softScheck
we identify vulnerabilities others don't

Spionage in Russland – Espionage in Russia

Technische Möglichkeiten und lokale Situation: Analyse und Bewertung von Spionagefällen auf der Grundlage ausgewerteter Berichte der deutschen Abwehrbehörden sowie der von Partnerstaaten

Stand: 1. Mai 2010

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter softScheck GmbH Köln
Hartmut.Pohl@softScheck.com
www.softScheck.com

soft5check
we identify vulnerabilities others don't

Spionage in Russland

Technische Möglichkeiten und lokale Situation: Analyse und Bewertung von Spionagefällen auf der Grundlage ausgewerteter Berichte der deutschen Abwehrbehörden sowie der von Partnerstaaten

Prof. Dr. Hartmut Pohl

Begründung und Ziele dieser Studie

Spionageaktivitäten in den Nachfolgestaaten der UdSSR haben nach amtlichen Erkenntnissen der zuständigen in- und ausländischen Sicherheitsbehörden (in Deutschland das Bundesamt und Landesämter für Verfassungsschutz sowie BND) mit dem sog. Ende des kalten Krieges nicht nachgelassen, sie sind beginnend mit 1995 sogar intensiviert worden.

Im Folgenden sollen die Aktivitäten gegnerischer Nachrichtendienste sowie die Aktivitäten sog. Partnerdienste in Russland auf Grund vorliegender Erkenntnisse detaillierter beschrieben werden.

Ausdrücklich muss darauf hingewiesen werden, dass Russland nach wie vor bestrebt ist, zukünftig ein Schwellenland zu werden. Derzeit ist es politisch, gesellschaftlich (überproportional starke Korruption) und insbesondere wirtschaftlich noch in einem Vorstadium mit Rubel-Verfall, Zahlungsunfähigkeit als Folge ungedeckter Staatsanleihen und Zusammenbruch der russischen Finanzmärkte Mitte 1999. Derzeit ist Russland zu 75% in der Hand von Oligarchen, gegen die die Regierung nicht vorgehen kann. Mehr als die Hälfte der Wirtschaft gehört der Schattenwirtschaft an. Viele Banken werden von mafiosen oder anderweitig kriminellen Strukturen zumindest beeinflusst.

Diese Situation wird nicht nur von den russischen Nachrichtendiensten ausgenutzt sondern auch von den Nachrichtendiensten einer ganzen Reihe anderer Nationen; das Ausmaß der nachrichtendienstlichen Aktivitäten wird schon allein durch die Quantität der aktiven Dienste deutlich - vergl. hierzu die Auflistung in Kapitel 6.

Mit den beiden folgende Aspekten muss in Russland gerechnet werden.

- Nachrichtendienstliches Vorgehen ist kein Selbst-Zweck. Informationssuche, Beschaffung und Auswertung dienen ausschließlich dem Zweck, nationale Unternehmen kostengünstig mit wirtschaftlich relevanten Informationen zu versorgen.
- Häufig werden die ausspionierten Informationen gar nicht den eigenen nationalen Unternehmen weitergegeben, sondern anderen Unternehmen im internationalen Bereich gegen Entgelt verkauft; damit werden Devisen erworben, die der Dienst und/oder das Land dringend benötigen.

softScheck
we identify vulnerabilities others don't

Inhaltsverzeichnis

Management Summary

Wirtschaftsspionage wird in Russland von einer ganzen Reihe von Nachrichtendiensten aktiv betrieben - vergl. die Auflistung in Kap. 6: Insgesamt sind mehr als 6 (!) russische Nachrichtendienste und Behörden identifiziert mit insgesamt mehr als 290.000 Mitarbeitern sowie etwa 40 (!) aktive ausländische Nachrichtendienste.

Wegen der vielfältig ausgenutzten menschlichen Schwächen sowie der technischen Möglichkeiten der vollständigen Überwachung (Video, akustisch, elektronisch) muss von jeglicher mündlichen persönlichen (!) Erörterung wichtiger Themen und auch per Telefon (Festnetz, Satelliten und mobil) und der Verarbeitung wertvollerer Informationen in Informationsverarbeitungssystemen (Computer, Telefone und Faxgeräte) strikt abgeraten werden.

Angesichts der ungeordneten gesellschaftlichen, politisch instabilen und sozial schlechten Verhältnisse dürfte die unten geschilderte Sicherheitslage noch einige Jahre anhalten.

1. Klassische Sicherheitsaspekte

Alle Spionageaktivitäten in Russland dienen zwar auch politischen Zielen - in erster Linie aber und zu etwa 85 % zur Erlangung wirtschaftlich relevanter Informationen (Wirtschaftsspionage). Diese Informationen wurden historisch und werden unmittelbar den russischen Unternehmen zur Nutzung weitergegeben. Der die Wirtschaftsspionage ausführende Nachrichtendienst ist hier nur die auf Spionage spezialisierte Einheit, die (Spionage)-Dienstleistungsfunktionen im Auftrag der Unternehmen erbringt.

In Russland sind eine ganze Reihe von Nachrichtendiensten aktiv - vergl. die Auflistung in Kap. 6: Insgesamt sind 14 (!) russische Nachrichtendienste und Behörden identifiziert.

Darüber hinaus kann davon ausgegangen werden, dass westliche Nachrichtendienste gleichermaßen in Russland aktiv sind - auf nationaler gesetzlicher Basis auch die der deutschen Partnerstaaten USA (CIA und NSA), England (GCHQ), die Niederlande (IDB) und Frankreich (DGSE). Insgesamt sind etwa 40 (!) ausländische Nachrichtendienste identifiziert.

Im Folgenden werden die nachgewiesenen Praktiken dargestellt.

1.1 Personelle Sicherheit

Mitarbeiter westlicher Unternehmen (und auch Behörden wie Botschaftsangestellte oder Mitarbeiter westlicher Nachrichtendienste (!)) wurden immer wieder von (männlichen und/oder weiblichen) Mitarbeitern russischer Nachrichtendienste erfolgreich kompromittiert, erpresst und verführt (durch Kunstwerke wie z.B. alte Ikonen oder (klassisch) gunstgewerbliche Aktivitäten), Sicherheitsmaßnahmen der Unternehmen und Behörden mitzuteilen, zu unterlaufen oder sogar abzuschalten. Auf diese Weise wurden direkt oder indirekt von den Mitarbeitern Zugangskontrollinformation oder auch Zugriffskontrollinformation wie Paßworte erhalten und wertvollste Informationen und Dokumente erlangt.

1.2 Klassisch-materielle Sicherheit

Die russischen Behörden besitzen mit Angriffen im Bereich der klassisch-materiellen Sicherheit einen seit Jahrzehnten aufgebauten hohen Wissensstand.

1.2.1 Unberechtigter Zugang

Dabei ist es unerheblich, dass alle Akten und Computer unter einer sog. Aufsicht durch das westliche Unternehmen stehen. Tatsächlich sind die Reinigungskräfte von den Nachrichtendiensten durchsetzt. Durch personelle Maßnahmen reicht es den Diensten völlig, für kurze Zeit oder auch nur gelegentlich Zugang zu Akten und Computern zu haben, um die aktuellen wertvollen Daten unerkannt zu kopieren.

So ist das folgende Verfahren gängig: Eine Person lenkt den Besitzer der Schlüssel zu den Büroräumen geeignet ab; eine zweite Person kopiert währenddessen die Daten und gibt den Schlüssel rechtzeitig zurück. Keiner bemerkt die unberechtigten Aktivitäten - noch nicht einmal die vorübergehende Entwendung des Schlüssels wird bemerkt; Passworte und andere Sicherheitsmaßnahmen werden durch social engineering erhalten.

Die Zahl unbemerkt entwendeter Notebooks mit wertvollen gespeicher-

ten Daten hat sehr stark zugenommen.

1.2.2 Installation von Abhöranlagen

Es muss davon ausgegangen werden, dass Privaträume wie Hotelzimmer und Wohnungen der Mitarbeiter vollständig verwanzt sind mit Mikrofonen und Kameras. Derartiges Mini-Equipment (Aufnahmegeräte und Sender) ist international frei erhältlich - in Deutschland für unter DM 500.-. Die Geräte werden für Laien unerkennbar in Lampen, Zimmerecken, Stuckdecken, Uhren etc. installiert.

So mussten die USA den (noch nicht bezogenen) Neubau ihres Botschaftsgebäudes deswegen abreißen, weil der Ausbau derartiger Komponenten teurer geworden wäre als ein (erneuter) Neubau; dieser (zweite) Neubau wurde mit (vollständig) aus den USA eingeflogenen Materialien, Sand, Zement, Stahl, Putz, Tapeten ... unter ständiger Aufsicht (!) mit US-Mitarbeitern errichtet.

1.3 Abstrahlung

1.3.1 Möglichkeiten des illegalen Abhörens

Die Möglichkeiten des illegalen Abhörens lassen sich in zwei Gruppen untergliedern

- Ausnutzen der bloßstellenden (kompromittierenden) Abstrahlung von IT-Geräten
- Optische und akustische Verfahren
- Eine Abhörmaßnahme erfordert in diesen Fällen keinen direkten Zugang zu dem abgehörten Konferenzraum/Büro; er kann von weit außerhalb erfolgen und ist nur schwer nachweisbar.

1.3.2 Optische Abstrahlung

Alle Gespräche (Raum, Telefon) können mit Laserstrahlen von den im Gesprächs- und Geräuschrhythmus schwingenden Fensterscheiben abgenommen werden. Dazu gehören auch die Geräusche mechanischer und elektrischer Schreibmaschinen, so dass der geschriebene Text abgehört werden kann.

1.3.3 Akustische Abstrahlung

Mit Hilfe von Mikrofonen können die o.g. Geräusche direkt aufgenommen werden.

Sofern Gespräche in abgelegenen Gegenden (sog. Einsamkeit) geführt werden, können diese (über Entfernungen von bis zu 2 km und meist unbemerkt) mit Richtmikrofonen abgehört werden. Dies gilt gleichermaßen für Gespräche in belebten Gegenden wie Boulevards und Kaufhäusern.

1.3.4 Elektromagnetische Abstrahlung

Die praktische Möglichkeit und auch Nutzung (!) der elektromagnetischen Abstrahlung wurde bis 1995 von den zuständigen deutschen Behörden (BND, ZSI, BSI) bestritten. Heute wird von denselben Behörden ausdrücklich vor den Risiken gewarnt: Alle (elektronischen) Geräte strahlen (etwa auf Fernsehfrequenz) die verarbeiteten Informationen auswertbar wieder ab; dies gilt für Telefone, Faxgeräte, Sichtgeräte,

Prozessoren, Plattenlaufwerke, Streamer, Router, Gateways, ...

1.3.5 Mikrowellen-Einstrahlung

Eingestrahlte Mikrowellen werden durch elektronische Geräte wie Telefone, Faxgeräte und Computer im Rhythmus der jeweils verarbeiteten Informationen moduliert; die modulierten Mikrowellen können wieder aufgefangen werden. Das Verfahren ist nur äußerst schwer zu bemerken.

2. Aufnehmen elektronischer Kommunikation

2.1 Telefon/Telefax, Mobil-Telefone

Jegliche Kommunikation lässt sich auf dem Leitungswege und auf Richtfunkstrecken gezielt und vollständig abhören.

Schnurlos Telefone besitzen wg. der fehlenden Verschlüsselung der sog. Luftschnittstelle keinerlei Sicherheit. Im Gegenteil sind sie leichter abzuhören als leitungsgebundene Telefone.

Mit Hilfe des sog. Mikrofonie-Effekts kann bei aufgelegtem Telefonhörer mit Hilfe des eingebauten Mikrofons der jeweilige Raum abgehört werden.

2.1.1 Mobil-Telefone

Die Abhörsicherheit ist bekanntlich grundsätzlich gering und eine missbräuchliche Nutzung von Mobiltelefonen jederzeit möglich. Es muss davon ausgegangen werden, dass jegliche Kommunikation abgehört wird.

Mobiltelefone bestehen aus zwei Komponenten: Dem Mobilfunkgerät selbst und dem Identifikationsmodul (SIM). Damit wird im GSM-Netz zwischen Nutzer und Gerät unterschieden.

Das Mobilfunkgerät ist durch seine international eindeutige Seriennummer (IMEI) gekennzeichnet. Der Nutzer wird durch seine auf der SIM-Karte gespeicherten Kundennummer (IMSI) gekennzeichnet. Diese Nummer wird dem Teilnehmer bei der Anmeldung vom Netzbetreiber zugeteilt. Sie ist zu unterscheiden von den ihm zugewiesenen Telefonnummern (MSISDN). Durch diese Trennung ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobilfunkgeräte nutzen kann.

Der Zugang zur SIM-Karte ist nur durch eine vier- bis achtstellige PIN, die nach dem Einschalten des Mobiltelefons eingegeben werden muss, gegen unberechtigten Zugriff geschützt.

Auf der Funkstrecke (sog. Luftschnittstelle) zwischen dem Mobiltelefon und der Basisstation wird in der Regel verschlüsselt übertragen. Das Verfahren ist allerdings geknackt. Aus betrieblichen Gründen besteht darüber hinaus die Möglichkeit, das Schlüsselverfahren abzuschalten und dann die Gespräche unverschlüsselt zu übertragen. Einige Länder nutzen die Möglichkeit der Verschlüsselung nicht und übertragen unverschlüsselt (z.B. Frankreich).

2.1.1.1 Verbindungsaufbau

Sobald der Besitzer sein Mobiltelefon einschaltet, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten zur Identität des Nutzers, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Dies erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

Bei der Mobil-Kommunikation können die übertragenen Signale auf der "Funkstrecke" nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden, weshalb ein Angreifer seinen Angriff ohne

weiteres durchführen kann. Ein zweites, generell bei den meisten Funkdiensten auftretendes Problem resultiert daraus, dass die mobilen Kommunikationspartner aus technischen Gründen geortet werden müssen, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls – im Zuge des Verbindungsaufbaus – Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber – aber auch von Dritten – zur Bildung sogenannter "Bewegungsprofile" verwendet werden.

Bei satellitengestützten Kommunikationsdiensten ist eine genaue Ortung zum Teil nicht erforderlich, aber gleichwohl möglich. Besonders problematisch ist hier, dass die Kommunikationsinhalte im gesamten Abstrahlbereich des Satelliten empfangen und ausgewertet werden können.

Da bei jeder Mobilfunk-Verbindung auch Festnetze benutzt werden, kann die Sicherheit im Mobilfunknetz nicht größer als im Festnetz sein.

2.1.1.2 Kartenmissbrauch

Gelangt ein Unbefugter in den Besitz einer SIM-Karte (z.B. durch Fund oder Diebstahl), kann er, sofern ihm die PIN bekannt ist, auf Kosten des rechtmäßigen Karteninhabers telefonieren - ggf. auch den Berechtigten vortäuschen.

Daten wie Telefonbuch oder Kurznachrichten, die auf der SIM-Karte gespeichert sind, können einen sensitiven Charakter haben. Ein Verlust der Karte bedeutet also unter Umständen die Offenlegung dieser gespeicherten Informationen.

Die Sicherheitsmechanismen bestimmter SIM-Karten können umgangen werden; damit ist möglich, diese SIM-Karten zu kopieren.

2.1.1.3 Erstellen von Bewegungsprofilen

Beim Einbuchen eines Mobiltelefons werden aus technischen Gründen Informationen über die genutzte Basisstation, die Identität des Nutzers und die Seriennummer des Mobilgerätes an den **Netzbetreiber** übermittelt. Damit kann ein Netzbetreiber feststellen, wann, wo und von wem ein bestimmtes Mobiltelefon eingeschaltet bzw. benutzt wurde. Die Erstellung von Kommunikationsprofilen und personenbezogenen Bewegungsprofilen ist möglich. Durch das Auswerten der Übertragungsprotokolle ist der Netzbetreiber auch in der Lage, die Entfernung des Teilnehmers zur Basisstation zu bestimmen. Diese Entfernungsauswertung wird zum Vorteil der Kunden für die Realisierung der sogenannten "Homezone" genutzt. Mittels spezieller **Angriffstechnik** ist es möglich, von allen Mobiltelefonen innerhalb des Erfassungsbereiches sowohl die Karten- als auch die Geräteidentität zu ermitteln, ohne dass der Zugang zu den beim Netzbetreiber gespeicherten Verbindungsdaten erforderlich wäre. Damit können ebenfalls Bewegungsprofile von bestimmten Personen oder Mobilfunkgeräten erstellt werden. Durch die zusätzliche Anwendung von **Peilempfängern** ist es darüber hinaus technisch möglich, den genauen Standort eines bestimmten Mobiltelefons zu lokalisieren.

2.1.1.4 Rufnummernermittlung

Auf den Richtfunkstrecken im Mobilfunknetz können die Gespräche anhand der Mobilfunkgerätenummer (IMEI) aus dem Datenstrom gezielt herausgefiltert werden. Die Gespräche können auch im öffentlichen Telefonfestnetz identifiziert werden. Hierfür ist die Kenntnis der Teilnehmerrufnummer (MSISDN) notwendig. Kundennummer (IMSI) und IMEI

können mit entsprechendem Angriffsgerät direkt auf der Funkstrecke zwischen Mobiltelefon und Basisstation (BTS) ermittelt werden.

Die Ermittlung der Rufnummer MSISDN kann durch einen Angreifer erfolgen,

- der beim Netzbetreiber aus der Bestandsdatenbank den Zusammenhang zwischen IMSI, IMEI und MSISDN herstellt oder
- der z.B. in einer Firma die dienstlichen oder privaten Telefonnummern aus Telefonlisten holt.

2.1.1.5 Abhören

Telefonate

Ein Angreifer mit Zugang zu den **technischen Einrichtungen des Netzbetreibers** (Leitungen, Vermittlungseinrichtungen, Basisstationen) ist in der Lage, alle Telefongespräche, die über diese Einrichtungen geführt werden, abzuhören. Dies gilt sowohl für Verbindungen im Mobilfunknetz als auch im Festnetz.

Werden die Verbindungen über leitungsgebundene Wege **von der Basisstation zu der Mobilfunkvermittlung** (MSC) geführt, ist ein physikalischer Angriff auf den Leitungswegen erforderlich. Basisstationen werden meist über eine unverschlüsselte **Richtfunkverbindung** an die Mobilfunkvermittlung (MSC) angebunden; dann besteht die Möglichkeit, diese Funksignale mit Antennen und Spezialempfängern unbemerkt aufzufangen und abzuhören. Die Gefährdung kann sich dadurch erhöhen, dass auf diesen Richtfunkstrecken alle Telefonate der angebundenen Basisstation übertragen werden.

Auch im **Festnetz** werden Telefongespräche gebündelt über **Richtfunkstrecken** übertragen. Da diese Übertragung in der Regel unverschlüsselt erfolgt, sind die übertragenen Gespräche mit einigem technischen Aufwand auch dort identifizierbar und abhörbar.

Die **Funkübertragung zwischen dem Mobiltelefon und der Basisstation** wird zwar grundsätzlich in allen Mobilfunknetzen verschlüsselt. Es gibt jedoch spezielle Angriffsgeräte, die die Schwäche der einseitigen Authentifikation im GSM-Netz (nur Mobiltelefon gegenüber Basisstation) ausnutzen, indem sie den Mobiltelefonen eine Basisstation vortäuschen, die Verschlüsselung abschalten und Klarbetrieb vorgeben.

Die Verschlüsselung kann auch durch technische Manipulationen am Mobiltelefon oder an technischen Einrichtungen des Netzbetreibers abgeschaltet werden.

Raumgespräche

Unter Verwendung von speziell manipulierten Mobiltelefonen ist es möglich, Raumgespräche abzuhören. Das Mobiltelefon dient dabei als Abhöranlage, die über das Telefonnetz von jedem Ort der Welt aktiviert werden kann, ohne dass dies am Mobiltelefon erkennbar wird. Es sind Geräte auf dem Markt, bei denen diese Sonderfunktion mittels zusätzlicher Schaltungseinbauten realisiert ist. Diese Manipulation kann durch eine Sichtprüfung nach Zerlegen des Gerätes oder durch spezielle Untersuchungsmethoden nachgewiesen werden.

2.1.1.6 Manipulationen

Hardware

Neben den zusätzlichen Einbauten sind Manipulationen der Freisprecheinrichtung mit dem Ziel der Ruftonabschaltung sowie manipulierte Akkus mit eingebautem Lauschsender bekannt. Hierdurch kann unbemerkt zu dem derart manipulierten Mobiltelefon eine Gesprächsverbindung zwecks Abhören der Raumgespräche geschaltet werden. Zur Manipulation benötigt der Angreifer das Gerät nur für eine kurze Zeit.

Firmware

Mobiltelefone können mittels regulärer Menüfunktionen, die durch Betätigung bestimmter Tastenkombination aktiviert werden, als Lauschsender geschaltet werden. So ist ein Gerätetyp bekannt, bei dem das Display (Anzeige) des Mobiltelefons abgeschaltet wird, obwohl zu dem Gerät eine Gesprächsverbindung existiert.

Weiterhin kann die geräteinterne Steuersoftware (Firmware) manipuliert werden; dies ist weitaus schwerer zu entdecken als Hardwaremanipulationen.

Eine versteckte, nicht dokumentierte Abhörfunktion kann auch schon bei der Entwicklung des Gerätes (gezielt oder ungezielt!) in die Steuersoftware einprogrammiert werden.

Die Steuersoftware kann auch nachträglich verändert werden z.B. wenn das Gerät bei einer Reparatur oder aus sonstigen Gründen (Verlust, Entwendung) für den Bediener/Nutzer (kurzzeitig) nicht kontrollierbar ist. Für Außenstehende ist diese Manipulation nicht erkennbar.

Durch die Erweiterung der Menüfunktionen der Mobiltelefone mittels "SIM-Toolkit" und einer neuen Generation von SIM-Toolkit-fähigen SIM-Karten werden Mobiltelefone noch flexibler. Ein so ausgestattetes Mobiltelefon lässt sich per Mobilfunk vom Service-Provider mit neuen Funktionen (remote) zum Lauschsender programmieren.

Card-Phones

Mit Hilfe von Mobiltelefonen in Form einer PC-Einsteckkarte (Card-Phone) ist es möglich, Daten vom PC über das Mobilfunknetz weltweit zu übertragen. Auch bei diesen Karten besteht, wie beim normalen Mobiltelefon, die potenzielle Gefahr der Manipulation. Darüber hinaus besteht hier die zusätzliche Gefahr der leichten Manipulierbarkeit der PC-Software. Eine Firewall, wie sie in Rechner-Netzwerken möglich ist, gibt es bei einer Ankopplung über das Mobilfunknetz (noch) nicht. Dieses Risiko ist als besonders kritisch anzusehen, da bei einem solchen Angriff nicht nur die gerade verarbeiteten Informationen, sondern auch der gesamte Datenbestand des PC unbemerkt abfließen oder zerstört werden kann.

Bei dieser Art des Lauschangriffes hat der Geschädigte bei fehlendem Einzelverbindungs-Nachweis weder eine Kontrolle über die Telefonrechnung noch darüber, wer wann mit wem kommuniziert hat. Auch eine nachträgliche Überprüfung ist nicht immer möglich, da die Verbindungsdaten beim Netzbetreiber schon gelöscht sein können.

2.2 Internet-Kommunikation

Internet-Kommunikation wird von Internet Service Providern abgewickelt.

Es muss davon ausgegangen werden, dass jegliche Kommunikation überwacht und (je nach Aufgabenstellung) manipuliert wird. Vergleiche

hierzu auch die Gesetzesdarstellung für Russland.

Wegen der o.g. aufgeführten klassisch-materiellen Risiken, der Abstrahlung und der Aufnahme elektronischer Kommunikation stellt die Verschlüsselung gespeicherter und übertragener Daten nur einen begrenzten Schutz dar.

3. Lagebewertung

3.1 Grundsätzliches

3.1.1 Klassische Erkenntnisse

Spionageaktivitäten werden nicht nur von sog. gegnerischen Diensten betrieben sondern auch von den Diensten sog. Partnerstaaten Deutschlands wie den USA, Frankreich, England und den Niederlanden; ein Beispiel dafür ist die Mitte März 1997 gegen das Bundesministerium für Wirtschaft gerichtete Spionageaktion des amerikanischen Auslandsgeheimdienstes CIA: Zwei CIA-Agenten haben als Angehörige der US-Botschaft versucht, sich über einen hohen Beamten des Bundesministeriums für Wirtschaft Informationen über deutsche Hochtechnologieprodukte sowie wirtschaftspolitische Hintergründe zu verschaffen.

Die Interessen fremder Nachrichtendienste sind außerordentlich breit gefächert; sie umfassen nahezu den gesamten Bereich der industriellen Forschung und Produktion, des Handels und der wirtschaftlichen Organisation. Dabei kann es sich im einzelnen um folgende Informationen handeln.

- Unternehmensleitung: Strategische/taktische Entscheidungen.
- Forschung und Entwicklung: Forschungsergebnisse, Produktideen, Designstudien.
- Produktion: Konstruktionsunterlagen, Herstellungsverfahren, Qualitätsprüfungsmaßnahmen, Spezialwerkzeuge, Steuerungssysteme.
- Einkauf: Lieferanten, Versorgungskonzeption, Lagerbestände.
- Verkauf: Verkaufsstrategien, Marketingstudien, Absatz- und Vertriebswege, Lizenzverträge, Umsätze, Kundenadressen, Angebote.
- Finanzwesen, Controlling, Kalkulationsunterlagen, Budgetplanungen, Investitionsvorhaben.
- Informationsverarbeitung sämtlicher Unternehmensbereiche.

Das Ausforschungsinteresse beschränkt sich also keineswegs auf die Beschaffung fertiger Endprodukte, sondern gilt - von der Idee über die Forschung, Entwicklung, Herstellung und Marktstrategie - grundsätzlich dem gesamten Zyklus eines Wirtschaftsguts.

Um die o.g. Informationen zu erlangen sind die folgenden Informationen hilfreich:

- Zugangsmöglichkeiten und Maßnahmen des Objektschutzes.
- Feststellungen über den Personalaufbau, die soziale Schichtung der Mitarbeiter, politische Tendenzen im Betrieb sowie eine Aufstellung des Schlüsselpersonals.
- Operative Ansatzpunkte in bezug auf die diversen "Wissensträger" (z. B. Personen, Mitarbeiter im Bereich Informationsverarbeitung, Dokumentationen und Akten).

Gleichermaßen betroffen sind auch Zulieferfirmen, Technologie- und Transferzentren, Übersetzungsbüros, Unternehmensberater, Zulassungsstellen und Information Broker.

3.1.1.1 Gesetzliche Grundlagen behördlicher Aktivitäten in Russland

Alle Abhör-Aktivitäten beruhen auf SORM - System of Operative and Investigative Procedures aus 1995. Im gleichen Jahr gab das Gesetz 'Operational Investigations' dem FSB die Möglichkeit der Überwachung jeglicher Kommunikation; die Internet-Dienst-Provider werden darin zur Kooperation verpflichtet.

Das Bundesgesetz Nr. 5 der Russischen Föderation "über die Auslandsaufklärung" vom 10. Januar 1996 deklariert als eines der Ziele der Nachrichtenbeschaffung die Wirtschaftsspionage.

3.1.1.2 Die Nachrichtendienste Russlands

Als Hauptträger dieser Aktivitäten fungieren die nachfolgend dargestellten sechs - voneinander weitgehend unabhängigen - Sicherheitsdiensten, die - wenn auch mit unterschiedlicher Gewichtung - alle im Inland operieren.

Ziviler Aufklärungsdienst SWR

Wie mehr oder weniger alle zivilen russischen Nachrichtendienste ist auch der derzeit rd. 15.000 Mitarbeiter umfassende SWR aus dem sowjetischen KGB hervorgegangen.

Militärischer Aufklärungsdienst GRU

Die GRU, die "Hauptverwaltung Aufklärung beim Generalstab", bildet das zweite wichtige Standbein der russischen Auslandsspionage. Als Nachfolgeorganisation des Geheimdienstes der früheren "Roten Armee" ressortiert sie seit 1992 beim Verteidigungsministerium der Russischen Föderation.. Die Hauptaufgabe dieses etwa 12.000 Mitarbeiter umfassenden Dienstes liegt in der Beschaffung nachrichtendienstlicher Informationen aus dem militärischen, militärpolitischen, -technischen und ökonomischen Bereich.

Technischer Aufklärungsdienst FAPSI

FAPSI, der "Bundesagentur für staatliches Nachrichten- und Informationswesen", wurden vielfältige Aufgaben auf dem Gebiet der elektronischen Aufklärung sowie im Bereich des Funk- und Fernmeldewesens übertragen. Der weltweit operierende Dienst kann das Pendant der US-amerikanischen "National Security Agency" (NSA) betrachtet werden. Die FAPSI beschäftigt bis zu 120.000 Mitarbeiter. Ihr weitgestecktes Tätigkeitsfeld schließt die globale Erfassung des internationalen Funk- und Fernmeldeverkehrs ein. Auf elektronischem Wege wird in ausländische Kommunikationsnetze und -kanäle eingedrungen und der Inhalt nachrichtendienstlich interessanter Verbindungen entschlüsselt.

Abwehrdienst FSB

Der "Föderale Sicherheitsdienst" ist zwar als inländischer Abwehrdienst zunächst einmal für die zivile Spionageabwehr, die innere Sicherheit der russischen Streitkräfte sowie die Bekämpfung von Terrorismus und "Organisierter Kriminalität" zuständig. Dem im wesentlichen aus dem gefürchteten Repressionsapparat des KGB hervorgegangenen Dienst wird im "Gesetz

über die Organe des FSB" vom 12. April 1995 zusätzlich aber auch die Kompetenz zur Wirtschaftsspionage eingeräumt.

Aufgrund seiner Aufgabenstellung, ausländische Staatsangehörige - Diplomaten, Journalisten und Geschäftsleute ebenso wie Privatreisende - während ihres Russlandaufenthalts zu überwachen, ergeben sich für den FSB günstige operative Ansatzpunkte für Aufklärungsaktivitäten. Seine Mitwirkung bei den Einreisekontrollen eröffnet ihm sehr frühzeitig die Möglichkeit, nachrichtendienstlich interessante Zielpersonen auszuwählen. Mit Hilfe von Telefon-Überwachungsmaßnahmen und der Befugnis, ohne spezielle richterliche Genehmigung - allein aufgrund bloßen Verdachts - (Geschäfts-)Räume zu durchsuchen, ist der FSB in der Lage, Ausländer während ihres gesamten Aufenthalts auf russischem Territorium lückenlos zu überwachen. Der FSB hat einen Personalbestand von rund 100.000 Mitarbeitern. Er wurde 1998/99 von Wladimir PUTIN geleitet.

Weitere russische Nachrichtendienste

Zusätzlich zu den vier etwas ausführlicher dargestellten Nachrichtendiensten unterhält Russland noch den "Föderalen Schutzdienst" (FSO) sowie die "Verwaltung Aufklärung der Grenztruppen". Dem FSO, der durch die Zusammenführung der bisher selbständigen Organisationen "Sicherheitsdienst des Präsidenten" (SBP) und "Hauptverwaltung Schutz" (GUO) entstanden ist, obliegt in erster Linie der Personen- und Objektschutz für die wichtigsten Repräsentanten und Einrichtungen des Staates. Darüber hinaus ist der derzeit ca. 40.000 Mitarbeiter umfassende Dienst auch für die Erledigung spezieller Informationsanliegen des russischen Präsidenten zuständig und operiert in diesem Zusammenhang gegebenenfalls auch im Ausland. Mit der "Verwaltung Aufklärung der Grenztruppen" wurde innerhalb des "Föderalen Grenzdienstes" eine eigenständige nachrichtendienstliche Komponente mit etwa 4.000 Mitarbeitern eingerichtet. Diese wird durch das Gesetz über die russische Auslandsaufklärung dazu ermächtigt, zum Schutz der Staatsgrenzen, der Wirtschaftszone sowie der russischen Hoheitsgewässer auch externe Informationsbeschaffung, insbesondere in den Grenzregionen (Flugplätze und Moskau) zu betreiben.

Nachrichtendienst	Mitarbeiter
SWR	15.000
GRU	12.000
FAPSI	120.000
FSB	100.000
SBP	40.000
FSO	4.000
Summe	**291.000**

Abb. 1: Anzahl der Mitarbeiter russischer Nachrichtendienste

3.1.2 Nachrichtendienste der übrigen GUS-Republiken

Nach dem Untergang der UdSSR bildete die Einrichtung eigener Geheimdienste in den neu- bzw. wiederentstandenen unabhängigen Staaten eines der ersten äußeren Anzeichen ihrer Souveränität. In aller Regel basieren in den früheren Unionsrepubliken die neuen zivilen Dienste auf den einstigen Strukturen des KGB. Sofern neben dem zivilen auch noch ein militärischer Nachrichtendienst etabliert wurde, ist dieser meist aus der ehemaligen regionalen Präsenz der GRU hervorgegangen.

Die intensivsten Verbindungen unterhält die russische Auslandsaufklärung zu den entsprechenden Diensten Weißrusslands und Kasachstans. Hier muss von einer umfassenden gegenseitigen Unterrichtung und einem regelmäßigen Informationsaustausch gewonnener Erkenntnisse ausgegangen werden. Eine weitere Effizienzsteigerung ist in die am 18. April 1997 von den Leitern der Abwehr- und Sicherheitsdienste der GUS in Moskau unterzeichneten Vereinbarung über den Aufbau eines gemeinsamen Dateninformationssystems in Moskau.

3.1.2.1 Ukraine

Die Kommunikation in der Ukraine ist unreglementiert!

3.1.2.2 Kasachstan

Die Gesetzeslage in entspricht der Russlands.

3.1.2.3 Nachrichtendienste sonstiger osteuropäischer Staaten

Schon bald nach Auflösung des Warschauer Paktes erklärten Ungarn und die seinerzeitige Tschechoslowakei ihren Verzicht auf die nachrichtendienstliche Ausforschung Deutschlands. Polen, Bulgarien und Rumänien hielten dagegen an der Spionage fest.

3.1.3 Volksrepubliken China

Das chinesische "Ministerium für Staatssicherheit" (MSS) mit seinem Personalbestand von mehr als 800.000 Mitarbeitern dürfte inzwischen der größte Geheimdienst der Welt sein. Ihm sind gleichermaßen Abwehr- und Aufklärungskompetenzen zugewiesen.

Als militärischer Nachrichtendienst Chinas fungiert die "2. Abteilung des Generalstabs der Volksbefreiungsarmee". Die im Auslandseinsatz tätigen Agenten dieser Organisation sind vielfach bei den Militärattaches der chinesischen Auslandsvertretungen angesiedelt.

3.2 Mitarbeiter

Für alle relevanten Bereiche stehen in Russland exzellente Fachleute (Akademiker und Praktiker) zu geringen Löhnen zur Verfügung. Da elektronische Geräte billig zu erwerben sind, ist der Gesamtaufwand für Spionage-Angriffe jeder Art gering.

Konspirativ auftretende Agenten im Zielobjekt ("Quelle im Objekt") - Innentäter stellen die größte Gefahr für die Sicherheitsinteressen eines Unternehmens dar. Die eigenen Mitarbeiter sind in Anbetracht ihrer legalen Zugangsmöglichkeiten und ihres Insider-Wissens über innerbetriebliche Schwachstellen in der Lage, mehr Vertrauliches zu verraten, als extern operierende Agenten fremder Nachrichtendienste je indirekt

herausfinden könnten. Die Dienste werden daher auch in Zukunft größte Anstrengungen unternehmen, hochqualifizierte Fachleute für nachrichtendienstliche Zwecke anzuwerben.

3.3 Personelle Sicherheit

Auf das (bekannte) Überangebot von im gunstgewerblichen Bereich aktiven, gebildeten Menschen muss hier der Vollständigkeit halber deutlich hingewiesen werden.

4. Schutzmaßnahmen

Angesichts der Breite der tatsächlichen Angriffe und deren Intensität sollen hier die wichtigsten Maßnahmen genannt werden. Unverzichtbar ist in jedem Fall eine Risikoanalyse - insbesondere zusammen mit einer Informationswertanalyse.

Genereller Verzicht auf wichtige Gespräche.

Genereller und vollständiger Verzicht auf wichtige elektronische Kommunikation (Telefon im Festnetz, schnurlos und mobil; Fax; e-mail; file transfer etc.).

4.1 Personelle, organisatorische, klassisch-materielle Schutzmaßnahmen

- Sensibilisierung aller (!) Mitarbeiter für die o.g. umfassenden Risiken. Erfahrungsgemäß ist gerade dies deswegen besonders schwierig, weil bestimmte Risikobereiche gar nicht ernst genommen werden.
- Eindeutige Zuweisung von Kompetenzen und Zuständigkeiten, klare Regelungen (erneute Schulung, Verpflichtung zur Teilnahme an Schulungs- und Fortbildungsmaßnahmen).
- Umfassende Kontrolle aller Mitarbeiter! Austausch der Mitarbeiter allein schon bei vermuteten (!) Unregelmäßigkeiten - unabhängig vom Verschulden oder auch nur bei Fahrlässigkeit!
- Förmliche Belehrung, Abmahnung, Umsetzung bis hin zu arbeitsrechtlichen Konsequenzen (Kündigung) bei erkannten Sicherheitsverstößen.
- Unverzichtbare organisatorische Schutzmaßnahme ist die Erstellung einer vollständigen unternehmensübergreifenden IT-Sicherheitspolicy.
- Eigene vollständige Raum- und Gebäudeüberwachung mit Zugangskontrolle des Geländes, des Gebäudes und aller Räume - ggf. auch der Wohnungen
- Erst-Überprüfung, Wiederholungsüberprüfung sowie anlassbezogene Überprüfungen aller Räume auf eingebaute Mikrofone (Wanzen) und Kameras.

4.2 Maßnahmen gegen Abstrahlung

Es können aufwendige Faraday'sche Käfige installiert werden. Eine Maßnahme gegen akustische Abstrahlung stellt die ausschließliche Nutzung von Innenräumen dar.

4.3 Schutz elektronischer Kommunikation

4.3.1 Illegales Abhören

- Verlagerung des Konferenzraumes/Büros in einen anderen (von außen nicht einsehbaren) Gebäudeteil, z.B. im Gebäudekern oder Keller (fensterlos).
- Einsatz von akustisch gedämmten und elektromagnetisch geschirmten Kabinen.
- Verwendung von Netz- , Telefon- und Datenleitungsfiltern.
- Regelmäßige Überprüfung der Netz-, Telefon- und Datenlei-

tungen auf Manipulationen.

- Einsatz von Einrichtungen zum Aufspüren aktiver Minisender.

4.3.2 Mobilkommunikation

4.3.2.1 Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte sollten stets sicher aufbewahrt werden. Die persönliche Geheimzahl PIN darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden.

Bei Verlust der SIM–Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch, und damit auch einen persönlichen Schaden, abzuwehren.

Bei Verlust oder Diebstahl des Mobiltelefons, kann der Netzbetreiber die weitere Nutzung des Mobiltelefons unterbinden. Hierzu benötigt er die Angabe der Gerätenummer (IMEI). Sie steht häufig auf der Rückseite des Gerätes und sollte daher notiert und unabhängig vom Gerät aufbewahrt werden.

Um die missbräuchliche Nutzung der SIM-Karte rechtzeitig zu bemerken, sollte in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

4.3.2.2 Erstellen von Bewegungsprofilen

Eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer wird zumindest erschwert, wenn Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden..

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons; der Akku muss entfernt werden.

4.3.2.3 Rufnummernermittlung

Der Austausch von Mobiltelefonen und SIM-Karten bietet aber nur einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen. Die Zuordnung zum Unternehmen bleibt aber bestehen!

- Andere Möglichkeiten zum Schutz gegen Rufnummernermittlung:
- Keine Veröffentlichung der Rufnummern im öffentlichen Telefonbuch,
- Keine Veröffentlichung der Rufnummern im internen Telefonbuch.

4.3.2.4 Abhören von Telefonaten

Es existiert kein Schutz.

Folgende Maßnahmen können zur Verringerung der Gefährdung empfohlen werden:

- Grundsätzlich keine Telefongespräche mit sensiblen Inhalt führen.
- Im Verdachtsfall sollte das Mobiltelefon seinen Nutzer wechseln.
- Einzelverbindungsnachweis auf unbekannte Rufnummern hin überprüfen.
- Prüfen, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden. Fehlende Gebühren für bestimmte Verbindungen deuten auf Abhören hin.

4.3.2.5 Abhören der Raumgespräche

- Das Abhören von Raumgesprächen mittels Mobiltelefonen kann nur dann sicher ausgeschlossen werden, wenn das Einbringen von Mobiltelefonen in den zu schützenden Raum verhindert wird.
- Das Ausschalten des Mobiltelefons reicht als Schutz nicht aus, da im Manipulationsfall ein unbemerktes Einschalten über die Funkstrecke nicht mit hinreichender Sicherheit ausgeschlossen werden kann. Eine ungewollte Inbetriebnahme lässt sich nur durch das Entfernen des Akkus unterbinden.
- Auf dem Markt sind passive Warngeräte verfügbar, die eingeschaltete Mobiltelefone melden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, solche Warngeräte zu installieren und diese bei Gesprächen mit sensitivem oder vertraulichem Inhalt zu aktivieren.
- Aktive Mobiltelefon-Detektoren, die auch Mobiltelefone im Ruhebetrieb (stand-by) detektieren können, sind ebenfalls sinnvoll.

4.4 Schutz vor Hardwaremanipulation

Das Risiko einer Manipulation, kann zumindest vermindert werden, wenn folgende Punkte beachtet werden:

- Der Kauf von Mobiltelefonen sollte bei vertrauenswürdigen Stellen erfolgen, damit nicht schon beim Erwerb mit einer Manipulation gerechnet werden muss. Bei großer Stückzahl ist der Erwerb nach dem Zufallsprinzip an verschiedenen Stellen sicherer.
- Generell sollten keine Mobiltelefone unbekannter Herkunft benutzt werden, da für diese Geräte keine Aussage über ihre Manipulationsfreiheit getroffen werden kann.
- Besteht der Verdacht einer Manipulation (Reparatur, Mobiltelefon wird eine zeitlang vermisst), sollte das Mobiltelefon aus dem Verkehr gezogen werden.
- Hardwaremanipulationen können z.B. sicher mit Röntgenprüfverfahren erkannt werden, indem man Referenzröntgenbilder von nicht manipulierten Mobiltelefonen (direkt nach Erwerb) mit aktuellen Bildaufnahmen (nach Manipulationsverdacht) vergleicht.

4.4.1.1 Schutz vor manipulierter Firmware

Derzeit existiert kein Prüfwerkzeug, mit dem die Firmware von Mobiltelefonen auf Manipulationen hin überprüft werden können..

4.4.1.2 Manipulierte Card-Phones

Mobilfunkkarten sollten auf sensitive Daten verarbeitenden PC's o.ä. nicht zugelassen werden.

4.4.2 Internetkommunikation

Die auch für die technische Aufklärung zuständige FAPSI intensiviert ihre Anstrengungen zur Teilnahme am Wirtschaftsleben. So hat sich dieser Dienst auf verschiedenen Fachmessen als Anbieter auf dem Gebiet der Datensicherheit und Verschlüsselungstechnik präsentiert. Die internationale Vermarktung solcher Produkte dient nicht nur der Deviseneinnahme, sondern eröffnet gleichzeitig weitreichende Zugriffsmöglichkeiten auf die verschlüsselte Kommunikation der Kunden.

5. Einige in Moskau nachrichtendienstlich aktive Nationen und deren Institutionen

Die im folgenden genannten Behörden und Einrichtungen stellen eine Auswahl der wichtigsten ständig in Moskau nachrichtendienstlich (Wirtschaftsspionage) aktiven Institutionen dar; je nach Projekt findet auch eine gegenseitige Abstimmung statt. Weitere Institutionen anderer Staaten sind ebenfalls aktiv.

5.1 Russland

CSR	Central Intelligence Service - Centralnaya Sluzhbza Razvedky.
FAPSI	Federal Agency for Government Communications & Information - Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii.
FPS	Federal Border Service - Federal'naya Pogranichnaya Sluzhba.
FSB	Federal Security Service - Federal'naya Sluzhba Bezopasnosti.
FSK	Federal Counterintelligence Service - Federal'naya Sluzhba Kontr-razvedky.
FSO	Federal Protective Service - Federal'naya Sluzhba Okhrani.
GosTekhKomissiya	State Technical Commission - Gosudarstvennii Tekhnologiam Komissiya.
GRU	Main Intelligence Directorate - Glavnoye Razvedyvatelnoye Upravlenie.
GUO	Main Administration for the Protection of the Russian Federation - Glavnoye Upravlenie Okhrani Rossiiskoy Federatsii.
KGB	Committee for State Security - Komitet Gosudarstvennoi Bezopasnosti.
MBR	SECURITY MINISTRY OF RUSSIA - Ministerstvo Bezopasnosti Ruskii.
PSB	Presidential Security Service - Prezidentskaya Sluzhba Bezopasnosti.
SOUD	Interlinked System for Recognizing Enemies - Sisteme Objedinennovo Utschotya Dannych o Protivniki.
SVR	Foreign Intelligence Service - Sluzhba Vneshney Razvedki.

5.2 China

CAIFC	China Association for International Friendly Contacts.
FD	Fourth Department.
NI	Naval Intelligence.
PAP	People's Armed Police.
PLA	People's Liberation Army.
PLAAF	PLA Air Force.
PLAN	PLA Navy.
SD	Second Department [Intelligence].

SRI	Sixth Research Institute.
TD	Third Department.
UCSR	8341 Unit - Central Security Regiment.

5.3 England

"D" Notice Committee.

DIS	Defence Intelligence Staff.
GCHQ	Government Communications Headquarters.
JARIC	Joint Air Reconnaissance Intelligence Centre.
JIC	Central Intelligence Machinery Joint Intelligence Committee.
MI5	Security Service.
NCIS	National Criminal Intelligence Service.
SIS	MI6 Secret Intelligence Service.

Strike Command.

5.4 Frankreich

BRGE	Intelligence and Electronic Warfare Brigade - Brigade de Renseignement et de Guerre Electronique
DGSE	General Directorate for External Security - Direction Generale de la Securite Exterieure
DISSI	Interministerial Office for Information Systems Security Service - Delegation Interministerielle a la Securite des Systemes d'Information
DPSD	Directorate for Defense Protection and Security - Direction de la Protection et de la Securite de la Defense
DRM	Directorate of Military Intelligence - Direction du Renseignement Militaire
SCSSI	Central Service for Information System Security - Service central de la s,curit, des systemes d'informations.

5.5 Israel

Mossad	Institute for Intelligence and Special Tasks - ha-Mossad le-Modiin ule-Tafkidim Meyuhadim
Shin Bet	General Security Service - Sherut ha-Bitachon ha-Klali
Aman	Military Intelligence - Agaf ha-Modi'in
Lekem	Bureau of Scientific Relations - Leshkat Kesher Madao
CPR	Center for Political Research - Ministry of Foreign Affairs

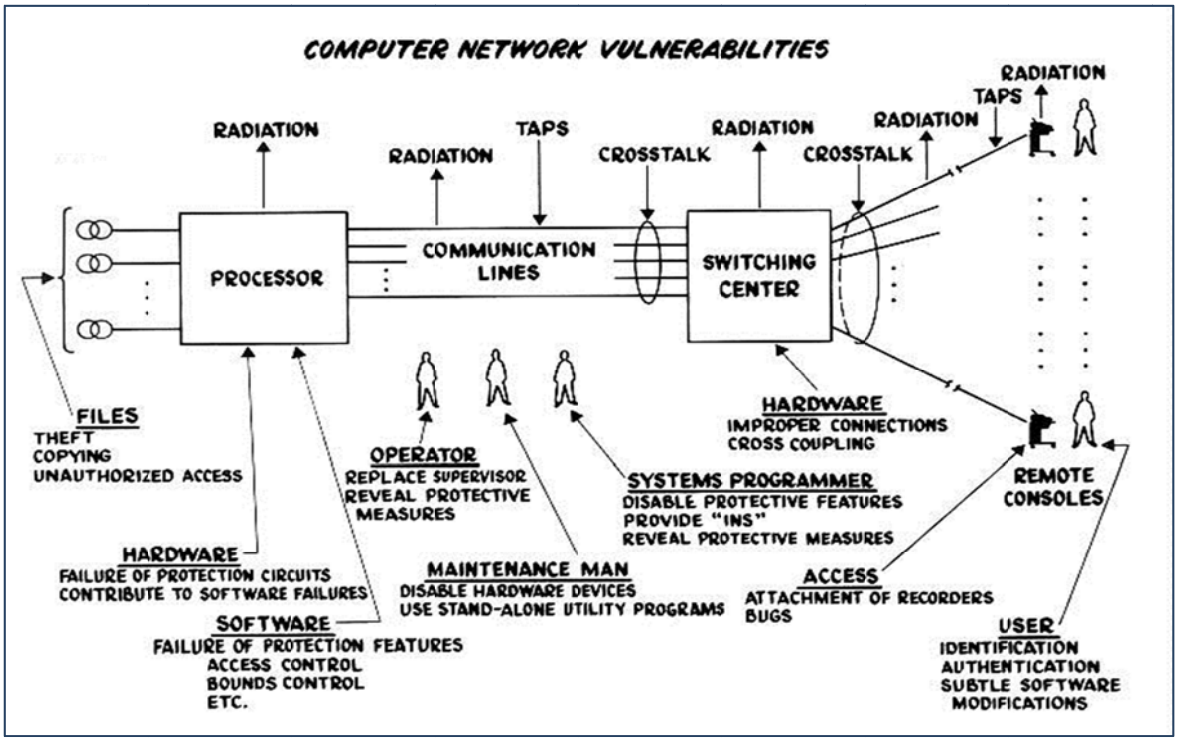
5.6 Niederlande

IDB	Foreign Intelligence Service
TIVC	Technisches Informationsverarbeitungszentrum (Marine-Geheimdienst).

5.7 USA

AI	Army Intelligence).
BIMS	Bureau of Intelligence of the military services (Air Force, Marine Corps, Navy Intelligence.
BIRDS	Bureau of Intelligence and Research of the Department of State.
CIA	Central Intelligence Agency.

DIA	Defense Intelligence Agency.
DoE	Department of Energy.
DoT	Department of Treasury.
MICS	Members of the Intelligence Community Staff.
NSA	National Security Agency.
SORP DoD	Special Offices of the Reconnaissance Programs of the Department of Defense.



Computer Network Vulnerabilities. Nach: Ware, W.: In: Security Controls fo Computer systems. Report of the Defense Science Board Task Force on Computer Security. Washington 1970