„Lasciate ogni speranza
Voi, ch'entrate!" [1]
Dante Alighieri

Wer hört mit? (I)

Die organisierte Überwachung von Politik und Wirtschaft

Der folgende Beitrag liest sich wie ein Politthriller. Er handelt davon, wie in der "freien Welt" die informationstechnischen Waffen des kalten Krieges in die falschen Hände gerieten und zur Überwachung von Politik und Wirtschaft auch befreundeter Staaten genutzt wurden. Im Zentrum des Artikels stehen zwei Instrumente, ECHELON und PROMIS, die den Geheimdiensten und Regierungsstellen der Weltmacht USA erlaubten, ein engmaschiges Netz um die Erde zu spannen. Der zweite Teil des Artikels von Jean-Philippe Boever behandelt (ab Seite 43) die Gefahren, die sich für die Privatsphäre des einzelnen Bürgers in der vernetzten Welt ergeben könnten.

Die Szene: Ein Fernsehstudio irgendwo in Bertrange, Luxemburg. Die Life-Sendung heisst: "Chip, Chip hurra!" Der Publikumsapplaus ist, nicht wie bei heutigen „Unter der Gürtellinie-Talks", echt und wahrhaftig. Der Moderator: Nic Jakob, Nachrichten- und Fernseh-Mensch, intelligente Mischung aus dem Lächeln eines Mandarins und dem Schnauzbart eines Walrosses, das ganze ashkenasisch verpackt[2]. Das Programm: RTL Plus, Deutschlands Skandal-Erfolgs-Privat-Kommerzsender. Die Herausforderung, die wohl auch jeden "Wettendass" Redakteur gereizt hätte: da wettet Jakob, er habe einen jungen Informatiker im Studio, der sich innerhalb der Sendezeit unentdeckt Zugang zu einem der best gesichertsten Computer Amerikas verschaffen wird. Zu Anfang der Sendung noch zuversichtlich lächelnd, muss der Chef einer der weltweit größten Tageszeitungen zusehen, wie „seines Lebens schönster Traum", „sein" Computer nach und nach aufgibt, die „firewalls" [3] lautlos in sich zusammenstürzen, die Schlagzeilen der Frontpage der Ausgabe des folgenden Tages auf dem Computerschirm sichtbar werden und der Computer schließlich den "Eindringling" als "administrator"[4] anerkennt und ihm unbegrenzt Zugang zu sämtlichen Dateien ermöglicht. Der Zeitungschef tobt, die Einschaltquote jubelt.

Zugegeben, das war in der Steinzeit der Datensicherheit, vor fast 15 Jahren – im Computerzeitalter, welches nach Produktzyklen von Software und Megahertzschlägen von Prozessoren rechnet, sind das fast schon 5 Generationen, nach dem Moorschen Gesetz über die Beschleunigung der Computerhirne sogar 10.

„Wenn dieses System existiert, handelt es sich um einen nicht tolerierbaren Angriff auf die Grundfreiheiten, den Wettbewerb und die Sicherheit der Staaten."

Martin Bangemann, ehemaliger EU-Kommissar

Generationen später aber hat sich kaum etwas geändert. Ein Beispiel: In einem Land in Mitteleuropa verschickt ein Staatsbediensteter, vielleicht aus Rage über die rezente Reform seines Statuts, während der Arbeitszeit eine Datei mit frivolem Inhalt, nachdem er sie aus dem Internet heruntergeladen hat, aus Versehen an den falschen Adressaten. Das ganze über einen Computer des zentralen, staatlichen Rechenzentrums. In dem kleinen Land, dessen Namen wir aus Gründen der Dezenz verschweigen, findet dieser Vorfall kaum Beachtung – und dies, obwohl das betroffene Land sich selbst gern als „moralische Anstalt an sich" sieht. Nein, es ist nicht die Schweiz. In einem Fernsehbericht wird der Vorfall kurz danach aufgearbeitet: Auf Anfrage der Journalisten erklärt der Direktor des Rechenzentrums, er habe von dem Vorfall keine Kenntnis, bestätigt später aber, nach Rückfragen intern, dass der Vorfall wirklich stattgefunden hat. Man entrüstet sich noch etwas über den Straftatbestand der Verbreitung pornographischen Materials via Internet, dann hat die Presse ihre Schuldigkeit getan, und der Mohr kann gehen.

Die Frage aber, wie es möglich ist, dass etwas Derartiges passieren kann, und dann auch noch in einer Dienststelle, welche datentechnisches Hirn und Herz des Landes ist, wird nicht gestellt. Die Ratlosigkeit und das Unwissen um den Vorfall seitens der Direktion unterstreicht, dass die elementarsten Massnahmen zum Schutz der Systeme vor Zweckentfremdung sowohl von ausserhalb (z.B. durch Hacker), als auch von innerhalb der Dienststelle selbst entweder inexistent sind, oder doch ernsthaft versagt haben – was einen Zyniker zu dem Kommentar verleitete: „Ich weiß jetzt, warum es noch nie einen Hackerangriff auf diese Behörde gegeben hat: die Herausforderung ist einfach viel zu klein." Womöglich könnte man die Schlösser am Ein-

gang zu den „restricted areas" mit der EC-Karte überlisten… Dass man die datentechnische Integrität des Landes und jedes einzelnen seiner Bürger - um die es schließlich allein hier geht - in „Saubermann-City" mit einer Porno-Datei gefährden kann, ohne dass irgendein Kontrollmechanismus eingreift, ist schon fast karikatural. Kabarettreif ist die Geschichte allemal.

„Too many Secrets" - „Zu viele Gehemnisse" – wie ein roter Faden zieht sich dieser Satz durch die Literatur und die Filmkunst derer, die sich mit dem Thema Datensicherheit kritisch auseinandersetzen, zwischen Transparenz und Schutz. Und auf einmal scheint selbst die reale Welt, ausserhalb der Kinosäle, auf diese Parole eingeschworen zu sein – von staatlich betriebener Industriespionage nach dem Ende des Kalten Krieges zur schonungslosen Ausbeutung privater Daten, über jeden einzelnen von uns. Von alledem wird im Folgenden die Rede sein.

ECHELON – oder: Der erste Kreis der Datenhölle

1948 – Das Jahr wird, für die Zukunft Europas und der Welt zu einem Schlüsseljahr. Ein Jahr voller Extreme, Todesjahr von Gandhi und Karl Valentin, Jahr der Machtübernahme der Kommunisten in der Tschechoslowakei und in China, der Blockade von Berlin, der Geburtsstunde der Bundesrepublik Deutschland und des Staates Israel, des Bruches zwischen Tito und Moskau, des Bürgerkriegs in Griechenland und der Exekution von 213 Kommunisten. Jahr des Marshall-Planes und der Gründung der Westeuropäischen Union, Zeit der beginnenden Inquisition in den USA, die mit McCarthy einen neuen Heiligen hervorbringen wird, …

1948 – die Rote Gefahr ist überall. Aus den misstrauischen Zweckalliierten der Front gegen die Achsenmächte werden die Feinde des Kalten Krieges. Im März beauftragt der Nationale Sicherheitsrat der USA („National Security Council") durch eine Resolution (NSC 4) den amerikanischen Auslandsgeheimdienst, alles Erdenkliche zu unternehmen, um den Wahlsieg der Christdemokraten in Italien zu sichern. Italien, Brückenkopf im Mittelmehr, an der Schwelle der kommunistischen Bedrohung: die Tschechoslowakei ist verloren, Griechenland wankt, Tito, trotz kommunistischer Affinitäten, provoziert den sowjetischen Bären in Moskau. Blockfreiheit ist suspekt. Die Amerikaner erkennen die strategische Wichtigkeit Italiens und liefern finanzielle Unterstützung an antikommunistische Bewegungen. Man rekrutiert Agenten aus den Reihen der Kollaborateure von gestern, unterstützt die Mafiaclans, die die Landung in Sizilien vorbereitet hatten und schleust den Gotha der Endlösung über die „Rattenlinie" nach Südamerika…

… ein (ultra-)rechtes Netzwerk, entstanden aus einer Zweckallianz gegen den von Links kommenden politischen Fortschritt in Europa, gestützt durch technologische Mittel, die viele damals noch für surreal hielten.

Es ist die Saat, in der „Gladio" – „das Schwert" – aufgehen wird, jenes geheime „Stay-behind" Netzwerk überzeugter Antikommunisten, welche nur darauf warten, angesichts der sozialistisch-kommunistischen „Bedrohung" den Umsturz zu vollziehen. Gladio wird sich von Italien aus nach Frankreich, Belgien, den Niederlanden, Großbritannien, Deutschland, Norwegen, Portugal (wegen der Verbindungen zu Spanien) und der Türkei ausbreiten. In Griechenland heißt das Pendant zu Gladio „Rotes Vlies" und beteiligt sich aktiv am Militärputsch 1967. Die große Zeit Gladios erstreckt sich von 1969 bis 1980: man plant die antikommunistische Konterrevolution in Italien. Attentate auf Züge und öffentliche Gebäude (in Erinnerung bleibt unter anderem die Bombe im Bahnhof von Bologna und die 85 Toten 1980) versucht man den Linksextremen in die Schuhe zu schieben. Gladio wird gestützt von der rechten Loge P2 Licio Gellis – in der, neben Hunderten von Persönlichkeiten aus Staat, Justiz und Gesellschaft, auch Roberto Calvi, der unglückliche Chef der Banco Ambrosiano, Mitglied ist.

Der erste Kreis schließt sich. Die Spuren zu Gladio zeigt, Ironie der Geschichte, ein Toter auf: Aldo Moro, Chef der italienischen Christdemokraten, in seinen in der Entführung verfassten Briefen. Moro war 1978 angeblich von den Roten Brigaden entführt und hingerichtet worden. Mino Peccorelli, Journalist und Herausgeber des Blattes „OP",hatte die Entführung Moros angekündigt, sowie seinen Tod im Mai des selben Jahres vorhergesagt. Er selbst wird ermordet, nachdem er erklärt hatte, der Kopf der Entführerbande habe nichts mit den Roten Brigaden zu tun.

Heute weiß man, dass die Entführung Moros vom amerikanischen Geheimdienst und der Partei Moros selbst organisiert worden war. Der Grund: Moro wollte die italienischen Kommunisten im Rahmen des „historischen Kompromisses" zum ersten Mal nach dem Krieg in eine Regierung aufnehmen, als Koalitionspartner der Christdemokraten. Das posthume „Menetekel" Moros zeigt auf Giulio Andreotti…

1948 – parallel zu Gladio entstehen in Großbritannien, aufgrund des Geheimabkommens „UKUSA" [5] mit den USA Strukturen, welche ermöglichen sollen, weit ins europäische Festland zu horchen und Erhorchtes geheimdienstlich auszuwerten. Großbritannien als fünfte Kolonne der USA. Es ist die Geburtsstunde von Projekt 415, genannt „ECHELON", einem Abhörnetzwerk, dem später noch Kanada, Australien und Neuseeland beitreten werden. Die englische Basis von ECHELON, ein Ort, welcher auf keiner Karte vermerkt ist, liegt etwa 280 Kilometer westlich von London. 2000 zumeist amerikanische Angestellte arbeiten dort, Militärs und Zivilisten.

Aus den wenigen, von den USA freigegebenen Dokumenten kann man herauslesen, dass ECHELON Ende der 60er Jahre richtig aktiviert wurde; ein ECHELON 2 gibt es seit 1979. Die Überschneidung der Daten mit den Schlüsseldaten von Gladio ist frappierend… ECHELON als technologisches Rückgrat der „Steh-auf-Männchen" von Gladio? Der Schluss ist, angesichts der Parallelen in den Daten und der logischen Synergien in der Praxis, verlockend, die Perspektiven, die er eröffnet, erschreckend: ein (ultra-)rechtes Netzwerk, entstanden aus einer Zweckallianz gegen den von Links kommen-

den politischen Fortschritt in Europa, gestützt durch technologische Mittel, die viele damals noch für surreal hielten.

An den Schalthebeln ECHELONs sitzt die NSA, die „National Security Agency", Amerikas geheimster Geheimdienst[6], mit 38000 Angestellten und einem Jahresetat von 3,6 Milliarden USD. Die NSA hat allein zum Zweck, die internationalen Telekommunikationsverbindungen in welcher Form auch immer, zwischen wem auch immer, abzuhören und gegebenenfalls auszuwerten. Zum Nutzen der freien Welt, versteht sich – oder doch nur für die Mitglieder von ECHELON…. Oder vielleicht nicht einmal für sie?

ECHELON arbeitet mit sämtlichen Mitteln modernster Technik: Vom Satelliten über die Hochfrequenzantenne bis zum Unterseeboot zum „Abhören" von transatlantischen Kabeln: weder Telefon, noch Fax, noch Telex sind vor ECHELON und der NSA sicher, von Computern, denen man beibringen kann „geschwätzig" zu sein[7] einmal ganz abgesehen. Auch das neue Medium Internet bleibt nicht ausgespart: „Schnüffelsoftware", an Internet-Knotenpunkten („Internet Exchange Points" IXPs) zum Beispiel, filtert e-mails, Dateien, etc. nach interessanten Inhalten.

Sämtliche abgehörten Mitteilungen werden gescannt und wenn nötig ins Englische übersetzt. Dann filtert ein Schlüsselwort- oder Gesprächsanalyseprogramm bestimmte Inhalte heraus (je nachdem, ob der Inhalt eines von mehreren hundert Schlüsselwörtern, wie „Präsident", „Bombe", „Terrorismus", „Freiheit", u.ä. enthält), die, nach Analyse durch Nachrichtendienstexperten, an amerikanische Behörden und Unternehmen weitergeleitet werden. „An Unternehmen"? – die britische und die US-Regierung bestreiten dies vehement. ECHELON, ein Kind des Kalten Krieges, wurde nach dem Fall der Mauer und dem Verschwinden des sich dahinter versteckenden Feindbildes "Kommunismus" umgeschult. Offiziell zur Bekämpfung von Terrorismus und organisierter Kriminalität. In Wirklichkeit aber auf Wirtschaftsspionage: 1993 überwachte die NSA z.B. die Gespräche des französischen Premierministers Alain Juppé mit Paris während der GATT-Verhandlungen: Vertrauen ist gut, Kontrolle ist besser.

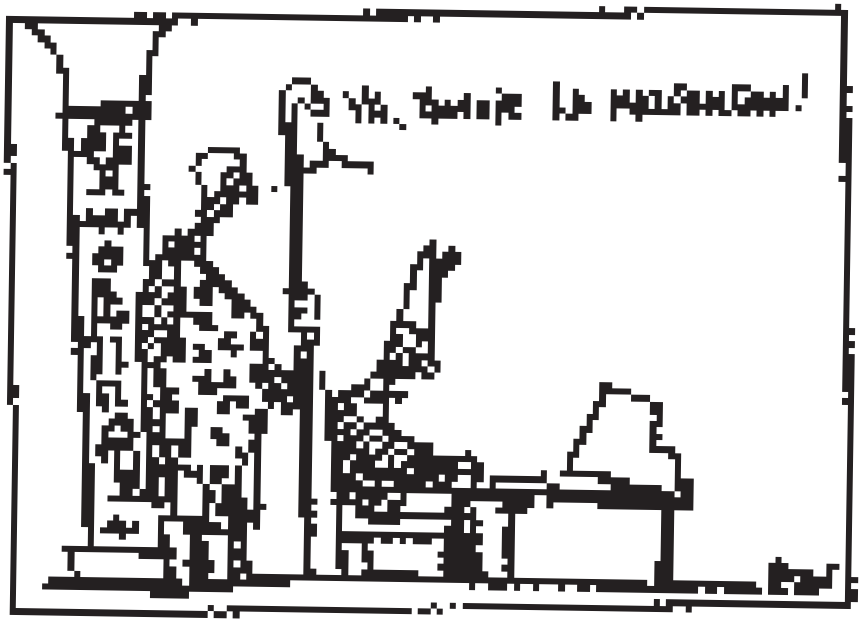
In dem 1999 veröffentlichten Bericht des Fachjournalisten Duncan Campbell, welcher vom Ausschuss für Menschenrechte des Europaparlamentes in Auftrag gegeben und Ende Februar 2000 dem Parlament in Strassburg vorgestellt wurde[8], werden weitere Verstrickungen zwischen Wirtschaft, NSA und ECHELON deutlich: von den 140 ECHELON-Überwachungssystemen weltweit dienen 9 der Überwachung des Internetverkehrs – deren Ziel auch wirtschaftlicher Natur ist. Des weiteren behauptet Campbell, würden US-amerikanische Firmen wie Microsoft und IBM, sowie große Chiphersteller, bereits heute Hintertüren (sogenannte „backdoors") für die spätere Überwachung in ihre Produkte für den Weltmarkt einbauen. Dabei haben die europäischen Unternehmen das Nachsehen: 1994 verlor Airbus ein Millionengeschäft mit Saudi-Arabien an den amerikanischen Konkurrenten McDonnell-Douglas, da dieser Zugriff zu Geheiminformationen von Airbus hatte. Geschätzte Verluste für die europäische Wirtschaft durch den Einsatz von ECHELON: 80 Milliarden EURO.

Das Europaparlament hat, 4 Monate nach der Anhörung Campbells, am 5. Juli 2000 in einer Abstimmung mit 340 gegen 210 Stimmen entschieden, trotz der allgemeinen Entrüstung keinen Untersuchungsausschuss einzusetzen, sondern nur eine provisorische Kommission ohne reale Kompetenzen. Thierry Jean-Pierre, designiertes Mitglied dieser Kommission, ehemaliger französischer Untersuchungsrichter und derzeitiger PPE-Abgeordneter (Europäische Christdemokraten und Konservative) im Europaparlament, kritisiert diese Vorgehensweise offen: es habe keine öffentliche Debatte zu ECHELON stattgefunden, Abgeordnete, die am Rednerpult dem Problem auf den Grund gehen wollten, seien sehr unwirsch von der Parlamentspräsidentin unterbrochen worden. Der Grund für die Vorgehensweise des Parlamentes liegt wahrscheinlich in der „Political correctness" Großbritannien gegenüber, das man nicht als unsolidarisches Mitglied und fünfte Kolonne der USA hinstellen will.

Bei seinem Amtsantritt hatte Clinton den Geheimdiensten eine Reorientierung verschrieben: an der nationalen Verteidigungsakademie wird jetzt das Fach „Datenkrieg" gelehrt. Die Wirtschaft und die in ihr tätigen Unternehmen werden als Schlüsselsteine der nationalen Sicherheit betrachtet; Internet als Waffe.

Aber nicht nur die USA greifen zu solchen Methoden, denn auch in Frankreich gibt es eine „Ecole de Guerre économique", welche von Christian Harbulot geleitet wird. Dort lernt man das Anlegen von „backdoors" und den

Pessin, in: Le Monde



Umgang mit Trojanischen Pferden, Virussoftware und "Agents".[9] Man lernt, wie man einen Konkurrenten oder einen unliebsam gewordenen Partner via Internet fertig macht, seinen Aktienkurs beeinflusst und seine Verkaufsziffern manipuliert.

Martin Bangemann, damals EU-Kommissar, meinte zu den ersten Berichten über die Existenz von ECHELON 1998: „Wenn dieses System existiert, handelt es sich um einen nicht tolerierbaren Angriff auf die Grundfreiheiten, den Wettbewerb und die Sicherheit der Staaten." Tatsächlich stellt der Betrieb von Systemen wie ECHELON die Fundamente und Wertstrukturen in Frage, auf die sich das gesellschaftliche und politische System sowohl Europas, als auch der Einzelstaaten gründet. Verknüpft man das von den USA gesteuerte ECHELON mit den rezenten, von den USA vorangetriebenen Geheim-Verhandlungen im Rahmen der Welt-Handelsorganisation über das AMI, das multilaterale Abkommen über die Investitionen, dann wird das Trauma der „gläsernen Wirtschaft" greifbar.

PROMIS – oder das nicht gehaltene Versprechen

1978 – während Italien sich auf eine kommunistisch-christdemokratische Regierung unter Aldo Moro vorbereitet, ist in den USA, wo diese Entwicklungen mit höchster Sorge aufgenommen werden, das von dem Vietnamveteran und NSA Mitarbeiter William Hamilton entworfene Computerprogramm PROMIS anwendungsreif. Hinter der Abkürzung "PROMIS" verbirgt sich das "Prosecutors' Management Information System", eine Software, ursprünglich gedacht für die Terminals der Staatsanwälte, um Raster- und Ringfahndungen, Informationsauswertung und -austausch zu vereinfachen. PROMIS funktioniert dabei wie ein Schleppnetz, das seinem Anwender erlaubt, Datenbestände aus ganz verschiedenen Datenbanken zusammenzuziehen und auszuwerten. Als dem Kommmunikationsexperten und genialen Tüftler Hamilton aufgeht, dass er mit PROMIS ein „zweischneidiges Schwert" entwickelt, verlässt er die NSA und übernimmt die Leitung eines gemeinnützigen Institutes, des „Institute for Law and Social Research", kurz INSLAW. Da INSLAW hauptsächlich von öffentlichen Zuwendungen und Aufträgen der öffentlichen Hand lebt, ist PROMIS zu der Zeit Public-Domain-Software, also öffentlich zugänglich und kostenfrei.

Nachdem INSLAW am Ende der Ära Carter aus Mangel an Geldmitteln in ein privates Unternehmen umgewandelt worden war, kommt der große Aufstieg 1982 in Form eines Regierungsauftrages des US-Justizministeriums: INSLAW soll 94 US-Staatsanwaltschaften mit PROMIS ausrüsten, um die Vernetzung von Datenbeständen, die in ganz verschiedenen Computersystemen abgelegt wurden, zu ermöglichen. Geschätzter Umfang des Deals: 3 Milliarden US-Dollar.

Pessin, in: Le Monde

Hamilton hatte inzwischen PROMIS weiterentwickelt und besaß das Copyright an der weiterentwickelten Version, die er nun dem US-Justizministerium in Form eines Leasings anbot. Das Ministerium reichte die Testversion von PROMIS an die „Central Intelligence Agency" (CIA) und die NSA weiter, zu Bewertungszwecken und zur Prüfung. Die Reaktion der Dienste folgte umgehend: Das Justizministerium forderte Hamilton auf, den lückenlosen Beweis vorzulegen dass die „neue" PROMIS-Version nicht ausschließlich mit Geldern aus öffentlicher Hand finanziert worden war. Das Ministerium bestritt den Copyrightvermerk von ISLAW. Es stellte jegliche Zahlungen an INSLAW mit der Begründung ein, dass es unbegrenzte Rechte an PROMIS hielt und demnach nicht zu zahlen brauchte und kündigte im folgenden den Restauftrag über die Ausrüstung der verbleibenden 74 Staatsanwaltschaften.

Zweck des ganzen Manövers: INSLAW aus dem Geschäft in den Bankrott zu führen, zum Vorteil eines Unternehmens, welches hohen Regierungsbeamten und Beratern um Präsident Reagan, darunter Edwin Meese, dem späteren Justizminister und Earl Brian nahe stand: Hadron Inc. Während INSLAW trotz wachsender Finanzprobleme an der Ausführung des Regierungsauftrages festhält, beginnt eine Parallelvermarktung von PROMIS unter den unterschiedlichsten Namen über Hadron und andere Scheinfirmen der Amerikaner und der Israelis. Auch wenn das quiproquo um INSLAW, Hadron und PROMIS bis heute nicht lückenlos geklärt ist, so werden doch die ersten Tentakel der Krake sichtbar, die die Reagan-Boys um Hadron in Kalifornien gebildet hatten.

1985 musste INSLAW schließlich Konkurs anmelden. Das Justizministerium sorgte dafür, dass das Konkursgericht gleich ein Liquidationsverfahren eröffnete. Jedoch gewann INSLAW in diesem Verfahren und auch in der darauffolgenden Berufungsinstanz: Das Justizministerium wurde zur Zahlung von Lizenzgebühren verurteilt und des Softwarediebstahls überführt. Ein Pyrrhussieg: die von dem Gericht INSLAW zugestandenen Summen wurden nie bezahlt, der erstinstanzliche Richter

wurde 3 Jahre später abberufen und in die Arbeitslosigkeit entlassen und INSLAW's Anwalt aus einer der größten Kanzleien in Washington erhielt eine großzügige Abfindung dafür, dass er den Fall gezwungenermaßen niederlegte und die Kanzlei verließ. Die 600.000 US-Dollar für den Anwalt wurden aus einem Fonds des Mossad an Hadron mit der Massgabe, damit den Anwalt herauszukaufen überwiesen.

Hamilton gelang es, Elliot Richardson, den ehemaligen Jusitzminister Nixons, als Anwalt für INSLAW gewinnen. Dank der Intervention Richardsons an höchster Stelle, befasste sich der Rechtsausschuss des US-Repräsentantenhauses unter dem Vorsitz des Texaners Jack Brooks 1989 mit der INSLAW-Affäre. Die Untersuchung wurde zu einem Machtkampf zwischen dem Parlament und dem Nachfolger Meeses im Amt des Justizministers Richard Thornburgh. Obwohl das hohe Haus in seinem Abschlussbericht zu keinen eindeutigen Schlüssen kam, wurde die Tatsache offensichtlich, dass das Justizministerium alles versucht hatte, um die Aufklärung auf allen Ebenen zu verschleppen: Von institutionalisierter Amnesie bis zum Verlust ganzer Akten reichte die Phantasie des Justizministeriums.

Hamilton hegte indes weiter die Hoffnung, dass es bei einem Regierungswechsel zur lückenlosen Aufklärung des Falles INSLAW kommen würde. Er wurde enttäuscht: weder Clinton, noch seine Justizministerin Janet Reno zeigten das geringste Interesse mit der republikanischen Vergangenheit um INSLAW abzurechnen. Hatte auch die Clinton-Regierung etwas zu vertuschen?

Fast zufällig erfährt Hamilton 1990, dass 900 Kopien einer dieser gestohlenen Versionen von PROMIS von der Royal Canadian Mounted Police benützt werden. Andere prominente Anwender sind die amerikanischen Geheimdienste CIA, NSA, DIA (Defence Intelligence Agency), sowie die Drogenpolizei DEA (Drug Enforcement Agency), der israelische Geheimdienst Mossad, Interpol, sowie Länder wie die Türkei, Zypern, Pakistan, Syrien, Südafrika, Südkorea, Saudi-Arabien, Kuwait, Japan, der Irak, Iran, Guatemala, Singapur, Libyen und, nicht zuletzt, Deutschland – insgesamt 88 Länder.

Was bei dieser Länderliste auffällt, ist, dass sie wahllos Alliierte der USA und sogenannte Feinde enthält. Die Logik, die dahinter steht, ist mehrschichtig: durch Verkäufe an die Türkei, Pakistan, Zypern, und Syrien zum Beispiel versucht die DEA, den Drogenhandel aus dem Vorderen Orient in den Griff zu bekommen – ein an sich sehr lobenswertes Ziel - ohne dabei das Interesse an zivilen und militärischen Daten der Freunde und Feinde außer Acht zu lassen. Es ist offensichtlich, dass es bei allen Ländern um bedeutend mehr geht als um Geld.

In der Logik des Schattenkabinetts aus amerikanischen Politikern und ehemaligen Geheimdienstlern läge eine Infiltrierung von Großbanken, von weltweit tätigen Clearing-Unternehmen usw.

Doch was, wenn PROMIS nicht nur an andere Geheimdienste und Behörden, sondern auch an Privatunternehmen verkauft wurde?

Auf der Kundenliste der Raubkopien von PROMIS Software standen z.B. auch Crédit Suisse (nach Aussage des israelischen Geheimdienstlers Ari Ben-Menashe), die Weltbank und der Internationale Währungsfonds. Wohin ist PROMIS noch verkauft worden, welche Systeme wurden noch mit der modifizierten Software infiziert? In der Logik des Schattenkabinetts aus Politikern und ehemaligen Geheimdienstlern läge eine Infiltrierung von Großbanken, von weltweit tätigen Clearing-Unternehmen, von einzelnen Sparten der Industrie und des ganzen Bereichs der neuen Technologien.

Mit einiger Sicherheit darf man davon ausgehen, dass auf der PROMIS-Kundenliste auch die BCCI stand. Die "Bank of Credit and Commerce International", deren Dachholding in Luxemburg ansässig war, gehörte noch Anfang der 90er Jahre zu den weltweit gößten Bankenimperien. Die BCCI, von ihrem charismatischen "Erfinder" Agha Hassan Abedi als erste wirklich weltweit tätige Bank der Dritten Welt für die Dritte Welt mit einer "moralischen Mission" vermarktet, wurde schnell zur Hausbank so manch eines Diktators und manch einer mafiösen Eminenz, die Bank des Hungers in den geplünderten Drittweltstaaten und der "Crooks and Criminals International", wie einer ihrer Zunamen lautete.

Für die amerikanischen Geheimdienste, die selbst bei der BCCI Konten unterhielten, mußte es ein Leichtes gewesen sein, aus der Bank dank einer Software wie PROMIS eine Art Trojanisches Pferd in der Weltfinanz zu machen. In einem von einem republikanischen Präsidenten und ex-CIA Direktor geführten Amerika, in den Nachwehen der "October Surprise" und der Iran-Contra Affaire wird der Anreiz für dieses Schattenkabinett aus Politikern und Geheimdienstlern groß gewesen sein, aus einer Bank, die ausnahmslos überall auf der Welt auftrat (sogar in Ländern, die andere Finanzinstitute sonst meiden würden) ein Element der Untergrundpolitik zu machen.

Genährt wird dieser Verdacht auch durch die Verbindungen dieses Schattenkabinetts über die BCCI hinaus zu den honorigen Kreisen der internationalen Gesellschaft. So konnten kurz vor dem unrühmlichen Ende der Bank einige "priviligierte" Kunden noch rechtzeitig ihr mühsam Erspartes von den Konten abziehen. Zum Schaden der Kleinanleger und Aktionäre, die nach Schließung der Bank am 5. Juli 1991 nur Schall und Rauch aber kein Geld mehr sahen, wurde dieser Personenkreis offenbar rechtzeitig gewarnt. In Monaco und anderen Ländern geht die Rede von mehreren Millionen Dollar, die auf diese Weise "gerettet" wurden. [10] Die Zweckallianz war in Gefahr und mußte geschützt werden.

Dabei muss nicht PROMIS selber benutzt worden sein – denn in jedes Programm lässt sich eine Hintertür einbauen, die dem Eingeweihten interessante Wanderungen durch den fremden Datendschungel ermöglicht.

PROMIS, die Schleppnetzsoftware, die fleißig wie eine Ameise aus heterogenen Systemen Daten sammelt, nach einer mehr oder weniger großen Anzahl von Kriterien ordnet (Raster-

fahndung), sie aufbereitet und auswertet, war manipuliert worden. Von einem Mann, der aussieht wie der Pizzabäcker von nebenan und fast auch so heißt: Michael Riconosciuto. Riconosciuto, der heute für dreissig Jahre wegen eines – laut seiner Aussage fingierten – Drogendeals in den USA einsitzt, behauptet, PROMIS im Auftrag der amerikanischen Geheimdienste mit einer Hintertür, einer sogenannten „backdoor" versehen zu haben, die es einem Außenstehenden, der den Zugangscode zur „backdoor" kennt, ermöglicht, ungesehen in den betreffenden Computer einzudringen. Dabei wird das Betriebssystem des Computers derart verändert, dass die „backdoor" direkten Einfluss auf die Zugangskontrolle zum Computer hat. Man braucht also nicht erst den Computer zu knacken, bevor man die „backdoor" in dem betreffenden Programm aktivieren kann. Eine derartige Manipulation bleibt für den normalen Computeranwender unsichtbar.

Die manipulierte Version von PROMIS wurde von den US-amerikanischen Diensten und dem Mossad als Trojanisches Pferd an Freund und Feind über Scheinfirmen und unter einer Vielfalt von Namen gleichermaßen verkauft. Durch die „backdoor" konnte man zu jeder Zeit die Daten aus dem Computer herauslesen. Spionage wie mit einer PlayStation: auf Knopfdruck erscheinen die „special effects" aus dem fremden Computer und man kann sich ungestört mit ihnen amüsieren. Für manch einen dieser Horcher ähnlich dem Cybersex. Kräftig die Werbetrommel für PROMIS soll auch der große Robert Maxwell gerührt haben, dank seiner Unternehmen in Israel und seiner guten Kontakte in Ost und West.

Anfang der 80er Jahre beginnen die „field studies" mit PROMIS. Da das Programm erlaubt, Datenbanken, zum Beispiel von Banken, Versicherungen, Wasserwerken, Elektrizitäts- und Telefongesellschaften, anzuzapfen und miteinander zu verbinden, ermöglicht es das Erstellen genauer Datenprofile über Einzelpersonen, Unternehmen und sogar Staaten – der gläserne Mensch auf Abruf. PROMIS landete über US-Tarnfirmen beim Jordanischen Militär und ermöglichte das Abzapfen von Millionen von Datensätzen über Palästinenser und ihre Organisationen. Sein Einsatz in Guatemala unter dem Staatschef General Oskar Mejia Victores führte dazu, dass Tausende von Intellektuellen, Oppositionellen, Priestern, Gewerkschaftlern und einfachen Indios verschleppt, gefoltert und ermordet wurden. Die „Erfolgsbilanzen" des Einsatzes von PROMIS in Südafrika, speziell in der Transkei zur Zeit der Apartheid, in Chile unter General Pinochet und in anderen geopolitischen Problemzonen sind, aus Sicht der Verfechter elementarster Menschenrechte, ähnlich verheerend. Sämtlichen Opfern war das Unglück geschehen, sich in dem von PROMIS ausgeworfenen Schleppnetz zu verfangen.

Ari Ben-Menashe, ehemaliger Mossad-Agent, bekennt, dass PROMIS zu einer datentechnischen Revolution führte und das Big Brother Zeitalter einläutete. Allerdings lösten die „backdoors" in PROMIS nicht das Problem der sogenannten „stand-alone" Computer, Rechner also, die an kein Netz angeschlossen sind und nicht mit der Außenwelt kommunizieren. Doch auch hierfür hatten die NSA und ihr „Pizzabäcker" Riconosciuto eine Lösung: durch die Manipulation einer Software wie PROMIS und die dadurch erreichte Modifizierung von Teilen der Betriebssoftware eines derartigen Rechners, kann ein „stand-alone" Computer dazu gebracht werden, geschwätzig zu werden, d.h. in zyklischen Abständen Daten abzustrahlen, welche dann einiger Entfernung empfangen werden können. Dieses, von der NSA entwickelte Verfahren, könnte in der zivilen Anwendung eine drahtlose Vernetzung von Computern bei relativ niedrigem Energieverbrauch ermöglichen. Bis Riconosciuto zu diesem Thema auspackte, schwiegen diejenigen sich darüber aus, die um das Potential dieser neuen Spionagemethode wußten.

Man stelle sich das vor: über manipulierte Software steigt man entweder durch eine „backdoor" in einen Computer ein, oder bringt ihn dazu, in regelmäßigen Abständen alle in ihm enthaltenen Daten abzustrahlen. Keine Datei ist mehr vor Zugriffen von außen sicher. Das Ende des Privaten: „Big Brother is watching you!"

Was wäre, wenn außer hochspezialisierter Software wie PROMIS auch andere (US-amerikanische) Software derart manipuliert worden wäre? Eines ist sicher: an der Beantwortung der Frage, wie nackt der Kaiser wirklich ist, hat niemand ein Interesse. Die Geheimdienste wollen keine billige Informationsquelle verlieren, Banken und andere Anwender keine Kunden und die Softwarefirmen möchten sich die Kosten für erhöhte Sicherungsmaßnahmen ersparen – eine Konspiration des Schweigens. Es ist allerdings schwer vorstellbar, dass Großkonzerne aus der Softwarebranche sich wirklich auf derartige „War Games" einlassen würden. Würden „backdoors", Trojanische Pferde oder andere Formen der Manipulation der Produkte bekannt, hätte das unweigerlich verheerende wirtschaftlich Folgen; es wäre das sichere Aus für den Hersteller, sowohl kommerziell wie rechtlich, im Rahmen etwa von Schadensersatzklagen. Und dennoch, das Risiko ist nicht ganz auszuschließen.

"Rechner besitzen keine Moral", sagt Nicolas Negroponte, "sie können für komplexe Themenbereiche, wie das Recht auf Leben und Sterben keine Lösungen anbieten." Darum töten sie ohne Schuld und Sühne. Das mußte unter anderen Danny Casolaro erfahren, der in dem Kreis um das Schattenkabinett und seine Tagesgeschäfte recherchierte.

Jean-Philippe Boever

[1] „Lasst alle Hoffnung fahren, Ihr, die Ihre hier eintretet". Inschrift über dem Eingang zur Hölle in Dante Alighieris „Göttlicher Komödie" .

[2] Ich kenne ihn gut – er wird die Beschreibung mögen.

[3] „Firewall": übers.: „Feuerwand" – ein Sicherungssystem, welches verhindern soll, dass ein Aussenstehender in einen Computer „einbrechen" kann.

[4] „administrator" - Bezeichnung für eine Person, die zu einem Computer, einem Netzwerk oder einem Datensystem unbegrenzt Zugang hat und nicht nur Daten aufrufen, sondern auch verändern oder ganz löschen kann.

[5] "United Kingdom-United States Agreement on Signals Intelligence".

[6] Darum trägt sie auch den Spitznamen "No Such Agency" – NSA.

[7] Siehe unten zu PROMIS.

[8] "Development of Surveillance Technology and Risk of Abuse of Economic Information"; Luxembourg, December 1999, PE 168.184/Vol 1/5/EN.

[9] Die Bank trat in Luxemburg mit dem Slogan auf, des Landes größter Steuerzahler zu sein. Kürzlich eiferte ihr ein Großunternehmen zumindest in bezug auf den Slogan nach.

[10] Vgl. den Artikel "Monaco: La vraie fortune des Grimaldi", in Le Vif/L'Express due 30.6.2000.