Simon Kirsch

Informationsschutz im Unternehmen

Prävention von Wissensabfluss
und die Erkennung von Innentätern
anhand derer Verhaltensmerkmale

Dieser Druck ist eine überarbeitet Ausfertigung meiner Abschlussarbeit, welche ich im Rahmen des Studienganges

„M.A. Kriminologie und Polizeiwissenschaften“

an der Ruhr-Universität Bochum absolviert habe. Mein Dank gilt dem gesamten Lehrstuhl für den gut strukturierten und organisierten Ablauf der Studienzeit.

Ebenfalls bedanke ich mich bei den Betreuern meiner Thesis,

Herrn Dipl. Oec. Bernd o. Bühler
und
Herr Dipl. Päd. Thomas A. Fischer.

„Der Nachrichtendienst muss seine Anstrengungen verstärken, um die russische Wirtschaft und die Interessen russischer Unternehmen im Ausland aktiver zu unterstützen.“

Vladimir Putin
Russischer Staatspräsident im Oktober 2007

„Selbstverständlich betreibt die DGSE Wirtschaftsspionage im Ausland, um damit staatlichen französischen Konzernen Vorteile zu verschaffen“

Claude Silberzahn
Ehemaliger Direktor des französischen Nachrichtendienstes DGSE

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

“Economics and war may serve different goals and obey different rules. But in both spheres one is confronted with the independent will of other parties.”

Jack Welch

Das Bestreben, sich einen Vorteil durch die Gewinnung von Erkenntnissen über seine Konkurrenten verschaffen zu wollen, ist so alt wie die Menschheit selbst.[3] Heutzutage werden diverse Einrichtungen und Behörden – als Nachrichtendienste bekannt – zur Informationsgewinnung, und zum Schutz des eigenen Wissens, von nahezu allen Staaten betrieben. Die dadurch erlangten Informationen werden unter anderem dafür genutzt, die eigene Regierung mit Informationen zu versorgen. Ein weiteres Ziel nachrichtendienstlicher Tätigkeiten mancher Staaten besteht darin, der Wirtschaft Informationen über die Entwicklungen ihrer Konkurrenten zu verschaffen.[4] Seit dem Fall des Eisernen Vorhangs[5] und dem Ende des Kalten Krieges[6] haben sich die Prioritäten der staatlich organisierten Informationsgewinnung verschoben.[7],[8],[9] Durch neue politische Abkommen zwischen den Staaten und die immer stärkeren wirtschaftlichen Auswirkungen der Globalisierung steigt der Wettbewerbsdruck zwischen Unternehmen im nationalen und internationalen Kontext.[10] Neben dem staatlich organisierten Informationsdiebstahl existiert ebenso die Industrie- und Konkurrenzspionage. Diese Art der Informationsgewinnung wird von den Wirtschaftsunternehmen selbst durchgeführt oder in Auftrag gegeben. Die durch Spionage in der Wirtschaft erworbenen Erkenntnisse müssen nicht immer aus dem Bereich neuer Entwicklungen durch Konkurrenzunternehmen stammen, sie

können beispielsweise ebenfalls Informationen über die Höhe einer Angebotsabgabe bei Ausschreibungen beinhalten.[11] Die unternehmerische Notwendigkeit, sich vor einem irregulären Informationsabfluss schützen zu müssen, liegt in der heutigen betriebswirtschaftlichen Wertigkeit von Informationen. Die Bedeutung eines Unternehmens ist von seinem Wissen und seinen Informationen abhängig. Im Rahmen des globalen Konkurrenzkampfes um Marktanteile sind Informationen mehr denn je als eine strategische Waffe zur Sicherstellung der Wettbewerbsfähigkeit zu sehen. Der betriebswirtschaftliche Regelfall in der Vergangenheit, dass sich die großen Unternehmen gegen kleinere behaupten können und diese dominieren, ist überholt. In der Gegenwart und auch zukünftig sind nicht selten Kleinstunternehmen führend und sorgen mit ihrem Dasein für empfindliche Marktverluste bei den eigentlichen Marktführern. Deren Erfolg liegt, neben der Gabe einer zügigen Adaption an erforderlichen Gegebenheiten, in deren Umgang, der Handhabung und dem Einsatz von Informationen. Informationen sind ein Strategiewerkzeug, welches in direkter Verbindung mit dem Erfolg eines Unternehmens steht. Demzufolge trägt der Informationsschutz als essentieller Baustein zum Unternehmenserfolg bei. Unzureichende, lückenhafte oder fehlerhafte Informationsschutzkonzepte können den Grundstein für Marktverluste oder den Niedergang eines Unternehmens bilden.[12]

Die Wirtschafts- bzw. Industriespionage ist eine Erscheinungsform der Wirtschaftskriminalität[13].[14] Wissenschaftliche Untersuchungen in diesem Teilbereich befinden sich, auch wenn der Beginn der wirtschaftskriminologischen Forschung mit Edwin H. Sutherland und seiner Definition des *White-Collar-Crime*[15] schon im Jahr 1939 stattfand, noch in ihren Anfängen.[16] Zur

erfolgreichen Reduzierung des Dunkelfeldes kommt erschwerend hinzu, dass Wirtschaftsunternehmen nur ungern bzw. selten solche Erkenntnisse anzeigen bzw. öffentlich machen. Solche Bekanntmachungen würden sicherlich Vertrauens- und erfolgsschädigende Konsequenzen für die betroffenen Unternehmen nach sich ziehen.[17] Resultierend aus diesen Tatsachen, besteht bei diesen Straftatbeständen ein unverhältnismäßig geringes und kaum repräsentatives Hellfeld. Die geschätzte Dunkelziffer sowie der durch Wirtschafts- und Industriespionage entstandene Schaden und die dadurch resultierenden Verluste für die deutsche Wirtschaft und die Regierung sind immens.[18] Diese Schädigungen haben weitreichende Konsequenzen, welche bis zu einer Schädigung der Gesamtgesellschaft reichen. Betrachtet man die bisher bekannten Vorgehensweisen der Wirtschafts- und Konkurrenzspionage näher, kann man diese durch die angewandte Methode der Informationsgewinnung einordnen. So ist heutzutage, im Zeitalter der Informationstechnologie, davon auszugehen, dass mit Hilfe elektronischer und IT-basierter Angriffe die meisten Versuche einer sogenannten Ausspähung – und gleichzeitig der größte Präventionsaufwand – unternommen werden.[19] Eine weitere Möglichkeit der Informationsabschöpfung ist die Einschleusung von Mitarbeitern in Konkurrenzunternehmen. Diese sollen gezielt Daten und Informationen gewinnen, welche dem bestohlenen Unternehmen schaden sowie dem Auftragsunternehmen einen Wettbewerbsvorteil verschaffen sollen.[20] Die dritte bekannte Möglichkeit, wie Unternehmensfremde gezielt an schützenswerte Informationen gelangen können, sind die in einem Unternehmen beschäftigten Mitarbeiter.[21] Vor allem diese sind als eine besondere Schwachstelle in der Wertschöpfungskette des Informationsschutzes anzusehen.[22] Diese Risikogruppe soll in dieser Arbeit im

Detail betrachtet werden. Weitere Möglichkeiten und Risikoquellen im Rahmen des Informationsschutzes können im Rahmen von Besuchern, auf Messen oder bei der Teilnahme an Gremien oder Tagungen auftreten. Die letzte Möglichkeit, mit welcher jede Spionageaktivität beginnt, ist die offene Beschaffung von Informationen.

Unternehmen mit zu geringer Sicherheits-Policy[23] geben häufig zu viele Informationen preis, welche sich für die Konkurrenten als sehr nützlich erweisen können.[24] So kann eine grundsätzliche Nachlässigkeit im Umgang mit Informationen in einem Unternehmen der Grund für einen erleichterten Know-how-Abfluss sein.[25] Ebenso besteht die Gefahr, durch unbedachte fahrlässige Handlungen und Aussagen Informationen unbewusst preisgeben. Eine solche leichtfertige Herausgabe von Wissen kann bei gesteigerter Unzufriedenheit des Arbeitnehmers und einer damit zusammenhängenden sinkenden Loyalität gegenüber seinem Arbeitgeber auch bewusst geschehen. Weiteres Gefahrenpotential bezüglich eines Verlusts von Unternehmens-Know-how birgt die Abwerbung von Mitarbeitern genauso wie ein Mitarbeiterwechsel in einem regulären Bewerbungsverfahren. Letztlich sind auch gekündigte Mitarbeiter, welche z.B. aus Rachegründen das Firmenwissen an deren zukünftige Arbeitgeber preisgeben oder in der Öffentlichkeit darüber sprechen, ein Sicherheitsrisiko im Rahmen eines Informationsschutzkonzeptes.[26]

Der Informationsschutz im Allgemeinen kann nur durch eine ständige Anpassung der Präventivmaßnahmen erfolgreich sein. Daher ist ein funktionelles Informationsschutzmanagement, bezogen auf die Aktualität und die ständige Nachbesserung der Abwehrmaßnahmen,

eine Daueraufgabe zur Sicherstellung des Unternehmensschutzes.[27]

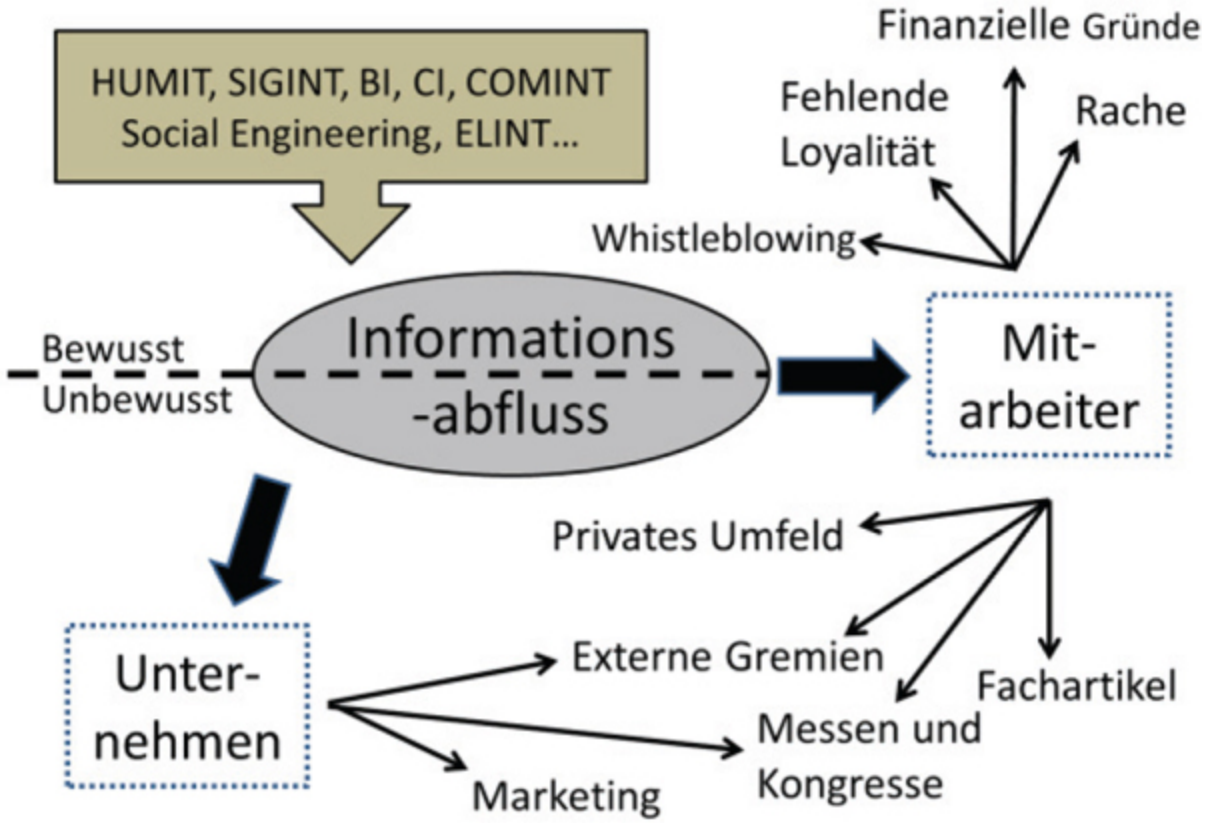

Abb. 1: Möglichkeiten des Informationsabflusses

---

[3] Vgl. Reitz, S.7

[4] Vgl. BMI, Verfassungsschutzbericht 2012, S.334

[5] Geprägt wurde dieser Begriff in einer Rede Churchills und bezeichnet die politische und weltanschauliche Trennungslinie zwischen Ost- und Westeuropa.

[6] Der Kalte Krieg beschreibt den waffenlosen Konflikt der beiden Supermächten USA und der damaligen UDSSR in der Zeit von 1945 bis 1991

[7] BfV, Wirtschaftsspionage, S.6

[8] Vgl. Grasberger

[9] Vgl. Griesshaber

[10] Vgl. Bühler und Sobbek, S. 13

[11] Vgl. Fussan, S.5

[12] Vgl. Bühler und Sobbek, S. 13 ff.

[13] Die Definition Wirtschaftskriminalität ist nicht einheitlich. Einmal gibt es das Unternehmen begünstigende Unternehmenskriminalität (Corporate Crime) sowie jene Delikte, bei der sich ein Mitarbeiter im beruflichen Umfeld persönlich bereichert (Occupational Crime).

[14] Vgl. Techmeier, Wirtschaftskriminalität.

[15] Sutherland definierte diesen Begriff und bewies, dass Kriminalität nicht nur unter den Faktoren wie Armut oder niedrigem sozialer Status vorkommt, sondern das auch Personen mit hohem gesellschaftlichem Status deviantes Verhalten an den Tag legen können.

[16] Vgl. Nolo´s

[17] Vgl. Bühler, Die deutsche Wirtschaft ist als Ziel interessant.

[18] Vgl. Hayranek, S.151

[19] Vgl. Corporate Trust, S.34 ff.

[20] Vgl. Hirschmann, S.60

[21] Vgl. BMI, Verfassungsschutzbericht 2012, S.336

[22] Vgl. ISM, Informationsschutz in der gewerblichen Wirtschaft, S.8

[23] Auch Sicherheitsrichtlinie genannt, beschreibt den erstrebten Sicherheitsanspruch eines Unternehmens und konzeptionell die Maßnahmen, um diese zu erreichen.

[24] Vgl. Bisanz, S.27

[25] Vgl. Maro, S.16

[26] Vgl. Hohlfeld, S.12 ff.

[27] Vgl. Bühler und Sobbek, S.13

2. Problemstellung

“In the business world, the rear-view mirror is always clearer than the windshield.”

Warren Buffet

Aus der Praxis:[28]

> ***Datenklau bei Vodafone-Deutschland***
> *Jemand hat zwei Millionen Kundendaten (Name, Anschrift, Bankdaten etc.) von Vodafone Deutschland gestohlen. Dies war laut Unternehmen nur mit Insiderwissen durchführbar. Nach einer Anzeige bei den zuständigen Behörden konnten diese den Kreis der Verdächtigen eingrenzen und führten bei diesen Hausdurchsuchungen durch.*

Gegenstand dieser Arbeit wird sein zu eruieren, wo Schwachstellen und Verbesserungsbedarf im Rahmen eines erfolgreichen Informationsschutzes in Unternehmen bestehen, welche Möglichkeiten präventiver Schutzmaßnahmen und deren Auswirkungen der Wirtschaft zur Verfügung stehen und welche Risiken einzelne Umsetzungen bergen. Ebenso wird der thematische Schwerpunkt, der Innentäter und die damit in Verbindung stehende Problematik, näher beleuchtet. Es wird untersucht, ob potentielle Innentäter aufgrund von Änderungen ihres Verhaltens oder ihrer Gesinnung erkennbar sind.

Damit erfolgreich gegen Wirtschafts- und Industriespionage vorgegangen werden kann, muss das Phänomen Spionage untersucht und analysiert werden. Erst wenn die

Erscheinungsformen, die rechtlichen Grundlagen und Grenzen bekannt sind, und welche Interessen dabei von den Unternehmen verfolgt werden, erst dann ist die Entwicklung erfolgreicher Präventionsmaßnahmen möglich. Die Analyse beginnt mit der Erhebung möglicher Ursachen von Wirtschafts- und Industriespionage und der Beantwortung der Frage, welche Faktoren eine sinkende Loyalität des Arbeitnehmers unterstützen. Dazu werden mögliche Verhaltensänderungen, welche sich bei den betroffenen Personen einstellen können, mit einbezogen. Anschließend werden Grenzen und Methoden des Informationsschutzes aufgezeigt, mit welchen Unternehmen sich gegen eine Ausspähung schützen. Darauf aufbauend werden ausgesuchte Einzelmaßnahmen zum Schutz vor irregulärem Informationsabfluss vorgestellt.

Bezug nehmend auf die beschriebenen Einzelmaßnahmen wird darauf hingewiesen, dass diese nur exemplarisch dargestellt und durch unzählige weitere Maßnahmen und im Rahmen situativer Anpassungen erweiterbar sind. Der Informationsschutz, als Schutzinstrument gegen die Wirtschafts- und Industriespionage, ist als ein sich ständig wandelnder und der jeweiligen Situation anzupassender Prozess anzusehen. Informationen bzgl. interner Schutzmaßnahmen von Unternehmen sind nur vereinzelt bzw. gar nicht verfügbar, daher resultiert diese Arbeit größtenteils auf Veröffentlichungen über den zu untersuchenden Themenbereich.

Handlungsempfehlungen:

- Prüfen Sie, ob Ihr Unternehmen ein Informationsschutzkonzept betreibt.
- Machen Sie sich über die persönlichen und unternehmerischen Gefahren – die dadurch

entstehenden kurz- und langfristigen Folgen – kundig.
- Informieren Sie ebenfalls Ihre Belegschaft im Rahmen einer Grundsätzlichen Sensibilisierung über die Gefahren eines irregulären Informationsabflusses und über die Folgen die dadurch jeden einzelnen betreffen können.
- Prüfen Sie, welche schützenswerten Informationen sich in Ihrem Unternehmen befinden.
- Haben Sie schützenswerte Informationen und sind die Schutzmaßnahmen den aktuellen Bedürfnissen angepasst?
- Wann wurden die Mitarbeiter das letzte Mal über die Richtlinien zum Informationsschutz geschult?
- Errechnen Sie die bisherigen finanziellen Verluste durch einen ungewollten Wissensabfluss.
- Prüfen Sie in der Vergangenheit liegende unerklärliche Umsatzschwankungen, ob dieses an einem Abfluss von firmeninternen, schützenswerten Informationen begründet ist.
- Prüfen Sie die Aktualität Ihrer Sicherheitsinvestitionen im Verhältnis zu Ihren Unternehmensrisiken.
- Nehmen Sie Ihre Pflicht bzgl. der Kontrolle und Aufsicht Ihrer Mitarbeiter wahr.
- Kontrollieren Sie, ob Sie schon Opfer eines Informationsdiebstahls geworden sind.

---

[28] Vgl. Geuking

3. Definition und Abgrenzungen

“When we look closer at the world economy, we see there a battlefield where the companies conduct a war without mercy.
No prisoner are made there. The one who falls, dies.
Following the example of military strategy, the winner is always inspired by simple rules:
best preparation, the fastest movements, the offensive on hostile ground, good allies, the will to overcome.”

Francois Mitterrand

Aus der Praxis:[29]

Spionage vs. Whistleblowing
Viele Handlungen werden mit dem Begriff der Spionage beschrieben, trotz oder aufgrund der unzähligen Möglichkeiten der Informationsgewinnung. Die wohl populärsten Verwechslungen finden jedoch mit dem Whistleblowing statt. In den letzten Jahren haben einige Whistleblower mit ihren Enthüllungen die Schlagzeilen dominiert. Hierzu gehören Bradley Manning, Aaron Schwarz und Edward Snowden. Erstgenannter gab als geheim eingestufte Dokumente an eine Internetplattform, der Zweite hackte einen Server und entwendete wissenschaftliche Artikel um sie der Öffentlichkeit zugänglich zu machen. Der Letzte war Informatiker und entwendete Dokumente der NSA, um diese dann vor seinem Untertauchen in Hongkong zu veröffentlichen.

Die Spionage hat viele Gesichter und erscheint in den unterschiedlichsten Gestalten. Sie hat sich stets den aktuellen Gegebenheiten angepasst, um effektiv an Informationen gelangen zu können. Aufgrund dessen gibt es heute eine Vielzahl von unterschiedlichen Arten wie Spionage betrieben werden kann. Zur Abwehr dieser vielfältigen Angriffsarten bedarf es spezieller Kenntnisse, sowie auch einer grundlegenden Erkenntnis. Grundsätzlich muss ein Verständnis vorhanden sein, dass jeder und alles ein Ziel von irregulärem Informationsabfluss sein kann. Zu einer erfolgreichen Abwehr der unterschiedlichsten Arten der Informationsgewinnung bedarf es des Wissens über die dementsprechenden Durchführungsmethoden – z.B. dass Human Intelligence (HUMINT) die Informationsbeschaffung unter Einbeziehung menschlicher Quellen ist – und einer Abstellung der diesbezüglichen Unternehmensschwachstellen.

Spionage – der sprachliche Ursprung und der allgemeine Sprachgebrauch

“The secret to success is to know something nobody else knows.”

Aristoteles Onassis

Das Wort Spionage ist eine Ableitung des lateinischen Wortes „spicari“ und des romanischen „spica“ und beschreibt das Ausspähen, Erspähen oder Auskundschaften zur Erlangung fremden Wissens.[30] In der Gesellschaft haben sich im Laufe der Zeit unzählige Beschreibungen für Mitarbeiter staatlicher Nachrichtendienste und für deren Informanten etabliert. Diese entstanden entweder im Zusammenhang bestimmter geschichtlicher Ereignisse oder können z.B. bestimmten Charakteristika bzgl. der

Durchführung zugeordnet werden. So ist Agent die offizielle Bezeichnung eines nachrichtendienstlichen Mitarbeiters.[31] Der Spion, obwohl fachlich und gesellschaftlich anerkannt, ist eine umgangssprachliche Nutzung und eine Ableitung aus dem Wort Spionage bzw. deren inhaltlicher Bedeutung. Neben diesem gibt es noch weitere umgangssprachliche Bezeichnungen. Darunter zählen ganz allgemeine Bezeichnungen wie z.B. „Schlapphüte“[32].[33] Diese Bezeichnung entstand durch das charakterisierende Bild eines observierenden Agenten mit dem dafür typischen Hut und Mantel.[34] Neben diesem besteht noch eine Reihe weiterer Bezeichnungen, welche die typisierte Art der Informationsbeschaffung beschreiben[35] oder als abwertend genutztes Synonym eines Informanten[36] genutzt werden.

Die Wirtschafts- und Industriespionage

“The most successful person is usually the one with the best information.“

Benjamin Disraeli

Die Medien und die Gesellschaft fassen Vorfälle, in denen es um Wirtschafts- oder Industriespionage geht, häufig unter dem Überbegriff Spionage zusammen. Teilweise wird, da es meist Unternehmen betrifft, von Wirtschaftsspionage gesprochen. Dennoch gibt es bedeutende Unterschiede zwischen den Begrifflichkeiten bzw. den damit in Verbindung stehenden Akteuren. So kann man diese dahingehend unterscheiden, dass die Wirtschaftsspionage durch fremde staatliche Aufklärungsdienste betrieben wird.[37] Bei einer durchgeführten Industrie- und Konkurrenzspionage sind grundsätzlich konkurrierende Unternehmen involviert. Die Abgrenzung der wirtschaftskriminellen Handlung in deren

Beschaffungsarten ist in den Verantwortlichkeiten der Behörden begründet. Diese sind aufgrund der Gesetzeslage zu einem Vorgehen gegen die fremdstaatlich organisierte Informationsabschöpfung verpflichtet.[38] Ein verpflichtendes Vorgehen deutscher Behörden bei Fällen der Industriespionage besteht wiederum nicht, hier liegt die Verantwortung der Abwehr bei den Unternehmen selbst. Dieses Paradoxon existiert in dieser Form, bzgl. der Verteilung von Verantwortlichkeiten, in keinem anderen Land. Weiß man doch bei einem anfänglichen Verdacht auf Spionage in der Regel nicht, wer Initiator einer solchen dolosen Handlung ist.[39] In Deutschland hat sich hinsichtlich der Bekämpfung und Prävention solcher Interaktionen eine Vielzahl deutscher und anderssprachiger Fachtermini durchgesetzt. So finden u.a. Begrifflichkeiten wie Wirtschaftsschutz und Informationssicherheit aus der deutschen Sprache[40] sowie Bezeichnungen aus dem angloamerikanischen Raum wie Counter Espionage, Counter Crime oder Counter Intelligence Anwendung.[41]

Abgrenzung des Spionagebegriffs

„Ein Spion am rechten Ort ersetzt 20.000 Mann an der Front.“

Napoleon Bonaparte

Durch die Globalisierung und den dadurch steigenden Wettbewerb sind das Wissen über die Konkurrenz und die dauerhafte Marktbeobachtung ein essentieller Bestandteil unternehmerischen Handelns.[42] Aufgrund dessen haben sich neue unternehmerische Tätigkeitsfelder entwickelt, welche oft einer Spionagetätigkeit gleichgestellt werden bzw. sich als eine solche darstellen. Diese sind u.a. unter den Bezeichnungen Communication Intelligence[43]