfirma Finmeccanica.

Ein ähnliches Konglomerat an „Sicherheitsexperten" ist überhaupt dafür verantwortlich, dass es ein Budget für Sicherheitsforschung auf Europäischer Ebene überhaupt gibt und wie es ausgestaltet wurde, wie Ben Hayes für das Transnational Institute und statewatch.org in seinem sehr lesenswerten Bericht „Arming Big Brother" beschrieb: Nach einem informellen Beschluss der Kommission im Jahr 2003 wurde eine „Group of Personalities" eingerichtet, die über Umfang und Ausgestaltung europäischer Sicherheitsforschung beraten sollte: Neben zwei Vertretern aus der Kommission und vier aus dem Parlament bestand dieses Gremium aus Vertretern der acht größten Rüstungs- und IT-Unternehmen: darunter EADS, BAE Systems, Thales, Finmeccanica, Ericcson, Diehl und: Siemens.

**In den besten Händen?**

In Deutschland war erst im April diesen Jahres öffentlich geworden, dass Siemens-Mitarbeiter dem Bundesnachrichtendienst (BND) Zugang zu von ihnen installierten Telefonanlagen im Ausland bereitgestellt hätten und bei der Entschlüsselung abgehörter Verbindungen behilflich gewesen seien. Eine Enthüllung, die Geheimdienstexperte Hans Leyendecker in der Süddeutschen Zeitung vom 14.4.2008 unter dem Titel: „Beste Verbindungen" als „banal" bezeichnete: „Im Bereich der elektronischen Funkaufklärung hat der Bundesnachrichtendienst immer mit deutschen Elektronikherstellern zusammengearbeitet - vor allem mit Siemens."

Andere große deutsche Unternehmen übernehmen geheimdienstliche Tätigkeiten gleich selber, wie es offensichtlich bei der Telekom der Fall war. Das Unternehmen hat Presseberichten zu Folge Mitarbeiter, Journalisten und Kritiker überwachen lassen, Verbindungsdaten an Dritte weitergegeben und Bewegungs- und Kontaktprofile erstellt, höchstwahrscheinlich auch Gespräche aufgezeichnet. Die Regierung samt Innenministerium gibt sich empört und fordert eine Selbstverpflichtung zum Datenschutz von den Unternehmen. Das ist freilich pure Heuchelei, hat doch die Bundesregierung selbst auf Europäischer Ebene Druck gemacht, die Vorratsdatenspeicherung für alle Telekommunikationsanbieter verbindlich zu machen und damit dafür gesorgt, dass diese eben solche Datensätze anlegen und Ermittlungsbehörden zugänglich machen sollen. Eine ähnliche Gesetzesinitiative auf nationaler Ebene war im Januar 2005 noch vom zuständigen Ausschuss im Bundestag abgelehnt worden. Einen Monate später nahm der damalige Innenminister Schily gemeinsam mit seiner Kollegin aus dem Justizministerium und Vertretern der Sicherheitsbehörden Gespräche mit der Telekom auf. Damals befand sich das Gesetz auf europäischer Ebene noch in der Planungsphase, die Speicherfrist der Telekom betrug nur 90 Tage. Heise-online berichtete seinerzeit: „Laut einem Ergebnispapier der Hinterzimmergespräche mit der Telekom, das heise-online vorliegt, drängen die Ermittler und Geheimdienste auf eine Speicherdauer von 180 Tagen für IP-Adressen und Login-Daten, die Verbindungsdaten bei einem Festnetzgespräch sowie im Mobilfunkbereich überdies die Standortkennung sowie ´gegebenenfalls Kartennummer (IMSI) oder Kennung der Endeinrichtung (IMEI)´. Die Telekom soll sich bereit erklärt haben, die entsprechenden persönlichen Daten für diese Zeitlänge zu archivieren." Im selben Zeitraum begann die Ausspähung von Mitarbeitern und Journalisten, mit der die Telekom den Recherchedienst Network Deutschland beauftragte und für die sie Verbindungsdaten, mutmaßlich auch anderer Telekommunikations-Anbieter, zur Verfügung stellte. Die Regierung zögert nun, strengere Gesetze gegen den Missbrauch der in staatlichem Auftrag erhobenen Daten durch private Anbieter zu erlassen und fordert zunächst eine „Selbstverpflichtung" und – in diesem Kontext vielleicht etwas zynisch - „mehr Transparenz".

Der Telekom drohen wegen Verstößen gegen den betrieblichen Datenschutz nun maximal 300.000 Euro Strafe. Unter anderem war 2005 der Betriebsratchef der Telekom überwacht worden und ihm wurden Kontakte mit einem Journalisten der Zeitschrift „Capital" nachgewiesen. Deshalb ermittelt nun die Staatsanwaltschaft gegen diesen wegen unlauteren Wettbewerbs.

Größter Anteilseigner an der Telekom ist übrigens mit rund einem Drittel der Aktien der Bund. Die Telekom ist wie die Daimler AG mit 45% am Joint Venture Toll Collect beteiligt, welches per Satellit die Bewegungen von LKWs auf deutschen Fernstraßen aufzeichnet und stichprobenartig die Kennzeichen von PKWs auf deutschen Autobahnen registriert. Dafür erhält Toll Collect etwa 650 Mio. Euro jährlich. Entgegen allen Beteuerungen vor der Einführung des Systems wird es in mehreren Bundesländern wie etwa im Umfeld des Weltwirtschaftsgipfels in Heiligendamm auch zur Verbrechensbekämpfung und –prävention eingesetzt.