



Der Fall „ENERCON“

Methoden, Instrumente und Auswirkungen der Wirtschaftsspionage am Beispiel der Gesellschaft „ENERCON“

Seminararbeit zur Vorlesung

Militärökonomie

Wintertrimester 2000

Daniel Trapp

Werner - Heisenberg - Weg 112

85579 Neubiberg

Matrikel-Nummer: 820 415

5. Trimester

Lehrstuhl:

Prof. Dr. J. Schnell

Betreuer:

Dipl.- Kfm.

Gabriel Straub

Inhaltsverzeichnis

	Seite
1. Einführung in die Thematik	1
2. Grundlagen der Wirtschaftsspionage	4
2.1 Definitionen und Begriffsabgrenzung	4
2.2 Übersicht über Methoden, Instrumente und Auswirkungen der Wirtschaftsspionage	6
3. Verlauf der Wirtschaftsspionage am Beispiel der Gesellschaft „ ENERCON “	11
4. Fazit	19
Literaturverzeichnis	22
Anhang	24

1. Einführung in die Thematik

Der Schaden, der alljährlich der deutschen Wirtschaft durch Spionage entsteht, ist nicht eindeutig zu quantifizieren, man geht jedoch von einigen Milliarden Mark aus. *Liebl* wies in einer Studie aus dem Jahre 1988 nach, dass derartige Verluste mindestens acht Milliarden Deutsche Mark pro Jahr ausmachten (Ulfkotte (1999), S. 46). Der Leiter der Abteilung Spionageabwehr des Verfassungsschutzes in Baden-Württemberg Harald Woll schätzt die aktuellen Verluste auf 20-40 Milliarden Deutsche Mark pro Jahr (o.V. (1999a), S.32). Diese Größenordnung zeigt schon die Wichtigkeit für die deutsche Wirtschaft, zumal für die Spionage nicht mehr die wie in der Vergangenheit vorherrschende Ausrichtung der Spionage an Freund-Feind-Konstellationen vorliegt, sondern zunehmend von Konkurrenzdenken und Kosten-Nutzen-Überlegungen überlagert wird. Besonders in innovativen Branchen (z.B. Luft- und Raumfahrt), in denen die Forschungs- und Entwicklungskosten einen bedeutenden Teil einnehmen, kann ein Wettbewerbsvorteil erreicht werden, wenn man die Produktentwicklungen aus den Forschungsabteilungen der Konkurrenz erhält. Dieser „Know-How-Abfluss“ schwächt massiv die Volkswirtschaft mit allen daraus resultierenden Folgen. Die F&E-Ergebnisse machen das wirtschaftliche Herzstück des Unternehmens aus und durch Wirtschaftsspionage wird das Wissen in oft solcher Konzentration abgezogen, dass die Existenz des betroffenen Unternehmens erheblich beeinträchtigt oder gar zerstört wird (Kragler (1987), S.5). Es ist noch nicht die notwendige Sensibilität vorhanden, sich mit dieser Thematik auseinanderzusetzen, weder von Seiten der Unternehmen noch von Seiten der Behörden. Am 9. November 1993 wurde ein erster Schritt getan. Die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) wurde gegründet. Dieses Zentralorgan der Wirtschaft in Sicherheitsfragen, hauptsächlich finanziert durch den Deutschen Industrie- und Handelstag

(DIHT), hat die Aufgabe, Sicherheitsbelange der gewerblichen Wirtschaft gegenüber Politik und Verwaltung zu vertreten. Auch soll die Zusammenarbeit zwischen Staat und Wirtschaft vertieft werden. Die Einrichtung dieser Arbeitsgemeinschaft ist ein erster Schritt in die richtige Richtung. Ein wesentlicher Teil der Spionagetätigkeiten geht von sogenannten befreundeten Staaten aus. Im Verfassungsschutzbericht des Landes Baden-Württemberg aus dem Jahre 1998 wird allerdings erwähnt, dass die Aktivitäten westlicher Industriestaaten gegenüber Deutschland zwar im Mittelpunkt des öffentlichen Interesses stehen, jedoch keine gesicherten Erkenntnisse darüber vorliegen (Innenministerium Baden-Württemberg (1999), S.236). Auch die Tatsache, dass in den Jahren 1989 bis 1997 gerade in sieben Fällen wegen geheimdienstlicher Agententätigkeit nach § 99 Strafgesetzbuch (StGB) ermittelt wurde, zeigt dass die Bemühungen zur Bekämpfung noch nicht ausreichend sind. Fakt jedoch ist, dass das Geschäft mit der Wirtschaftsspionage boomt, da sich zu Zeiten des Kalten Krieges viele Agenten neue Betätigungsfelder gesucht haben. Der scharfe internationale Wettbewerb fördert zudem ihr Geschäft (o.V. (1999a), S.32). Weiterhin wird es Spionage gegen Armeen geben. Im März 1999 war zu lesen, dass der Datenverkehr der Deutschen Bundeswehr bald von US-Geheimdiensten mitgelesen werden kann. Die Bundeswehrverwaltung wird gerade mit der Netzwerk-Software Lotus-Notes ausgestattet. Lotus-Hersteller IBM hat sich als Mitglied der Key Recovery Alliance verpflichtet, den US-Sicherheitsbehörden den Zugriff auf den Klartext verschlüsselter Daten zu ermöglichen (o.V. (1999b), S.16).

Zunächst erfolgt eine Nennung der Definitionen und eine Begriffsabgrenzung, um eine Grundlage für das Gesamtverständnis zu schaffen. Um eine einheitliche Begrifflichkeit zu gewährleisten, werde ich eine Übersicht über die angewandten Instrumente und Methoden

erstellen. Anschliessend wird im dritten Kapitel die Problematik anhand des Beispiels der Gesellschaft „ENERCON“ verdeutlicht. Den Abschluss bildet ein Fazit mit einem Ausblick für die mögliche weitere Entwicklung der Wirtschaftsspionage. Allgemein gesprochen, möchte ich mich im Rahmen meiner Seminararbeit eingehender mit dieser Situation der gegenseitigen Auskundschaftung beschäftigen, um die Brisanz der Sachlage zu verdeutlichen. Die nötige Sensibilität innerhalb der Unternehmen ist grösstenteils noch nicht vorhanden, obwohl Sicherheit ein Grundbedürfnis der Menschheit ist.

2. Grundlagen der Wirtschaftsspionage

Hier werden die theoretischen Hintergründe erarbeitet, damit im folgenden „in der gleichen Sprache“ gesprochen werden kann. Es wird eine Definition erarbeitet, um die Vielfältigkeit und Vielschichtigkeit der Definitionsversuche in der Literatur darzulegen. Im zweiten Kapitel werden einzelne Instrumente und Methoden der Wirtschaftsspionage beschrieben und gleichzeitig gezeigt, in welchen Anwendungsbereichen diese schwerpunktmässig zum Einsatz kommen.

2.1 Definitionen und Begriffsabgrenzung

Der Begriff „Spionage“ ist sehr vielschichtig, komplex und wird in der öffentlichen Diskussion häufig von irreführenden Vorstellungen geprägt. Eine einheitliche begriffliche Definition gibt es nicht (Schurgers (2000), S. 1). Als Spionage wird das Auskundschaften von Informationen mit Schwerpunkten aus den Bereichen Politik, Militär und Wirtschaft mit Mitteln der geheimen Nachrichtenbeschaffung verstanden. Besondere Beachtung wird dabei auf jegliche als Geheimnisse besonders geschützte Information gelegt. Ziel der Spionage ist es, durch kostenloses technischen Know-How und durch Wissen über die Angebote der Wettbewerber oder deren Marketingstrategien, dem eigenen Unternehmen respektive der eigenen Volkswirtschaft entscheidende Vorteile zu verschaffen. In den Gesetzen des Strafrechts und des Verfassungsschutzes wird der Begriff Spionage nicht gebraucht. Hier finden sich Bezeichnungen wie geheimdienstliche Agententätigkeit oder geheimdienstliche Tätigkeiten für ein fremde Macht. (Bundesamt für Verfassungsschutz (2000), S.1)

Wirtschaftsgeheimnisse, also Betriebs- und Geschäftsgeheimnisse liegen vor, wenn Tatsachen im Zusammenhang mit einem Geschäftsbericht, die nur einem eng begrenzten Personenkreis bekannt und nicht offenkundig sind, nach dem Willen des Arbeitgebers aufgrund eines berechtigten

wirtschaftlichen Interesses geheimgehalten werden sollen (Kragler (1987), S.29). Im Bereich der Wirtschaftsspionage muss unterschieden werden zwischen der Konkurrenzspionage bzw. Industriespionage, also der Spionage der im Wettbewerb stehenden Unternehmen untereinander, wobei dies durch nicht-staatliche Einrichtungen geschieht, und der Wirtschaftsspionage, die von staatlichen Geheimdiensten durch fremde Nationen betrieben und gesteuert wird. Die Unterscheidung ist von Bedeutung, da nur für letztere die Bundes- und Landesämter für Verfassungsschutz nach den einschlägigen gesetzlichen Bestimmungen zuständig sind. Diese können bereits im Vorfeld systematisch beobachten und ausleuchten und somit auch rechtzeitig durch darauf aufbauende Präventivmassnahmen die Spionageangriffe wirksam bekämpfen. Die Strafverfolgung gestaltet sich gemäss §§ 94 StGB und gilt als geheimdienstliche Agententätigkeit. Im Falle der Konkurrenzspionage kann diese durch die Sicherheitsbehörden weniger präventiv, sondern überwiegend repressiv bekämpft werden. Der Verrat von Geschäfts- oder Betriebsgeheimnissen ist ein Verstoß gegen §§ 17 Gesetz gegen den unlauteren Wettbewerb (UWG). Eine Unterscheidung ist demzufolge recht einfach zu bestimmen, zumal beide Möglichkeiten zur Informationsgewinnung von grundsätzlich unterschiedlichen Voraussetzungen ausgehen, verschiedene Zielsetzungen haben und teilweise andere Methoden einsetzen (Schurgers (2000), S.1).

Die Schwerpunkte der Spionage fremder Nachrichtendienste aus der Zeit des Kalten Krieges „Militär“ und „Politik“ verlieren im Verhältnis zur Wirtschaftsspionage immer mehr an Bedeutung. Der Anteil der von ausländischen Nachrichtendiensten gelenkten technologisch-wirtschaftlich orientierten Spionage von Unternehmen nimmt im Vergleich zur militärischen und politischen Informationsgewinnung permanent zu. Sie macht mittlerweile etwa zwei Drittel der nachrichtendienstlichen Spionage aus. Dies ist zum einen auf die Veränderung der politischen Verhältnisse

innerhalb Europas, zum anderen aber auf den immer härter werdenden globalen Konkurrenzkampf zurückzuführen.

2.2 Übersicht über die Tätigkeiten, Instrumente und Methoden der Wirtschaftsspionage

In diesem Gliederungspunkt wird eine Übersicht die Instrumente darstellen, die im Bereich der Wirtschaftsspionage zum Einsatz kommen. Zudem wird schematisch auf die Methoden und Vorgehensweisen eingegangen. Die notwendige Unterscheidung in Konkurrenz- und Wirtschaftsspionage ist in diesem Gliederungspunkt nur insofern von Bedeutung, als dass ausländische Geheimdienste weiterhin nur im Bereich der Wirtschaftsspionage tätig sind. Ansonsten ist ein unterschiedlicher Einsatz in diesen zwei Bereichen nicht zu erkennen, da grundsätzlich sowohl die Wirtschafts- als auch die Konkurrenzspionage diese im Folgenden beschriebenen Mittel zum Einsatz bringen. Die Aufklärungsziele gegnerischer Nachrichtendienste umfassen die gesamte Bandbreite der Wirtschaft. Das Hauptinteresse liegt dabei insbesondere in den wettbewerbsintensiven High-Tech-Bereichen:

- Luftfahrt-, Rüstungstechnik, Navigation, zivile und militärische Nutzung der Kernspaltung, Telekommunikation und Pharmazie,
- Biotechnologie und Medizin, wie angewandte Molekularbiologie,
- Energie- und Umwelttechnik wie Filtertechnik, Emissionskontrolle,
- Information und Kommunikation, Software, Mikro- und Optoelektronik, Hochleistungsrechner und -netzwerke,
- Hochdefinitions-Bildtechnik wie Sensor- und Signaltechnik. Datenspeicherung und Peripheriegeräte sowie Computersimulation,
- Materialtechnik, insbesondere Materialsynthese, elektronische

und photonische Materialien, Keramik, Verbundwerkstoffe, Hochleistungsmetalle und -legierungen und

- Produktion, hier flexible computergesteuerte Fertigung, Mikro- und Nanofabrikation und Systemmanagement-Technologien (Ulfkotte (1999), S.56).

In diesen Bereichen gilt grundsätzlich, dass sämtliche Informationen von Bedeutung sind. Dies unterscheidet die langfristig angelegte Wirtschaftsspionage von der eher prozess- und produktorientierten Industriespionage. Bei letzterer hat man es insbesondere auf folgende Information abgesehen:

- Preisinformationen,
- Unterlagen zu Produktionsverfahren und zur -technologie,
- Produkte,
- Markt- und Absatzstrategien,
- Angaben über Hersteller,
- Lieferanten und Kunden sowie
- Verträge, Kalkulationen und
- Personallisten (Schurgers (2000), S.3).

Einen immer bedeutenderen Platz unter den verschiedenen Möglichkeiten an Informationen zu kommen, ist der Einsatz von Computer. In der Medienberichterstattung finden computergestützte Angriffe gegen Unternehmen („Hacking“) grosse Beachtung. Die Möglichkeiten der modernen Technologie haben dem versierten Angreifer hier bisher ungeahnte Wege eröffnet (Schurgers (2000), S.4).

Betriebsgeheimnisse können auch ohne die körperliche Anwesenheit eines Spions in der Firma in Erfahrung gebracht werden. Die moderne Kommunikationstechnik macht es möglich, dass beispielsweise ISDN -

Telekommunikationsanlagen (Integrated services digital network) von aussen so manipuliert werden können, dass ein unbemerktes Mithören von Gesprächen stattfinden kann. Auch ist man in der Lage, sich in Telefon- und Faxleitungen einzuklinken und die Abstrahlung normaler Computer auch ausserhalb des Gebäudes aufzufangen und in „Schriftform“ umzusetzen. Generell wird die Problematik der Telekommunikation zu sehr unterschätzt. Vor allem die drahtlose Kommunikation ist einfacher abzuhören, also man sich eigentlich bewusst ist (o.V. (1997), S.2).

Neben dem „Mithören“ von Informationen, z.B. während sie zwischen Geschäftspartner oder ortsverschiedenen Unternehmensbereichen ausgetauscht werden, ist auch ein Eindringen in firmenintern gespeicherte sensible Informationen möglich. Selbst sogenannte „Firewalls“, welche dazu dienen das eigene Netz vor externen Angriffen zu schützen, bieten keinen absoluten Schutz.

Grundsätzlich kommen alle traditionellen nachrichtendienstlichen Mittel der Aufklärung zum Einsatz:

- Auswertung offener Quellen,
- Gesprächsaufklärung,
- Werbung von sogenannten „Innenquellen“,
- Gründung von Schein- und Tarnunternehmen,
- Einschleusung von Agenten in das Zielunternehmen,
- Gründung von Joint Ventures,
- Technische Aufklärung und
- Computerspionage (Schurgers (2000), S.4).

Weitestgehend unbeachtet bleibt demgegenüber die verwundbarste Stelle eines Unternehmens. Der „einzelne Mitarbeiter“ verfügt über vielfältige

unternehmensinterne Kenntnisse und ist daher ein besonders begehrtes Objekt für Wirtschafts- und Industriespione. Warum sollte man den aufwendigen und mitunter riskanten Weg eines technischen Eindringversuchs unternehmen, wenn ein gut vorbereitetes Gespräch mit einem unbedarften Mitarbeiter des Zielunternehmens nicht nur konkretere Daten, sondern auch noch die entsprechende Bewertung dieser Fakten liefert?

Zudem ist ein solches Vorgehen in den meisten Fällen noch nicht einmal strafrechtlich zu verfolgen. Im Bereich der Wirtschaftsspionage spielen die Geheimdienste der Länder eine entscheidende Rolle. Diese sind teilweise angewiesen, den eigenen inländischen Unternehmen durch gezielte Informationsgewinnung zu Wettbewerbsvorteilen zu verhelfen. Die Tätigkeiten des amerikanischen Geheimdienstes umriss der Central Intelligence Agency (CIA)-Chef Gates 1992. Es sollten Analysen der globalen wirtschaftlichen Entwicklung und der Positionen anderer Länder bei internationalen Verhandlungen erfolgen. So sollten Untersuchungen bezüglich wettbewerbsbeeinträchtigender Massnahmen von Konkurrenten US-amerikanischer Firmen, beispielsweise Subventionen, Exportförderungen, Vertragsabsprachen und Schmiergeldzahlungen durchgeführt werden. Zudem stand eine Überwachung technologischer Entwicklungen an, die die nationale Sicherheit gefährden könnten. Ein wichtiger Bestandteil war auch die Gegenaufklärung, da laut Gates die Angriffe auf die US-Wirtschaft massiv verstärkt wurden (Förster (1997), S.75). Gerade auch im Bereich Spionageabwehr liegt ein wesentlicher Bestandteil, da es primär gilt, das Wissen im eigenen Land zu behalten. Und erst in den weiteren Überlegungen sollte man sich um die Beschaffung fremder Informationen aus dem Ausland bemühen.

Im Bereich Wirtschaftsspionage gibt es nicht nur die Möglichkeit, passiv Informationen abzugeben, sondern es ist ebenfalls möglich, aktiv anhand beeinflussender Massnahmen in die Abläufe des Zielobjektes

einzugreifen. Diesen Bereich nennt man Wirtschaftskrieg. Die dort zur Anwendung kommenden Methoden werden als „Dirty Tricks“ bezeichnet (Schmidt-Eenboom/Angerer (1994), S.169).

3. Schematische Darstellung und Folgen der Wirtschaftsspionage am Beispiel der Gesellschaft „ENERCON“

Im folgenden Kapitel wird auf den Fall von Wirtschaftsspionage am Beispiel der Gesellschaft „ENERCON“ eingegangen. Dieser verdeutlicht die Arbeitsweise von Geheimdiensten, lässt die fehlende Sensibilität gerade von mittelständischen Unternehmen erkennen und zeigt die daraus resultierenden Folgen und Konsequenzen für ENERCON.

Aloys Wobben war Erfinder und besessen von der Vision mit einer eigenen Firma Umwelttechnologien zu verwirklichen. Zunächst einmal war er an der Entwicklung von Zukunftstechnologien wie dem Transrapid oder dem Windkraftanlagenbau an der Technischen Universität Braunschweig beschäftigt. Im Jahre 1984 konnte er einen eigenen Betrieb aufbauen, der sich zunächst auf Leistungselektronik wie dem Frequenzrichter konzentrierte. Nach einigen Erfolgen der ENERCON, die im ostfriesischen Aurich ansässig ist, wie die Belieferung von Mercedes-Benz mit Wechselrichtern für die Fließmontage, konzentrierte sich der Firmengründer auf die Umsetzung seiner Vision, dem Eigenbau des Prototyps einer Windenergieanlage. Da das junge Unternehmen auf diesem Gebiet einen großen Know-How-Vorsprung besaß und zudem die weltweite Nachfrage nach Windenergieanlage aufgrund des Ökologiewahns ein immer größeres Wachstum vollzog, konnte man im Jahre 1998 einen Umsatz von 525 Millionen Mark vorweisen. Das nun mittelständische Unternehmen ENERCON hat 1500 Beschäftigte und es sind bei einer Arbeitslosigkeit von über 20% im strukturschwachen Emsland 10000 Beschäftigte indirekt davon abhängig. 1984 startete das Unternehmen mit der Windkraftanlage E-16, die in der Lage war, 50 Kilowatt zu produzieren. Kurze Zeit darauf ging die E-17/18 in Serie. Die drehzahlvariable Anlage mit einem Rotordurchmesser von 17 Metern erzeugt noch heute einen nicht unwesentlichen Teil des Strombedarfs des Verwaltungsgebäudes. Es folgten weitere technische Neuerungen wie die

sogenannte Pitch-Regelung, ein Verstellmechanismus der Rotorblätter abhängig von der Windstärke. Trotz der im Jahre 1990 erreichten Marktführung gab sich das junge Unternehmen mit dem Stand der Technik nicht zufrieden. Nach achtjähriger Erfahrung mit Getriebemaschinen und zehn Millionen Deutsche Mark Entwicklungskosten startete ENERCON 1992 mit der E-40 (500 Kilowatt) den Bau der ersten getriebefreien Windmühle. Mit einem Verkauf von über 1650 Anlagen ist die E-40 die meistgebaute Windenergieanlage der 500 Kilowattklasse. Durch den großen Erfolg mit dieser neuartigen Technik war man in der Lage, neue Produktionsstätten zu errichten. Mittlerweile besitzt man mit Produktionsstandorten in Deutschland, Indien und Brasilien die weltweit größte Kapazität für Windenergieanlagen. Durch das feinmaschige Vertriebsnetz von Österreich bis Japan konnte der Export-Anteil auf über 20% ausgedehnt werden. Auch technisch hat man sich mit der aktuellen Version E-66, die 1500 Kilowatt leisten kann, einen sehr guten Namen gemacht (Ulfkotte (1999), S.22).

Solch ein wirtschaftlicher Erfolg sorgt aber auch dafür, dass Konkurrenten aus der gleichen Branche versuchen, an Unterlagen zu gelangen, um das Produkt des Marktführers imitieren zu können. Das mittelständische Unternehmen ENERCON konnte sich jedoch nicht vorstellen einmal selbst Opfer einer gezielten Spionageaktion zu werden. Heute ist man sich sicher, dass zumindest der Konkurrent Kenetech Windpower aus den USA seit Ende der achtziger Jahre sämtliche Besprechungen und Telefongespräche abgehört und Faxe sowie E-Mails abgefangen hat. Nur so ist es zu erklären, dass die Firma Kenetech Windpower am 01.02.1991 beim U.S. Patent Office eine Patentanmeldung mit 138 Ansprüchen einreicht, deren Schwerpunkt sich auf drehzahlvariable Windenergieanlagen erstrecken soll. Dieser Typ Windkraftanlage mit 300 Kilowatt Leistung wurde im fernen Emsland bereits gebaut. Es wurde nach erfolgter Entwicklung der Anlage schlicht versäumt, das Patent für die eigene

Entwicklung zu sichern. Die Fachzeitschrift „Windpower Monthly“ beschreibt die Anmeldung sechs Jahre später wie folgt. „Dies sei so, als ob man heute versuche, ein Kraftfahrzeug mit Diesel oder Ottomotor zum Gegenstand einer Patentanmeldung zu machen“ (o.V. (1999a), S.32).

Im Jahre 1993, als ENERCON mit der Serienproduktion der E-40 begann, beschloss Kenetech Windpower das neueste Produkt der Auricher Gesellschaft genau zu betrachten. An der Aktion beteiligt waren der nach ENERCON-Angaben in der Branche einschlägig bekannte norddeutsche Techniker Ubbo de Witt, ehemaliger Mitarbeiter des Wilhelmshavener Deutschen Windenergie-Instituts (DEWI), die amerikanische Kenetech-Angestellte Ruth Heffernan und der niederländische Kenetech-Repräsentant Robert Jans. Über de Witt wurde ermittelt, dass er von mehreren Unternehmungen Zuwendungen als Gegenleistung für Informationen erhielt. Diese Person fungierte zudem bei dieser Spionageaktion als Bindeglied zwischen dem amerikanischen Unternehmen und dem Vorsitzenden des Bundesverbandes Windenergie e.V. Peter Ahmels. Dieser hatte auf seinem Grundstück die neue E-40 von ENERCON installiert. Ahmels gestattete den Kenetech-Mitarbeitern im März 1993 nur aufgrund seines persönlichen Verhältnis zu Herrn de Witt Zugang. Ihm wurde gesagt, zwei potentielle Kunden wollten die Anlage besichtigen. Den drei Spionen kam zu Gute, dass der Landwirt zur Zeit der Besichtigung selbst nicht anwesend sein konnte und den Schlüssel hinterlegte. Der von Heffernan am 21. März 1994 angefertigte Bericht ist ein einzigartiges Dokument der Dreistigkeit amerikanischer Spionage auf deutschem Boden (Ulfkotte (1999), S.29).

Vor Besteigen des Turms wurde das Häuschen unten am Turm geöffnet, wo sich der untere Schaltschrank befindet. Dort wurden Fotos von den leistungselektronischen Umrichterplatinen gemacht. Nach Eingriffen in das Sicherheitssystem wurde die Turbine abgestellt und der Turm von Heffernan und de Witt mittels Leiter bestiegen. Während des einstündigen

Aufenthalts in 42 Meter Höhe wurden Fotos gemacht in den nahezu unzugänglichen Bereichen der Windenergieanlage. Nach längerer Unterhaltung über die Technik mit dem Physiker und Meteorologen de Witt, erschien der Landwirt. Es wurde im Anschluss noch etwa 45 Minuten mit dem Landwirt über seine Erfahrungen und Eindrücke gesprochen. In dem etwa zehneitigen Bericht über diesen Besuch wurden sämtliche technischen Bereiche mit einem separaten Kapitel bedacht, was auf die genaue und detaillierte Arbeit der drei Spione hinweist. So wurde der Generator, die Leistungselektronik und die Rotorblätter näher untersucht, wobei die Blindleistungskompensation fotografisch festgehalten wurde. Genauso untersucht wurden auch Azimutantrieb, Blattverstellung samt Blattverstellsystem und Elektronik, Schleifringe, Akustik, Turbinenwindmessung, die Konstruktion des Turms, die tragende Struktur sowie das Fundament. Zusätzlich enthalten im Bericht war die exakte Leistungskurve und ausführliche Bemerkungen zum Standort und Kommentare des Eigentümers. Hier lässt sich klar die Professionalität der Durchführenden erkennen, wobei bis heute die Herkunft des Insiderwissens nicht gänzlich geklärt werden konnte.

Dass der Besuch der amerikanischen Kenetech-Abordnung Erfolg hatte und das neu hinzu gewonnene Wissen auch umgesetzt werden konnte, zeigte die Patentverletzungsklage des U.S. District Court in San Jose, die der Geschäftsleitung der ENERCON GmbH im Januar 1995 zuzuging. Zudem folgte drei Monate später eine Klage vor der International Trade Commission (ITC) in Washington D.C.. Beide Verfahren wurden von der Kenetech Windpower angestrengt, die mittlerweile Inhaberin der Patente geworden ist. Da der Geschäftsführer und Firmengründer Wobben nichts von dem Eindringen der National Security Agency (NSA) in das Telefonnetz ahnte und sich auch nicht bewusst war, dass eine Abordnung genau dieses Konkurrenzunternehmens seine Anlage im März 1994 inspizierte, ging er von einer Verwechslung aus. Dass sich dies als

Trugschluss erweisen sollte, zeigten die Gerichtstermine in den USA. Nach Auffassung des Geschäftsführers Wobben ging es hierbei nicht um die Feststellung der Rechte an dieser Technologie, sondern lediglich um die Verdrängung eines potenziellen Importeurs. Es wurden Fotos gezeigt, die während des Besuchs der Spione in Aurich gemacht wurden. Dem Verdachtsmoment der Industriespionage wurde aber im weiteren Verlauf der Verhandlungen nicht nachgegangen. Nie kam zur Sprache, dass sich Kenetech das patentieren liess, was ENERCON bereits viele Jahre herstellte. Auch der besagte Artikel der Zeitschrift „Windpower Monthly“ kam nicht zur Sprache. Während die Klägerin den Patentverletzungsstreit in Kalifornien nur sehr zögerlich betrieb, kam es vor der ITC in Washington D.C. zu einer ersten Beweisaufnahme. Die ITC, die dem U.S.-Handelsministerium unterstellt ist und als Verwaltungsbehörde mit gerichtsähnlicher Kompetenz agiert, lässt den Geschäftsführer der ENERCON GmbH zwei Wochen lang fast täglich von den Anwälten der Gegenseite verhören. Es wurden alle Mittel ausgeschöpft, die der „Tariff Act 1930“ zulässt.

Im Laufe des Verfahrens kommt es zu einer unbeabsichtigten Verfahrenspanne. Die ITC hebt einen Geheimhaltungsbeschluss auf, der Teile des gegnerischen Aktenmaterials betraf. Somit konnte erstmals Beweismaterial über die von Kenetech erfolgte Wirtschaftsspionage eingesehen werden. Daraufhin entschliesst sich die Geschäftsleitung der ENERCON Strafantrag wegen Vergehens nach den §§ 17 UWG zu stellen. Erst nach Bemühungen, den Informant in Mitarbeiterkreisen zu finden, kommt es zu Durchsuchungen der Geschäfts- und Wohnräume des Ingenieurs de Witt. Jedoch rückt der Abschluss des Verfahrens, trotz der wegen der einzigartigen Dokumentation der Vorgänge eigentlich eindeutigen Situation in immer weitere Ferne. Zuletzt interessierte sich der Staatsanwalt in einem Schreiben an ENERCON-Justitiar Knottnerus-Meyer vor allem dafür, ob ENERCON nicht Schwachstellen im eigenen

Sicherheitskonzept gehabt habe. Man vermutete, dass Aufträge zur Prüfung und Messung an externe Institute erteilt worden sind und darüber Messprotokolle und Prüfberichte bereits einige Zeit früher öffentlich gemacht wurden. Knottnerus-Meyer erwiderte, dass sämtliche Forschungsunterlagen, die von externen Instituten erstellt worden sind, zum Zeitpunkt des Verfahrens nicht öffentlich waren. Im Sommer 1996 äußert die ITC erstmalig die Ansicht, es bestehe die Gefahr einer Patentverletzungsklage und stellte einen Verstoß gegen §337 Tariff Act 1930 fest. Daraufhin wird ein generelles Importverbot verhängt, welches ENERCON bis zum Jahre 2010 untersagt, Anlagen in die USA zu exportieren. Diese Entscheidung erregt großes Aufsehen und ruft die politischen Kräfte auf den Plan. In persönlichen Treffen bat man den damaligen Ministerpräsident von Niedersachsen Gerhard Schröder um seine Unterstützung. Nach Meinung Wobbens scheint aber nie etwas seitens des Ministerpräsidenten getan worden zu sein, da eine derartige Spionageattacke des westlichen Bruders nach Ansicht des Politikers unmöglich schien. Die EU-Kommission schließt sich mit einer offiziellen Protestnote dem Protest des Bundeswirtschaftsministeriums an. Es wird zum Ausdruck gebracht, dass die U.S.-Regierung entgegen den Vorschriften des Welthandelsabkommens „General Agreement on Tariffs and Trade“ (GATT) handelt, indem sie Inländern ein doppeltes Forum im Vorgehen gegen ausländische Wettbewerber eröffne. Diese müssen sich nicht nur, wie international üblich, vor den ordentlichen Gerichten verteidigen, sondern sehen sich parallel noch einer Institution wie der ITC gegenüber. Trotz der massiven Kampagne machte der U.S.-Präsident von seinem befristeten Einspruchsrecht, das am 04.11.1996 endete, keinen Gebrauch. Nach Aussage des Justitiar Knottnerus-Meyer verhält hierbei jedes rechtlich und sachlich vorgetragene Argument ungehört in der letzten Phase des Präsidentschaftswahlkampfes. Letztlich ist die Berufung gegen die ITC-Entscheidung zurückgewiesen worden ebenso wie der

Antrag auf Zulassung der Revision. Somit scheint die Aussage der ASW in einer Sonderinformation vom März 1996 zuzutreffen. „Die amerikanische Konkurrenz will offenbar mit allen Mitteln verhindern, dass sich ENERCON in den USA etablieren kann...Die ITC ist...eine Art Verwaltungsgericht, das Importe von ausländische Firmen kontrolliert, um den landeseigenen Firmen den Rücken zu stärken...Die ITC ist eine Einrichtung, die den landeseigenen Unternehmen sogar die Spionage erleichtert.“ Nach Ansicht des Geschäftsführers Wobben, muss seine Firma ENERCON GmbH aufgrund des allzu sorglosen Umgangs mit vertraulichen Betriebsinformationen auf Umsätze in Höhe von etwa 100 Millionen Mark und 300 neue Arbeitsplätze verzichten. Darin sind noch keine nicht realisierten Umsätze aus dem entgangenen Export in die USA enthalten. Das langwierige Gerichtsverfahren in den Vereinigten Staaten verschlang eine Summe von 2 Millionen US-\$. Anders als das deutsche Prozessrecht kennt das US-amerikanische Verfahrensrecht keine Kostenentscheidung. Unabhängig vom Ausgang des jeweiligen Verfahrens hat jede Partei ihre eigenen Kosten zu tragen. Der Aussage des ENERCON-Justitiar zu Folge, scheint die Vorgehensweise des US-amerikanischen Wettbewerbers intensiv und langfristig vorbereitet worden zu sein. Bereits die Anmeldung des streitgegenständlichen Patents wurde auf bewährter Technik der ENERCON GmbH aufgebaut. Auch die Antrags- und Klageschriften wären ohne die im März 1994 gewonnen Kenntnisse zu wohl unsubstantiiert gewesen. Bemerkenswert ist seiner Meinung nach vor allem, dass das rechtswidrig erlangte Know-How keineswegs in die eigene Entwicklung geflossen ist, sondern für ein „rechtsstaatliches“ Verfahren Verwendung fand. Der Patentstreit konnte vor den ordentlichen Gerichten nicht geklärt werden. Dies hätte ansonsten auch zu einer Aufhebung der ITC-Entscheidung geführt. Das Gerichtsverfahren in Kalifornien wurde ohne Möglichkeit der Wiederaufnahme eingestellt, so dass bis heute nur eine summarische Prüfung der rechtlich relevanten Fragen nach dem

„Tariff Act 1930“ stattgefunden hat. Welchen politischen Geist diese gesetzlichen Vorschriften verkörpern, lässt sich nicht zuletzt aus dem Entstehungsjahr herleiten. Dieses protektionistische Instrument wurde bereits mehrfach ohne Erfolg von der EU-Kommission gerügt, da es mit dem Welthandelsabkommen GATT unvereinbar ist (Knottnerus-Meyer, (1999), Kapitel 9).

Nur der soliden wirtschaftlichen Situation der Unternehmung ist es zu verdanken, dass die ENERCON sich überhaupt am Markt halten kann.

4. Fazit

Gerade auch in Deutschland sind unterschiedliche Auffassungen gegenwärtig, was den Einsatz des Geheimdienstes für die eigene Wirtschaft erschwert. Wirtschaftsspionage ist „...weder ein Kavaliersdelikt, noch umgibt sie ein Flair von Abenteuerertum, wie uns manche Zeitgenossen glauben machen wollen. Vielmehr verursacht sie Jahr für Jahr erhebliche Vermögensschäden...zu Lasten unserer Volkswirtschaft“ (Ulfkotte (1999), S.48). Gerade bei ENERCON konnte man gut erkennen, dass von einer wenige Minuten andauernde „Bespitzelung“ die gesamte Zukunft der Unternehmung in Gefahr sein kann. Durch die fehlende Möglichkeit, in die USA zu exportieren, konnte der Betrieb nicht weiter in dem Maße expandieren. Auch schliessen sich Konkurrenzunternehmen im Zuge der weltweiten Fusionen sehr rasch zu größeren Unternehmen zusammen und können somit die Marktführerschaft übernehmen. Gerade auch an diesem Fall kann man gut erkennen, dass in manchen Ländern die Sensibilität zum Schutze der eigenen Unternehmen vorhanden ist. So konnte das Exportverbot für die Firma ENERCON in die USA nur wegen der unzureichenden Verfahren aufrechterhalten werden. Wie bereits im Text angedeutet, vermutet man hier eine gewisse Absicht bei den amerikanischen Institutionen zum Schutze der eigenen Wirtschaftsmacht. Auch beschloss man am 11.10.1996 mit dem „Economic Espionage Act“ ein härteres Gesetz gegen die Ausspähung von Firmen. Nun drohen Spione, die im Auftrag eines anderen Landes oder einer ausländischen Unternehmung arbeiten bis zu 25 Jahren Gefängnis und einer Viertelmillion Dollar Geldstrafe. In den USA hat sich in den vergangenen zehn Jahren eine eigenständige Disziplin entwickelt, die das gewinnen kritischer Unternehmensinformationen zum Gegenstand hat. Unter dem Schlagwort „Business Intelligence“ sind in erster Linie Personen aktiv, die ihr Handwerk beim Militär und im Geheimdienst gelernt haben. Auch bei unseren französischen Nachbar zeichnen sich ähnliche Entwicklungen ab.

Unter der Führung des ehemaligen Leiters des Auslandgeheimdienstes wurde 1997 in Paris die „Ecole de Guerre Economique“ gegründet (Schurgers (2000), S.5). Daraus ist eigentlich klar zu ersehen, dass sich einige Länder auf einen sich immer mehr verschärfenden Wirtschaftskrieg vorbereiten. In Deutschland ist die Situation etwas komplexer gelagert. Der Verfassungsschutz sammelt und wertet Informationen über geheimdienstliche Tätigkeiten fremder Mächte aus. Die Konkurrenzspionage darf ihn nicht interessieren. Der Staat nimmt und darf aus Rechtsgründen keinen unmittelbaren Einfluss darauf nehmen, welche Maßnahmen die Unternehmen zur Spionage ergreifen, auch wenn Spionage zu volkswirtschaftlichen Schäden führt und sogar Arbeitsplätze gefährdet. Man sollte sich hier der Frage nicht verschließen, ob das Verhältnis zwischen Staat und Wirtschaft in Deutschland auf dem Gebiet der Spionageabwehr so gestaltet ist, dass es gegen die professionelle Zusammenarbeit von Wirtschaft und staatliche Stellen in anderen Ländern den eigenen Unternehmen große Nachteile bereitet. Die Qualität der eigenen Geheimdienste scheint die einschlägige Literatur nicht in Frage zu stellen.

So ließt man über den Bundesnachrichtendienst (BND), dass man es hier mit einem fähigen, effizienten Nachrichtendienst mit engagierten und tüchtigen Mitarbeitern zu tun hat. Auch kann man erfahren, dass bereits seit Mitte der sechziger Jahre, die Geheimdienste besonders aktiv im Bereich der Wirtschaftsspionage sind. Der BND hat Verbindungsleute beauftragt, Forschungseinrichtungen und Firmen in den USA, Frankreich, Großbritannien und Italien auszuspionieren. Durch elektronische Abhöreinrichtungen ist man in der Lage, die Telekommunikation internationaler Unternehmen zu überwachen. Vor allem auch in den USA ist der BND aktiv (Schweizer (1993), S.208). An der fehlenden Kompetenz dürfte es den deutschen Institutionen im sogenannten zweitältesten Gewerbe der Welt wohl nicht fehlen (Eltgen (1995), S.7). Die Schwierigkeit

scheint in der Kommunikation dieser Einrichtungen und der Wirtschaft zu liegen. Man kann sich natürlich grundsätzlich die Frage stellen, ob denn ein Ausspionieren der eigenen Verbündeten und Freunden notwendig und richtig ist. Dass es zumindest gängige Praxis ist, zeigt uns eindrucksvoll die USA durch ihr weltweites ECHOLON-System (Netz von Abhöreinrichtungen), mit dem sie in der Lage sind, fast die gesamte Welt zu überwachen. Und der Fall „ENERCON“ belegt, dass eine solche verbesserte Zusammenarbeit auch notwendig ist, um den Wirtschaftsstandort Deutschland auch weiterhin erfolgreich am Leben zu erhalten.

Grundsätzlich fehlt meiner Meinung nach die notwendige Sensibilität, mit der man dem ungewollten Abzug von jeglicher Information begegnen muss. Hier liegt es an den einzelnen Unternehmungen, das Bewusstsein im eigenen Management und gerade auch bei den einzelnen Mitarbeitern zu schärfen. Eine Umfrage der KPMG Deutsche Treuhand-Gesellschaft unter den 1000 grössten deutschen Unternehmen ergab, dass mehr als zwei Drittel der Manager theoretisch das Problem der Wirtschaftsspionage kennen. Doch die meisten übertragen dieses Bewusstsein nicht auf die eigene Unternehmung (Ulfkotte (1999), S.47). Zuerst gilt es präventiv den Abzug von Wissen aus dem eigenen Land zu verhindern und im nächsten Schritt muss eine konsequentere Zusammenarbeit zwischen Wirtschaft und Staat erfolgen, um sich nicht gänzlich den dreisten Methoden der ausländischen „Konkurrenten“ ergeben zu müssen.

„Die russischen Geheimdienste sollen Wirtschaftsspionage betreiben, um den technologischen Rückstand zum Westen aufzuholen.“

Boris Jelzin

Literaturverzeichnis

Eltgen, Hans (1995),

Ohne Chance, Erinnerungen eines HVA-Offiziers, Berlin 1995

Förster, Andreas (1997),

Maulwürfe in Nadelstreifen, Wirtschaftsspionage - Der neue Job der Geheimdienste, Berlin 1997

Knotnerus-Meyer, Stephan (1999),

Kapitel 9 - Das mittelständische Unternehmen als Ausspähungsobjekt: die ENERCON GmbH, Symposium Spionageabwehr- Ein Beitrag zur Sicherung des Technologiestandortes Baden-Württemberg am 21.Juni 1999 in Stuttgart,

Kragler, Peter (1987),

Schutz des geheimen Know-How - Rechtliche Grundlagen und Massnahmenkatalog, Landsberg/Lech 1987

Innenministerium Baden-Württemberg (2000),

Landesamt für Verfassungsschutz Baden-Württemberg: Verfassungsschutzbericht 1998, Stuttgart 1998

o.V., (1997),

Technische Spionageangriffe auf die deutsche Wirtschaft, Sicherheit und Management, 6/97, S.2

o.V., (1999a),

Märkte und Chancen, Wirtschaftsspionage, DM, Nr.7, Juli 1999, S.32-34)

o.V., (1999b),

com!online März 1999, S.16

Schmidt-Eenboom, Erich; Angerer, Jo (1994),

Die schmutzigen Geschäfte der Wirtschaftsspione, Düsseldorf, et al. 1994

Schurgers, Frank (2000),

Wirtschafts- und Industriespionage in Deutschland, Online AVL: URL:
<http://www.krisennavigator.de/a-ne-sp.htm> (26.01.2000)

Schweizer, Peter (1993),

Diebstahl bei Freunden, Wie die Geheimdienste der Japaner und Deutschen die US-Wirtschaft ausspionieren, Hamburg 1993

Ulfkotte, Udo (1999),

Marktplatz der Diebe - Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert, München 1999