

## Information Warfare

die unbekannte Bedrohung aus dem Schattenreich

Es hat wohl kaum eine Zeit gegeben, in der Technologiesprünge so schnell aufeinander folgten wie in den letzten 25 Jahren. Angefangen mit dem Siegeszug des PCs in den 80iger Jahren, über die rasante Ausbreitung des Internets, die Mobiltelefone, die Einführung von WLAN-Netzen bis zu VoIP hat sich die Welt grundlegend verändert. Der technologische Fortschritt bei den IT- und Kommunikationssystemen stellte die Grundlage für industrielle Globalisierung dar. Raum- und Zeitgrenzen lösen sich auf. Was auf der einen Seite wie ein Motor der Wirtschaft aussieht, bringt auf der anderen Seite auch enorme Sicherheitsrisiken. Die Prozesse und Systeme in den Unternehmen werden immer komplexer, unkontrollierbarer und damit angreifbarer.

Nun gab es schon immer Risiken, gegen die sich Unternehmen schützen mussten, aber die umfassende Vernetzung der Informationssysteme und die enorme Abhängigkeit der Kernprozesse von der IT-Unterstützung führt zu einer ganz neuen Dimension der Bedrohung. Wir leben im Informationszeitalter. Die Information stellt heute das höchste Gut dar. Informationsvorsprung bedeutet Wettbewerbsvorteil, bedeutet Profit und letztlich Überleben des Unternehmens. Die Information gilt es einerseits zu schützen und andererseits zu gewinnen. Was so selbstverständlich und harmlos klingt, ist nichts anderes als ein rücksichtsloser, verdeckt ablaufender Krieg um Informationen – der Information Warfare. Dieser Krieg, und ich verwende den Namen dabei ganz bewusst, findet unterschwellig und lautlos im Geheimen statt. Er wird zwischen Staaten und Wirtschaftsunternehmen geführt, stellt aber gleichermaßen auch eine terroristische Bedrohung dar.

Das Phänomen des Information Warfare besteht darin, dass es praktisch allgegenwärtig ist und trotzdem kaum wahrgenommen wird.

Information Warfare war zwar in den letzten Jahren kurzzeitig ein Hype-Thema, ist dann aber schnell wieder in den Hintergrund gerückt. Woran liegt das? Nun das hat sehr viel mit unserer Mentalität zu tun. Wir glauben nur Dinge, die wir sehen, anfassen, also beweisen können. Wenn Terroristen eine Bombe zünden, kommt das Ereignis in den Nachrichten. Wir verstehen die Situation und reagieren darauf. Genau diese Kriterien umgeht aber Information Warfare. Es ist äußerst schwierig, Menschen für etwas zu sensibilisieren, was sie weder rational noch emotional erfassen können. Noch problematischer wird es, wenn in Zeiten knapper Budgets für dieses scheinbar imaginäre Phänomen auch noch Geld ausgegeben werden soll. Und genau davon lebt dieses sehr reale Szenario. Wenn man dieses Phänomen verstehen will, muss man es erst einmal entmystifizieren und über die Erforschung und Darstellung der Hintergründe, Strukturen und Methoden zu einem plastisch sichtbaren Bild werden lassen, das in einem Pool von unterschiedlichen Wahrnehmungen auf einmal deutliche Konturen bekommt. Dazu muss man aber bereit sein, (Die Anamorphose alte / junge Frau als Beispiel) seinen Blickwinkel zu verändern.



Beginnen wir mit einer Definition. Was ist eigentlich Information Warfare?

*Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own.*

*Such actions are designed to achieve advantages over military or business adversaries.*

[Dr. Ivan Goldberg](#)

Diese Definition beschreibt schon sehr gut, worum es hier geht. Das Ziel heißt Erreichung der Informationsüberlegenheit, im Idealfall sogar Informationshoheit. Der Anwendungsbereich kann militärisch, aber auch wirtschaftlich sein. Eine interessante Erweiterung dieser Information Warfare Definition findet sich in einem Handbuch der US-Navy:

*„Bombing a telephone switching facility is information warfare. So is destroying the switching facility's software. Information warfare is any action to protect our information functions, regardless of the means.“*

Information Warfare ist also nicht, wie der Name suggerieren könnte, nur eine Sache von Hackern und Computerfreaks. Auch der Einsatz massiver Gewalt, verbunden mit physischer Zerstörung gehört dazu und geht damit weit über die bekannten Internetangriffe wie Viren, Trojaner oder Denial of Serviceattacken hinaus.

Information Warfare beschränkt sich auch nicht auf die militärische Auseinandersetzung zwischen Staaten. Auch zivile Unternehmen sind davon betroffen. Die folgende Definition der US-Navy zeigt den umfassenden strategischen Ansatz von Information Warfare, der sich zeitlich und räumlich völlig von den klassischen Vorstellungen eines Krieges löst.

*At the grand strategy level, nations seek to acquire, exploit, and protect information in support of their objectives. This exploitation and protection can occur in the economic, political, or military arenas. Knowledge of the adversary's information is a means to enhance our own capabilities, degrade or counteract enemy capabilities, and protect our own assets, including our own information.*

Aus den verschiedenen Definitionen lassen sich folgende Kernaussagen isolieren:

- Information Warfare ist ein Krieg um Informationen und Informationssysteme
- Information Warfare richtet sich auch gegen Unternehmen
- Information Warfare findet bereits in Friedenszeiten statt
- Information Warfare beginnt weit vor einer kriegerischen Auseinandersetzung
- Information Warfare ist vorbereitend und richtet sich grundsätzlich gegen jeden zu jeder Zeit, um für jeden Eventualfall gerüstet zu sein
- Information Warfare ist strategisch.

Das heißt ganz konkret, Spionage im Sinne einer politischer Informationsgewinnung, aber auch Wirtschaftsspionage finden gemäß dieser Definitionen als ganz legitimes Mittel einer strategischen Absicherung und Vorbereitung im Vorfeld eines möglichen Konfliktes ständig statt. Und das sind natürlich keine rein amerikanischen Doktrinen. Andere Staaten verhalten sich ebenso. Wir sehen uns einer allgegenwärtigen multinationalen Aufklärungsmaschinerie ausgesetzt, ohne dass wir dies wahrnehmen. Das Ziel der Informationsüberlegenheit wird aber nicht nur durch Informationsgewinnung, sondern auch durch das bewusste Verbreiten von Falschinformationen erreicht. Beides steht oft in einer Wechselbeziehung zueinander. Diese Mechanismen sind keineswegs neu und wurden bereits in der Vergangenheit angewendet.

Ein wunderbares historisches Beispiel für eine derartige Täuschung ist die Geschichte des „Major Martin“.



Geheimoperation Mincemeat (30.April1943)

*ein Toter macht Geschichte*

- Die Operation beginnt im Herbst 1942
- Ziel war die Vorbereitung der Invasion der Alliierten auf Sizilien
- Einsatzdurchführung war der 30. April 1943 in der Bucht von Huelva
- Major Martin wurde am 2. Mai 1943 nördlich von Gibraltar begraben
- Die Landung auf Sizilien erfolgte im Juli 1943 und Major Martin spielte dabei die Hauptrolle

Das wohl prominenteste Beispiel der Historie für die Informationsgewinnung ist vermutlich die deutsche Verschlüsselungsmaschine ENIGMA.



Entwickelt 1920 als hoch technisierte Entschlüsselungsmaschine galt sie mit einem Schlüsselraum  $3 \times 10^{14}$  als fortschrittlichstes und unberechenbares Verschlüsselungsgerät. Trotzdem konnte der Code dieser Maschine später im Rahmen einer 13 Jahre währenden multinationalen nachrichtendienstlichen Operation entschlüsselt werden.

Die Geschichte der „unlösbaren“ Verschlüsselungsmaschine

- entwickelt 1920 als hoch technisierte Entschlüsselungsmaschine
- Schlüsselraum  $3 \times 10^{14}$
- 1928 der polnische Geheimdienst kauft eine zivile Version der Enigma
- 1932 verkauft ein deutscher Überläufer die Kryptologie an den französischen Nachrichtendienst.
- die Informationen werden an den polnischen Geheimdienst weitergeleitet
- 1932 bricht der polnische Kryptologe Marian Rejewsky den Algorithmus
- 1939 im Juli informieren die Polen den britischen und französischen Geheimdienst über ihre Fortschritte
- im September 1939 wurde Blechley Park gegründet
- Alan Turing baut die Turingmaschine
- Mai 1941 wurde das deutsche U-110 gekapert
- von Juni 1941 konnten alle Nachrichten der deutschen U-Boote mitgelesen werden. Das Ziel der Informationsüberlegenheit war erreicht.

... der Rest ist bekannt

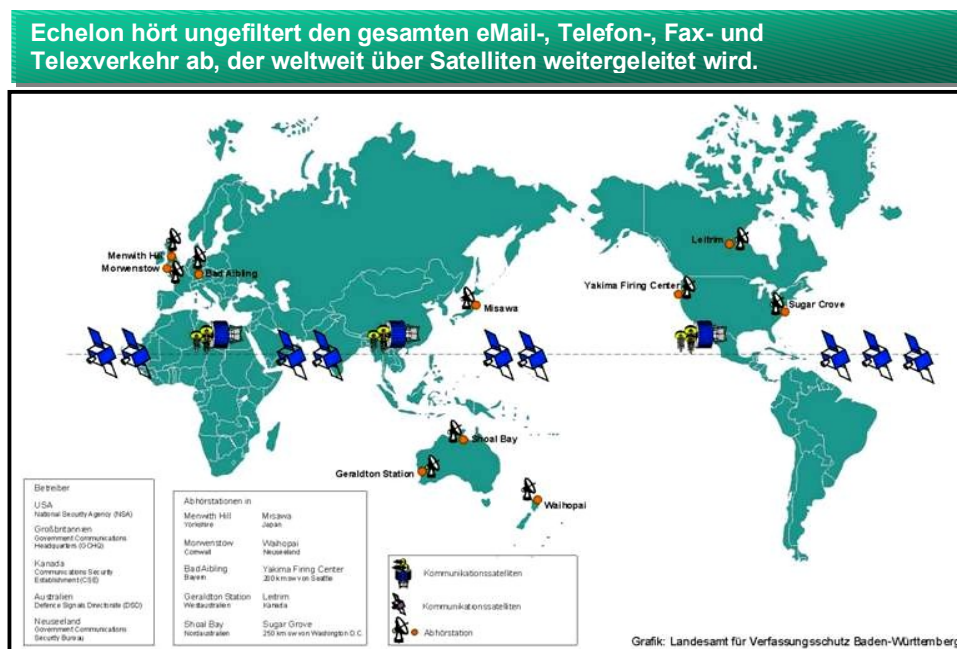
Diese historischen Beispiele belegen die strategische Bedeutung, die Mechanismen des Information Warfare für den Ausgang einer Operation haben. Diese Methoden sind im Zuge der fortschreitenden Kommunikationstechnik wesentlich verfeinert worden.

Dabei betreiben auch Unternehmen professionell Konkurrenzspionage. Die wesentlichen Auftraggeber bei Spionage gegen Unternehmen sind laut einer Studie der Wirtschaftsprüfungsgesellschaft Ernest Young mit 39 % Konkurrenten, mit 19 % Kunden, mit 9 % Zulieferer und mit 7 % Geheimdienste. Spioniert wird von eigenen Mitarbeitern, privaten Spionagefirmen, bezahlten Hackern und Profis der Geheimdienste.

Die Zahl der Firmen, die sich auf das Ausspähen von Daten spezialisiert haben, wächst ständig. Teilweise arbeiten ehemalige Mitarbeiter von Nachrichtendiensten in solchen Firmen. Diese Firmen arbeiten häufig sowohl als Sicherheitsberatungsunternehmen als auch als Detekteien, die im Auftrag Informationen beschaffen. In der Regel werden legale Methoden eingesetzt, aber es gibt auch Firmen, die sich illegaler Methoden bedienen.

Die Angaben zu den Nachrichtendiensten, die gemäß dieser Studie nur 7% der Fälle ausmachen, müssen sicher relativiert werden. Die Dunkelziffer ist hier besonders auch, weil die Industrie trotz inzwischen vorhandener Beweise die Existenz und vor allem die Effizienz der nachrichtendienstlichen Wirtschaftsspionage ignoriert oder grob unterschätzt. Dabei greifen Nachrichtendienste auf der ganzen Welt rund um die Uhr nach interessanten Informationen.

Im Juli 2001 wurde der EU dazu ein Bericht von Gerhard Schmid vorgelegt, in dem die Existenz des Abhörsystems Echelon nachgewiesen wird.

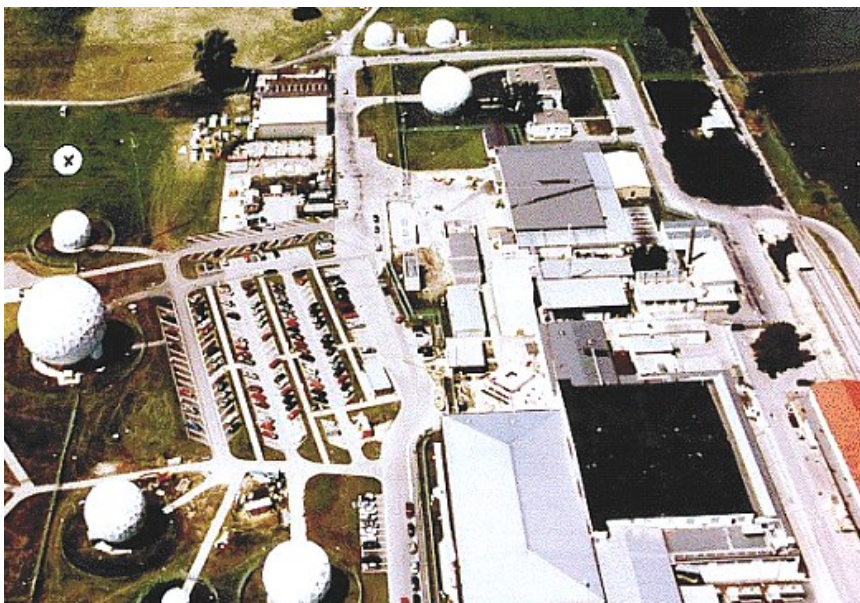


Echelon ist ein Verbund von Abhörstationen rund um den Globus, der systematisch Telefonate, Faxe und E-Mails abhört. Da die Öffentlichkeit keine klaren Informationen hatte, gab es auch hier viele Spekulationen, aber die Bedrohung wurde nicht wirklich ernst genommen.

Tatsächlich ist Echelon aber ein Kernelement des Information Warfare. Es ist jeden Tag rund um die Uhr im Einsatz, allgegenwärtig und liefert eine ungeheure Informationsmenge, die durch Selektionsmechanismen ausgedünnt und durch Supercomputer ausgewertet wird.

Das System wird durch die USA, Großbritannien, Kanada, Australien und Neuseeland betrieben. Keine zufällige Zusammensetzung. Diese Staaten haben 1948 das sogenannte UKUSA-Abkommen unterzeichnet. Ein SIGINT-Abkommen zwischen Großbritannien (United Kingdom, UK), den Vereinigten Staaten (USA) sowie Australien, Kanada und Neuseeland.

Mit seinen geostationären Satelliten und den ca. 120 rund um die Erde verteilten Abhörstationen ist das System in der Lage jeden Ort auf unserem Planeten abzudecken. Damit können mehr als 90% des Internetverkehrs mitverfolgt werden. Die Antennen des Echelon-Systems sind in der Lage, elektromagnetische Wellen einzufangen und dann zur weiteren zentralen Auswertung weiterzuleiten. Abgefangen werden die Nachrichten wahllos, die Auswertung erfolgt nachträglich über Stimm-, Schlüsselwort- oder sonstige Filter. Diese Vorgehensweise wird als "strategische Fernmeldekontrolle" bezeichnet.



Men with Hill, UK

Aber auch andere Staaten betreiben ähnliche Systeme. In den Schweizer Gemeinden Leuk und Heimenschwand stehen die Parabolantennen des Schweizer Systems Onyx, die den Satellitenfunkverkehr abhören und auffangen.



Bodenstation Leuk

Stationen des französischen Nachrichtendienstes DGSE (Direction générale de la sécurité extérieur) werden in den überseeischen Gebieten Kourou in Französisch Guyana sowie in Mayotte vermutet. Weitere Stationen sollen in Frankreich in Domme in der Nähe von Bordeaux sowie in Alluetts-le-Roi in der Nähe von Paris angesiedelt sein. Die Anzahl der Satellitenantennen werden auf insgesamt 30 geschätzt.

Der russische Nachrichtendienst betreibt bzw. betrieb außerhalb Russlands Bodenstationen in Lettland, Vietnam und Kuba. Zusammen mit in Russland selbst vorhandenen Stationen ist eine globale Abdeckung möglich.

Auch andere Staaten wie z.B. die Volksrepublik China betreiben Abhörstationen, haben aber weder eigenes Territorium noch enge Verbündete in den dafür notwendigen Teilen der Welt, um ein globales Abhörsystem zu betreiben.

Dennoch gibt es zumindest drei global wirkende Abhörsysteme, die regional noch durch die kleineren Staaten ergänzt werden.

Kaum vorstellbar, dass dabei auch nur ein Telefonat, eine E-Mail oder ein Fax unentdeckt bleibt.

Und von all dem bemerken wir nichts.

Im Gegensatz zu den anderen Staaten geben die USA die Abhörtätigkeit jedoch zu und rechtfertigen ihr Verhalten als zumindest moralisch legitimiert.

Woolsey, 7. März 2000 in Washington

*Der ehemalige Direktor der CIA, James Woolsey, bestätigte am 7. März in Washington, dass die USA Wirtschaftsgeheimnisse stehlen, „mit Spionage, durch Abhören, durch Aufklärungssatelliten“.*

*Wirtschaftsspionage sei gerechtfertigt, da europäische Unternehmen eine "nationale Kultur" der Bestechung hätten.*

*Zum Thema Echelon sagte er: Der Bericht "Interception Capabilities 2000 ist intellektuell aufrichtig.*

*Ich hoffe, ...dass die Regierung der Vereinigten Staaten fortfährt, Bestechung zum Ziel von Spionage zu machen.“*

*Würde [...] man eine technologische Analyse von etwas aus einem befreundetem Land machen ...und das dann in der Schublade liegen lassen... das wäre ein Missbrauch von Ressourcen der Nachrichtendienste.*

The Wall Street Journal 17. März 2000

*„Ja, meine kontinentaleuropäischen Freunde, wir haben euch ausspioniert. Und es stimmt, dass wir Computer benutzen, um die Daten nach Schlüsselbegriffen zu durchsuchen.“*

*„Die meiste europäische Technologie lohnt den Aufwand gar nicht, sie zu stehlen.“*

Aus einem früheren CIA-Bericht

*1993 habe die CIA so in 51 Fällen im Wert von 28 Mrd. Dollar Informationen gesammelt, bei denen ausländische Firmen oder deren Regierungen durch Bestechung oder Insider-Informationen zu Ungunsten von US-Firmen versucht haben, Geschäfte abzuschließen. 6,5 Mrd. gingen nach Intervention an US-Firmen.*

The Wall Street Journal, April 13, 2000

*Air Force Lt. Gen. Michael Hayden (Dir. NSA) bestätigt, dass die NSA europäische Firmen abhört, um Geldwäsche, Technologietransfer und Korruptionfälle zu ermitteln.*

Angesichts dieser Aussagen wird folgendes klar:

- Nicht nur Politiker und Militärs sondern auch Unternehmen werden systematisch abgehört
- Die Informationen werden an die Konkurrenz weitergegeben
- Die betroffenen Unternehmen verlieren Umsatz
- Wir haben von all dem nichts gemerkt
- Die Bedrohung wurde und wird weiterhin weitgehend negiert.

Und das ist nicht etwa graue Theorie. Der Fall Rabta in Libyen ist ein konkretes Beispiel dafür, daß diese Mechanismen auch genau so genutzt werden. Der deutsche Unternehmer Hippenstiehl-Imhausen hat dies mit allen Konsequenzen erfahren. US-Geheimdienste haben Telefonate und Faxe seiner Firma Imhausen Chemie abgehört und dabei festgestellt, dass das Unternehmen Substanzen zur Erzeugung von Giftgas nach Libyen liefert. Dies stellt einen Verstoß gegen das Kriegswaffenkontrollgesetz dar und ist strafbar. Die deutsche Regierung wurde darüber informiert, das Unternehmen wurde angeklagt und der Unternehmer verurteilt. Auch wenn in diesem Fall von einer moralischen Rechtfertigung gesprochen werden kann, beweist der Vorgang eindeutig die gängige Abhörpraxis. Diese Informationen konnten nur gewonnen werden, weil Satellitenverkehre wie mit einem Staubsauger aufgefangen und ausgewertet wurden. An dieser Situation hat sich bis heute nichts geändert. Nur anders als in dem Fall Rabta erfährt das betroffene Unternehmen nicht, was mit seinen Daten passiert. Geheimdienste veröffentlichen natürlich nur ungern Ihre technischen Möglichkeiten. Immerhin handelt es sich hier um Staatsgeheimnisse. Aus dem Echelonbericht sind dennoch einige Zahlen über die Erfassungsmöglichkeiten bekannt.

Das methodische Vorgehen von Nachrichtendienste besteht darin, mittels einer **strategischen** Fernmeldekontrolle Informationen aus dem Ausland über das Ausland zu beschaffen. Dazu werden mit einer Reihe von Suchbegriffen Satellitenverkehre abgegriffen. Das Mengengerüst für den Bereich Deutschland stellte sich so dar (Stand Jahr 2000):

Von den rund 10 Millionen internationalen Kommunikationsverbindungen/Tag, die von und nach Deutschland stattfanden, wurden etwa 800.000 über Satellit abgewickelt. Davon wurden knapp 10 % (75.000) über eine Suchmaschine gefiltert.

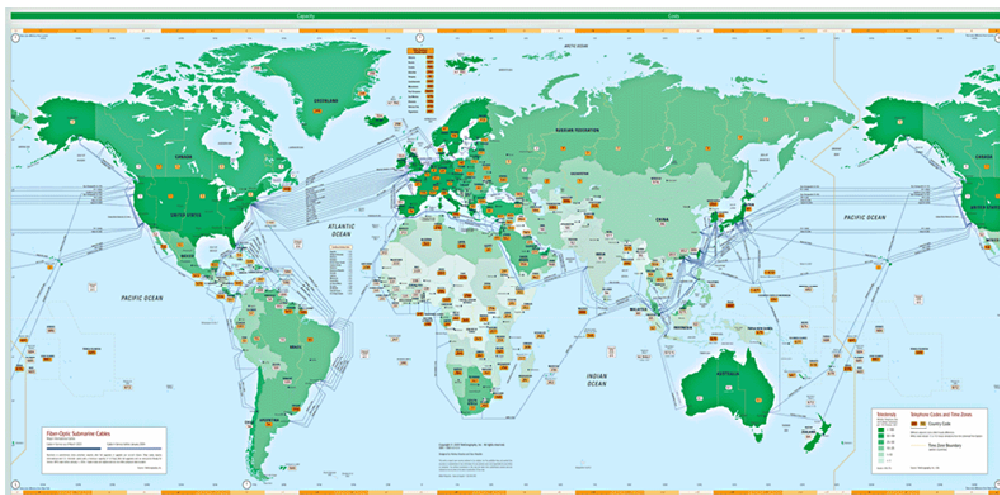
Für die Selektion wurden ca. 2.000 Suchbegriffe im Bereich der Proliferation, 1.000 Suchbegriffe im Bereich des Rüstungshandels, 500 Suchbegriffe im Bereich des Terrorismus und 400 Suchbegriffe im Bereich des Drogenhandels verwendet.

Wenn die Suchmaschinen feststellten, dass ein Suchbegriff vorhanden war, wurde die Nachricht dann der weiteren Bearbeitung zugeführt.

Die Kapazität von über Satelliten geführten digitalen Verbindungen beschränkte sich pro Transponder am Satelliten auf **1890** Sprachkanäle mit ISDN-Standard (64 kbits/sec). Demgegenüber konnten auf einer einzigen Glasfaser bereits **241920** Sprachkanäle mit dem gleichen Standard übertragen werden.

Das entspricht einem Verhältnis von **1:128!**

Die Qualität von Glasfaser-Seekabel Verbindungen ist besser als über Satelliten.



Allerdings waren 2000 nur 15 % der Weltbevölkerung an das globale Kabelnetz angeschlossen. Inzwischen hat sich dieser Wert zwar verbessert, aber für bestimmte Anwendungen werden Satellitensysteme trotzdem weiterhin genutzt.

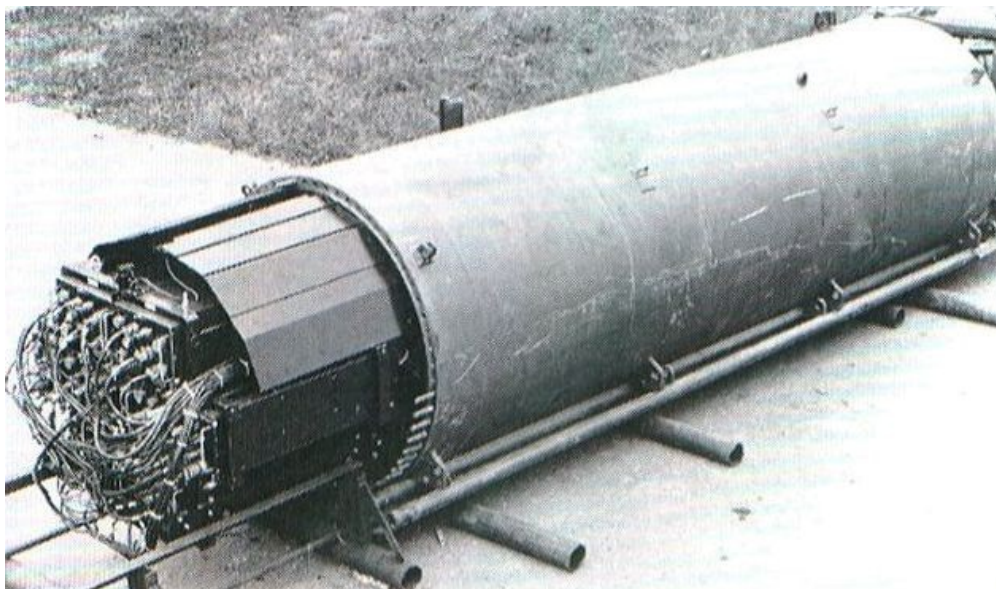
Nationale, regionale und internationale Telefon- und Datenverkehre in Gebieten mit geringem Kommunikationsaufkommen werden auch weiterhin über Satelliten geführt.

Die Abstrahlung eines einzigen geostationären Satelliten kann fast 50 % der Erdoberfläche überdecken, auch unwegsames Gelände kann überbrückt werden. In diesem Gebiet werden dann 100 % der Benutzer, egal ob zu Land, zur See oder in der Luft abgedeckt.

Satelliten sind in wenigen Monaten betriebsbereit, unabhängig von der Infrastruktur vor Ort, sie sind zuverlässiger als Kabel und können müheloser abgelöst werden. Und sie können ebenso mühelos abgehört werden.

Wohl gemerkt, dies war der Stand vor sechs Jahren. Inzwischen hat sich die Technik revolutionär weiterentwickelt. Sowohl das Verkehrsaufkommen als auch die Erfassungs- und Auswertungsmöglichkeiten haben sich vervielfacht. Kommunikation findet heutzutage im Wesentlichen digital statt.

Nun wäre es aber falsch zu glauben, die Verkehre über die Seekabel wären sicher. Auch diese Verbindungen können abgehört werden. Bereits 1971 stand die Technik dafür zur Verfügung. Das US U-Boot Halibut drang in das Ochotski-Meer ein und hörte ein sowjetisches Unterseekabel ab, um das technische Prinzip zu prüfen. 1972 kam das U-Boot wieder und montierte eine Abhörvorrichtung mit dem Code-Namen "Ivy Bells" in der Nähe des Kabels. Da das Kabel selbst physikalisch nicht beschädigt wurde, blieb diese Abhöraktion geheim. Sie wurde erst 1982 aufgedeckt, als ein ehemaliger NSA-Mitarbeiter die Information an die UdSSR verkaufte.

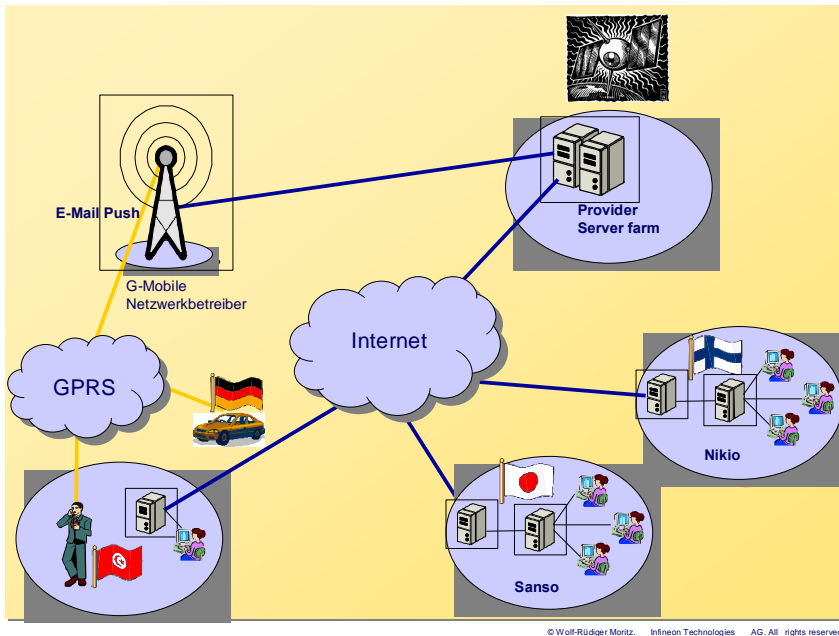


„Ivy Bells“ Abhörvorrichtung aus 1971

Aus diesen Vorgängen lässt sich erkennen, dass in einigen Staaten eine starke Motivation vorhanden ist, Information Warfare auch in der Wirtschaft einzusetzen. Dennoch findet man in vielen Unternehmen die Einstellung vor: „Ich glaub ja, dass es so etwas gibt, aber wir sind für einen Nachrichtendienst nicht interessant“ oder noch schlimmer: „Wir übertragen soviel Daten, damit kann keiner etwas anfangen. Dies ist ein fataler Irrglaube. Die Kriterien techn. Transfer, Korruption und Geldwäsche lassen grundsätzlich jedes Unternehmen verdächtig erscheinen. Im Umkehrschluss muss also jedes Unternehmen abgehört werden. Zweifelsohne gibt es hier Untergrenzen, unterhalb derer ein Unternehmen nicht mehr interessant ist, aber grundsätzlich sollte sich niemand wirklich sicher fühlen. Der Grad der Bedrohung steigt natürlich mit dem Spezialisierungsgrad und der Marktdurchdringung eines Produkts. Unternehmen der Militärtechnik stehen hier natürlich an vorderster Front.

Neben den klassischen Abhörmethoden spielt inzwischen das Internet eine große Rolle in der Information Warfare Welt. Hier gibt es inzwischen eine Vielzahl von Spionagetools zum Downloaden für jedermann. Aber es gibt auch Provider, die zunehmend sensible Informationen von Behörden, Unternehmen und Privatleuten verwalten. Web-Konferenzen, E-Mailer etc. speichern eine Vielzahl von

Informationen. Wer kann heute noch nachvollziehen, was damit geschieht. Zudem gibt es Systemarchitekturen, deren Design sicherheitstechnisch extrem bedenklich erscheint.



Ein ganz neuer Aspekt des Information Warfare ist die terroristische Bedrohung. Auch Gruppierungen wie AL Quaida machen sich die moderne Technik als Waffe zu eigen. Hier treten wir in eine ganz neue Dimension ein. Al Quaida Mitglieder haben von außerhalb der USA die kritische Infrastruktur des Landes aufgeklärt. Auch dabei wurden u.a. folgende Informationen gesammelt:

- Wo sind die Knotenpunkte des Schienenverkehrs?
- Wo sind die großen Erdgaslager?
- Wo sind die großen Brücken über Flüsse, in denen Glasfaserleitungen für das Internet verlaufen?

Die moderne Kommunikations- und Informationstechnologie macht es heute möglich, eine derartige Aufklärung zu betreiben. In der Vergangenheit hätte man dazu eine große Anzahl von Menschen benötigt, die sich im ganzen Land verteilt, die Informationen hätten zusammensuchen müssen. Das Risiko, dabei aufzufallen, war relativ hoch. Heute ist es möglich, in einem Cyber Cafe in Peshawar zu sitzen und eine derartige Aufklärung zu betreiben. Und dies, geschützt vor einer strafrechtlichen Verfolgung, möglicherweise sogar mit Duldung und Unterstützung des jeweiligen Landes. Einige Al Quaida Mitglieder haben inzwischen eine Ausbildung in Computer Security und besuchen Hacker Trainings. Damit sind sie zukünftig in der Lage, aus ihrer Sicht feindliche Staaten aus dem Internet anzugreifen. Die Angriffe werden sich gegen die kritische Infrastruktur richten. Kernkraftwerke, Schaltzentralen für Luft- oder Schienenverkehr, Chemiewerke, Telekommunikationseinrichtungen, Energieversorger oder das Know How der High Tech Industrie. Die Auswirkungen können verheerend sein. Ohne dass nur ein Schuß fällt. Die Beispiele in USA und Italien haben gezeigt, wie anfällig unsere Stromnetze bereits heute auf einzelne Störungen sind. Was geschieht bei einem planmäßigen Angriff auf die Stromversorgung?

Das ist die Herausforderung, der wir uns zu stellen haben.

An dieser Stelle sei aber auch erwähnt, dass die Unternehmen in aller Regel über geeignete IT Sicherheitsmaßnahmen verfügen. Zur Panik gibt es keinen Anlaß, aber es gibt auch keine hundertprozentige Sicherheit und Microsoft Schwächen werden immer nur zeitverzögert erkannt und das Expertenwissen von professionellen Angreifern und Terroristen steigt. Deshalb müssen wir wachsam bleiben.

*“The world is a dangerous place to live, not because of the people who are evil, but because of the people who don't do anything about it.”* Albert Einstein