



Blankenfelder Straße 69

**D- 13127 Berlin**

Lauschabwehrexperte seit 1971

Unternehmensberater seit 1990

**Hotline: +49(0)30 42 45 441**

<http://www.herbertsbuero.de>

<http://www.lauschabwehr-kunz.de>

<http://www.lauschtechnik.eu>

<http://www.lauschabwehrteam.eu>

## Thema: Lauschabwehr

Unter dem Begriff Lauschabwehr versteht man die Aufklärung und Abwehr elektronischer Raumüberwachung und verdeckten Telefonanzapfungen zum Zwecke des Abhörens, das Aufspüren von Manipulationen in und auf IuK- Netzwerken zur Informationsgewinnung, das Erkennen von verdeckten [vercontainterter] Video- und Beobachtungssystemen sowie die Enttarnung von Datenklau auf und in technischen Systemen und Strukturen. Insgesamt ist die Lauschabwehr ein ganzheitlicher Prozess von wissenschaftlichen und technischen Maßnahmen unter Nutzung neuester technologischer Verfahren sowie der Anwendung geeigneter technischer Mittel und Methoden, die in ihrer Komplexität aus visuell-technischen Untersuchungen und operativ-technischen Überprüfungen zur Aufklärung und Abwehr von Informationslecks beitragen.

Versuche in den Besitz fremder Informationen zu gelangen sind vermutlich so alt wie die Menschheit selbst. Schließlich ist „Wissen - Macht“ und „Nichtwissen - Ohnmacht“. Einen Informationsvorsprung zu erzielen oder ein Geheimnis zuhüten, dieses waren schon immer die grundlegende Eckpfeiler von Erpressungen, von Machtausübung und von Einflussnahme sowie der Manipulation von Menschen, der Wirtschaft, der Politik oder der gesellschaftlichen Prozesse. So schuf man, z.B. im Mittelalter geheime Lauschkanäle und Beobachtungsschlitze, um u.a. in Kirchen und Klöstern [Sitz der damaligen Eliten] zu spionieren.

Mit den technischen Entwicklungen, der Drahttelefonie (1876), der drahtlosen Telegrafie (1897) aber insbesondere mit der Entdeckung der elektromagnetischen Wellen (1886) und der ersten drahtlosen Hörtonübertragung (1895) sowie der Patentierung des Röhrensenders (1913) und der Ausstrahlung der ersten Rundfunkübertragung (1920) wurden die Grundlagen für das technische Abhören nach dem heute noch gültigen Grundprinzip „*Aufnehmen- Übertragen- Empfangen*“ gelegt. Mit der Einführung des Stereoprinzips (1960) und den Abstrahlung auf den UKW-Frequenzen im VHF/UHF-Bereichen auf den Bändern I-III, später Band IV erfolgte in den 1950-iger Jahren ein weiterer Qualitätssprung des drahtlosen Abhörens.

Heute nutzt man für die geheime Informationsbeschaffung weiterhin die klassischen Verfahren in Verbindung mit den technologisch neuartigen Materialien. So z.B. unter anderem, drahtlose und drahtgebundene digitalisierte RF/VLF- Mittel u. Methoden, drahtlose und drahtgebundene Körperschallsysteme, drahtlose und drahtgebundene analoge und digitalisierte Videoverfahren, Ausnutzung der Infrarottechnik zur Übertragung des gesprochenen Wortes sowie bildlicher Darstellungen, Einsatz neu entwickelter Lichtmikrofone ohne Metallverwendung (nicht detektierbar), Lichtwellenspiegelung durch Prismen usw. In den Frequenzbereichen 5 kHz bis 25 THz ist technologisch heute schon fast alles möglich!

Auf dem Gebiet der Abhörtechnik u.a. Spionagemethoden hat sich in den letzten Jahrzehnten einiges rasant geändert: So, unter anderem die technologischen Möglichkeiten, die eingesetzten

Mittel, Methoden und Materialien, aber auch die Vielfalt wissenschaftlich-technischer Erkenntnisse. Diese sind geradezu exponentiell gewachsen. Unsere heutige „unverzichtbare“ hochtechnologische Umgebung [DECT, Mobilfunk, WLAN-, dLAN-, Glasfaser(LWL), Breitbandkabel etc.] bieten eine Vielzahl von „verwundbaren“ Angriffszielen. Unsere Informations- und Kommunikationssysteme strahlen „*ungewollt*“ elektromagnetische Wechselfelder [NF/VLF] und hochfrequente Aussendungen [RF/VLF] ab. Unsere Kommunikation und Datenübertragung kann ohne Manipulationen, ohne Platzierung von Spionagetechniken und anderer Aufklärungshilfen belauscht, bespitzelt und beklaut werden. Abschöpfungswürdige Datensätze mit z.T. kompromittierenden Inhalten befinden sich ständig auf den stromführenden Leitungssystemen und schaffen übrige Gefahren. Dazu kommt, dass in der gegenwärtigen Phase des wissenschaftlich-technischen Prozesses ein schneller Wechsel von analogen Einheiten hin zu den digitalen Systemen stattfindet. Das betrifft u.a. nicht nur, die nicht mehr detektierbare Materialien und Werkstoffe, die Vercontainerung, die Miniaturisierung, die Lebensdauer die Übertragungsgeschwindigkeit, die Verschlüsselungsarten sowie die Reichweiten sondern auch die viele anderen neuen Funktionalitäten heutiger Spionagetechnik. So können u.a. mit Hilfe der GSM-, GPS- und UMTS- Frequenzen [kein Open end, absehbar] praktisch schon heute über Kontinente hinweg echtzeitmäßig gelauscht, gespitzelt und beobachtet sowie Datenklau betrieben werden. Mit dem Wettstreit der Systeme Ende der 1940-iger Jahre und mit der Entwicklung der sog. Harmonika-(Telefon)-Wanze und ihres Einsatzes in den 1960-iger Jahren fand auch auf dem Gebiet der geheimen Informationsgewinnung und der illegalen Datenbeschaffung eine Globalisierung (heute: Echolon) statt.

Mit einer Ausspionierung z.B. des Unternehmensaufbaus, der innerbetrieblichen Strukturen und des internen Firmenablagensystems eines Unternehmens der Begierde, ist auch eine optimale und zielorientierte Informationsbeschaffung und Datenspionage durch einen äußeren technischen Angriff jederzeit möglich. Ein Betreten des Zielobjektes, ein Manipulationen firmeninterner Systeme oder das Platzieren von Spionagetechnik sowie das Abschöpfen menschlicher Quellen ist nicht mehr [kaum noch!] notwendig. Die wesentlichen Angriffspunkte der Wirtschaftsspionage und der Konkurrenzausspähung bilden zurzeit u.a.;

- das Abhören der „*öffentlichen*“ Kommunikationsstrecken
- die Platzierung von „*vorbereitetem Equipment*“
- das nachträgliche Einschleusen von „*Aufklärungshilfen*“
- das Eindringen in die „*strategische IuK- Infrastruktur*“ u.a. Schwachstellen des Zielobjektes [SIGINT]
- Social- engineering- Techniken, Nutzung menschliche Quellen, Abschöpfung im Gesprächen [HUMINT]
- Auswertung von Studien, Statistiken, Veröffentlichungen, Kongresse und Veranstaltungen [OSINT]

Die klassischen Angriffsrichtungen bilden weiterhin, der Angriff auf das *gesprochene Wort* und zunehmend der Angriff auf die *digitale Information*.

In der technischen Abwehr- und Aufklärungsarbeit bei der Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung stehen u.a. folgende Erkenntnisse zur Aufarbeitung an;

- das Problem, der zunehmende Komplexität der IuK- Systeme
- das Problem, dass bei allen technischen Systemen, die „Funktionalität“ vor „Sicherheit“ geht
- das Problem, dass eine nachträgliche Sicherheitsüberprüfung, auf Grund der Komplexität der Systeme einen hohen Zeitaufwand in Anspruch nehmen und dadurch eine 100%ige Überprüfung kaum noch durchführbar wird
- Und das Problem, dass unter dem Gesichtspunkt der Wirtschaftsspionage jederzeit mit einer „vorsätzlichen“ Schwächung strategischer IuK- Systeme auch in mittelständigen Firmen zu rechnen ist und das eine solche technische Beeinflussung dann faktisch nicht mehr detektierbar ist

Dieser Problemstellungen müssen sich, die Handvoll existierenden, hauptsächlich technisch ausgerichteten Unternehmen, der inländischen Lauschabwehranbieter stellen, um nicht Gefahr laufen zu müssen den technologischen Anschluss zu verlieren um auch zukünftig weithin in der Weltspitze mitspielen zu können.

erarbeitet: LAT Herbert Kunz / Berlin