Elisa Wallwaey, Esther Bollhöfer, Susanne Knickmeier (Hrsg.)

Wirtschaftsspionage und Konkurrenzausspähung

GEFÖRDERT VOM

Das diesem Band zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung im Zuge der Bekanntmachung „Zivile Sicherheit – Schutz vor Wirtschaftskriminalität“ des BMBF im Rahmen des Programms „Forschung für die zivile Sicherheit“ der Bundesregierung unter dem Förderkennzeichen 13N13410 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen und Autoren.

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Kriminologische Forschungsberichte

Herausgegeben von Hans-Jörg Albrecht
und Günther Kaiser

Band K 187

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Elisa Wallwaey, Esther Bollhöfer, Susanne Knickmeier (Hrsg.)

Wirtschaftsspionage und Konkurrenzausspähung

Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern

Duncker & Humblot • Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

www.mpicc.de
Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
www.duncker-humblot.de
Umschlagphoto: Pixabay
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany

ISSN 1861-5937
ISBN 978-3-86113-275-2 (Max-Planck-Institut)
ISBN 978-3-428-15989-5 (Duncker & Humblot)

DOI https://doi.org/10.30709/978-3-86113-275-2

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706

Vorwort

Der vorliegende Band präsentiert die wesentlichen Ergebnisse aus dem zweiten von insgesamt drei Modulen des Forschungsprojekts Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS). Das im Rahmen der Bekanntmachung „Zivile Sicherheit – Schutz vor Wirtschaftskriminalität" des Bundesministeriums für Bildung und Forschung geförderte Projekt widmete sich der kriminologischen Untersuchung von Wirtschaftsspionage und Konkurrenzausspähung und der rechtsvergleichenden Analyse ihrer straf- und verfahrensrechtlichen Regulierung in Deutschland und Europa. Das Forschungsvorhaben war als Verbundprojekt angelegt; Verbundpartner waren das Fraunhofer Institut für System- und Innovationsforschung, Karlsruhe, und das Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg i.Br., als Konsortialführer. Als assoziierte Partner unterstützten das Bundeskriminalamt, das Landeskriminalamt Baden-Württemberg und die Sächsische Hochschule der Polizei das Vorhaben.

Neben einer Bestandsaufnahme des (rechtlichen) Status quo wurden in dem Projekt der Phänomenbereich analysiert, mögliche Optimierungspotenziale identifiziert und entsprechende Empfehlungen ausgearbeitet. Im Fokus des zweiten Projektmoduls stand eine Mehrebenen-Evaluation, die eine Literaturanalyse, Dokumentenanalyse, exemplarische Fallstudien sowie Experteninterviews mit Vertretern kleiner und mittlerer Unternehmen (KMU), Wissenschaftsorganisationen und Behörden umfasste. Ziele dieser Untersuchungsschritte waren die Analyse der Phänomenologie von Wirtschaftsspionage und Konkurrenzausspähung, der Erkennbarkeit von Vorfällen, der Präventionsstrategien von KMU und Wissenschaftsorganisationen sowie deren Kooperation mit behördlichen Akteuren. Dabei wurden die Ergebnisse aus Deutschland u.a. zur Identifizierung von Best Practices mit denen ausgewählter europäischer Länder (Bulgarien, Dänemark, Großbritannien, Österreich und der Schweiz) verglichen.

Die empirische Forschung ist ganz wesentlich von dem Zugang zu relevanten Daten abhängig. Unser besonderer Dank gilt den Staatsanwaltschaften in Deutschland, der Schweiz, Österreich und Bulgarien, die uns Zugang zu den bei ihnen geführten Strafverfahren gewährt haben, den zahlreichen Vertreterinnen und Vertretern von KMU, Behörden und Wissenschaftsorganisationen in Deutschland, Bulgarien, Dänemark, Österreich und der Schweiz, die sich die Zeit für Experteninterviews genommen haben, sowie der Bibliothek des Max-Planck-Instituts für ausländisches und internationales Strafrecht, die alle für die qualitative Literaturanalyse benötigten Publikationen zur Verfügung stellte.

Die umfangreiche Erhebung, Auswertung und Analyse der Daten aus den Experteninterviews, Strafakten in Deutschland und den exemplarischen Fallstudien wäre ohne die Unterstützung der studentischen Mitarbeiterinnen und Mitarbeiter am

Max-Planck-Institut für ausländisches und internationales Strafrecht nicht möglich gewesen. Für ihre Mitwirkung danken wir *Anna-Lisa Bähr, Sonja Bühler, Claudio Calabro, Sarina Gäckle, Nico Hanke, Johannes Huschka, Egzona Hyseni, Alexandre Kunz, Peter Müller, Luca Schler, Tim Schmetzer, Aline Vugrinic* und *Jasmin Winkler*. Besonderer Dank gilt, last but not least, auch *Katharina John* – mit dem gesamten Team des kriminologischen Lektorats des Max-Planck-Instituts für ausländisches und internationales Strafrecht – für die umfangreichen Lektorierungsarbeiten.

Zu guter Letzt noch ein Hinweis zum Sprachgebrauch. In dem Bewusstsein, dass es sich um ein sprachliches Dilemma handelt, wird in bestimmten Kontexten, in denen Rollen-, Funktions-, Tätigkeits- bzw. Berufsbezeichnungen Verwendung finden, am Gebrauch des generischen Maskulinums festgehalten – sofern die deutsche Sprache dort jeweils keine linguistisch überzeugende Alternative für eine geschlechtsneutrale Bezeichnung bereithält. Diese Handhabung zielt nicht nur auf eine bessere Lesbarkeit des Textes ab, sondern gründet auch in der Erkenntnis, dass Personenbezeichnungen auf einem Referenz-Kontinuum zwischen den Bezugspolen „funktional-abstrakt, geschlechtsneutral“ und „konkret individualisierend, geschlechtsspezifisch“ verortet werden müssen und somit in jedem Einzelfall eine Abwägung stattfinden sollte, ob eine generische – bzw. generisch gemeinte – Form oder eben eine Paarbezeichnung jeweils treffender ist. Zwingend wird die Nutzung einer verallgemeinernden Form dieser Ansicht zufolge dort, wo die Bezugsebene eindeutig unpersönlich und geschlechtsneutral ist und die schematische Verwendung von Paarbezeichnungen Gefahr läuft, Bedeutungsverschiebungen zu generieren. Dies zu entscheiden obliegt den jeweiligen Autorinnen und Autoren.

Freiburg, im Dezember 2019 Die Herausgeberinnen

Inhaltsverzeichnis

Abkürzungsverzeichnis

A1–A9	Arbeitspakete des Forschungsprojekts WiSKoS
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AKIF	Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen
AUT	Österreich
BDI	Bundesverband der Deutschen Industrie e.V.
BDSG	Bundesdatenschutzgesetz
BG	Bulgarien
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BfV	Bundesamt für Verfassungsschutz
BIP	Bruttoinlandsprodukt
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CD	Compact Disc
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CH	Schweiz
CIO	Chief Information Officer
CiSP	Cybersecurity Information Sharing Partnership (UK)
CPNI	Centre for the Protection of National Infrastructure (UK)
CT	Corporate Trust
DDoS	Distributed-Denial-of-Service
DE	Deutschland
DEFCON	Defense readiness conditions
Destatis	Statistisches Bundesamt
DFN	Deutsches Forschungsnetzwerk
DIN	Deutsches Institut für Normung
DK	Dänemark
DNS	Domain Name System
DoS	Denial-of-Service

EFTA	Europäische Freihandelsassoziation
EU	Europäische Union
EUR	Euro
FBI	Federal Bureau of Investigation (USA)
F&E	Forschung und Entwicklung
Fraunhofer ISI	Fraunhofer Institut für System- und Innovationsforschung
GAU	Größter anzunehmender Unfall
GCHQ	Government Communications Headquarters (UK)
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GVG	Gerichtsverfassungsgesetz
HAZ	Hannoversche Allgemeine
HMG	Her Majesty's Government (UK)
HUMINT	Human Intelligence
ICT	Information and Communications Technology
IfM Bonn	Institut für Mittelstandsforschung Bonn
IKT	Informations- und Kommunikationstechnologie
IfD	Institut für Demoskopie Allensbach
IP	Internet Protocol
i.S.d.	im Sinne der/des
ISMS	Informationssicherheitsmanagementsystem
IT	Information Technology
KMU	kleine und mittlere Unternehmen
LKA	Landeskriminalamt
MELANI	Melde- und Analysestelle Informationssicherung (CH)
MI6	Military Intelligence Service, Section 6 (UK)
MPICC	Max-Planck-Institut für ausländisches und internationales Strafrecht
m.w.N.	mit weiteren Nachweisen
M1, M2, M3	Module 1, 2, 3 des Forschungsprojekts WiSKoS
NC3	Danish National Cyber Crime Center
NDB	Nachrichtendienst des Bundes (CH)
NStZ	Neue Zeitschrift für Strafrecht
OSINT	Open Source Intelligence
PKS	Polizeiliche Kriminalstatistik

PPP	Public-Private-Partnership
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
Seq.	(Interview-)Sequenz
SiFO BW	Sicherheitsforum Baden-Württemberg
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWR	Sluschba Wneschnei raswedki [russischer Auslandsgeheimdienst für zivile Spionage]
TECHINT	Technical Intelligence
UK	United Kingdom
USB	Universal Serial Bus
USD	US-Dollar
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
WiSKoS	Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (Forschungsprojekt)
WLAN	Wireless Local Area Network
WoS	Web of Science
WTO	World Trade Organization
ZPO	Zivilprozessordnung

Einleitung

Wirtschaftsspionage und Konkurrenzausspähung in Theorie und Praxis[1]

Elisa Wallwaey, Susanne Knickmeier & Michael Kilchling

Spektakuläre (Einzel-)Fälle von Wirtschaftsspionage und Konkurrenzausspähung sorgen in der Öffentlichkeit immer wieder für Schlagzeilen. Trotz ihres hohen Schadenspotenzials sind diese Kriminalitätsformen jedoch empirisch bislang nur rudimentär untersucht. Dies ist unter anderem darauf zurückzuführen, dass sich neben den ‚klassischen' Vorgehensweisen im Zuge des technologischen Wandels und der damit einhergehenden Entwicklung zur „Industrie 4.0" immer neue Ausspähmethoden, vor allem auf elektronischem Wege, entwickeln, sodass sich die Erscheinungsformen dieser Deliktsbereiche und die Gefahrenlage kontinuierlich ändern. Das Forschungsprojekt Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS) hatte zum Ziel, Wirtschaftsspionage und Konkurrenzausspähung in ihrer aktuellen Bedeutung und ihren phänomenologischen Ausprägungen empirisch zu analysieren und strukturiert zu erfassen. Insbesondere sollten der Brückenschlag zwischen betrieblichen Innovationsprozessen und Angriffspunkten vollzogen, Bedrohungsszenarien erfasst und innerbetriebliche Erkennungs- und Präventionsstrategien entwickelt werden.

Der vorliegende Band enthält – aufbauend auf der vorausgegangenen rechtsvergleichenden Analyse der Straftatbestände und verfahrensrechtlichen Regelungen in allen europäischen Mitgliedsstaaten und der Schweiz[2] – Beiträge zu verschiedenen Analyseschritten,[3] die im Rahmen einer Mehrebenen-Evaluation des Phänomenbereichs in Deutschland und ausgewählten Ländern[4] durchgeführt wurden (*Modul 2* des Projektes WiSKoS).

---

1 Herrn stud. iur. *Christophe Dierdorf* danken wir für seine Ausarbeitungen zum Geschäftsgeheimnisgesetz (GeschGehG), die Erstellung der Synopse sowie die Literaturrecherchen zur Schnittstelle von organisierter Kriminalität und Wirtschaftsspionage/ Konkurrenzausspähung.

2 *Carl & Kilchling* 2018.

3 Siehe *Abschnitt 3.2* in diesem Kapitel.

4 Zu den Kriterien für die Länderauswahl siehe *Abschnitt 4* in diesem Kapitel.

1. Stand der Wissenschaft

Das Gesamtphänomen „Wirtschaftsspionage und Konkurrenzausspähung" ist ein empirisch bislang unzulänglich erforschter Bereich. Zwar wurden in der Vergangenheit vereinzelte Fragestellungen – vor allem in rechtswissenschaftlichen Studien – untersucht;[5] einschlägige wissenschaftliche Literatur und empirische Untersuchungen neueren Datums, insbesondere solche aus dem deutschsprachigen Raum, liegen jedoch nur in eingeschränktem Maße vor.[6] Die Aussagekraft älterer Literatur und Studien ist aufgrund der sich stetig ändernden Begehungsformen – insbesondere im Hinblick auf die kontinuierliche Entwicklung neuer Bedrohungsszenarien, die mit den Möglichkeiten des digitalen Zugriffs auf geschützte Informationen einhergehen – für die Aufklärungsarbeit ebenso wie für die Entwicklung wirksamer Präventionsmaßnahmen von untergeordneter Bedeutung. Neuere empirische Untersuchungen zur Wirtschafts- oder Cyberkriminalität, in die vereinzelte Fragen zur Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung einbezogen wurden, lagen vor Projektbeginn vor allem von außerwissenschaftlichen Organisationen vor, z.B. von den Unternehmensberatungen KPMG, PwC (Letztere regelmäßig in Zusammenarbeit mit der Martin-Luther-Universität Halle-Wittenberg) und Corporate Trust, sowie von Verbänden, wie z.B. Bitcom e.V. Die Unternehmensberatung PwC gibt zudem in ungefähr zweijährigem Rhythmus den „Global Economic Crime and Fraud Survey" heraus, für den Unternehmen in ca. 30 Ländern weltweit befragt werden.[7] Zwei weitere Studien, eine von der Universität Lüneburg im Auftrag des Sicherheitsforums Baden-Württemberg (2004) und eine vom Sicherheitsforum Baden-Württemberg (2010) selbst, beschäftigten sich mit dem Schadenspotenzial des

---

5 Zum Beispiel: Spionage und Sabotage im Betrieb (*Amelunxen* 1977); Betriebsspionage (*Liebl/Woll* 1987); Konsequenzen neuartiger Erscheinungsformen des wirtschaftlichen Wettbewerbs für den strafrechtlichen Schutz von Geschäfts- und Betriebsgeheimnissen (*Metzler* 1990).

6 Seit 2008 sind in Deutschland einige Beiträge, studentische Abschlussarbeiten oder Dissertationen, die sich aus der Perspektive verschiedener Disziplinen mit Fragen zur Phänomenologie auseinandersetzen, erschienen, zum Beispiel: Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen (*Aldoney Ramirez* 2009); Industriespionage (*Schaaf* 2009); Industriespionage. Risikofaktor Mensch (*Röder* 2011); Gefahren der Wirtschaftsspionage und Auswirkungen auf das IT-Projektmanagement (*Scherf* 2013); Geheimnisschutz – Kernaufgabe des Informationsmanagements im Unternehmen (*Ann* 2014); Spionage in Wirtschaft und Industrie. Identifikation und Auswahl von Tätern (*Detlinger* 2014); Informationsschutz im Unternehmen (*Kirsch* 2014); Der „Datendiebstahl" (*Wagner* 2014); Schutz vor Industriespionage. Analyse, Prävention und Abwehr des irregulären Verlustes von Know-how in Unternehmen (*Sendzik* 2014); Industriespionage im deutschen Mittelstand. Wie schützt man Know-how wirkungsvoll? (*Zwickl* 2015).

7 Siehe PwC, Global Economic Crime and Fraud Survey; https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html [15.08.2020].

Know-how-Verlusts[8] und Maßnahmen des Know-how-Schutzes.[9] *Tabelle 1* enthält eine Auswahl dieser in den vergangenen Jahren erschienenen Publikationen.

Tabelle 1 Auswahl an Studien in Deutschland (2010–2018)

Jahr	**Hrsg.**	**Thema**
2018	KPMG	Wirtschaftskriminalität in Deutschland
2018	Bitcom e.V.	Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie
2017	PwC & Uni Halle-Wittenberg	Wirtschaftskriminalität in der analogen und digitalen Wirtschaft
2016	PwC & Uni Halle-Wittenberg	Wirtschaftskriminalität in der analogen und digitalen Wirtschaft
2016	KPMG	Tatort Deutschland – Wirtschaftskriminalität in Deutschland
2016	Bitcom e.V.	Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie
2016	Bitcom e.V.	Spezialstudie Wirtschaftsschutz
2015	Bitcom e.V.	Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter
2014	KPMG	Wirtschaftskriminalität in Deutschland
2014	PwC & Uni Halle-Wittenberg	Wirtschaftskriminalität und Compliance – Handel und Konsumgüterindustrie 2014
2014	Result Group & F.A.Z-Institut	Kriminelle Risiken im Mittelstand – Gefahren, Schäden und Prävention
2014	Corporate Trust	Industriespionage 2014 – Cybergeddon der Deutschen Wirtschaft durch NSA & Co.?
2012	KPMG	Wirtschaftskriminalität in Deutschland
2012	PwC & Uni Halle-Wittenberg	Wirtschaftskriminalität Versicherungsbranche
2012	Corporate Trust	Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar
2010a	KPMG	Computerkriminalität in der deutschen Wirtschaft
2010b	KPMG	Wirtschaftskriminalität in Deutschland – Fokus: Mittelstand
2010	Sicherheitsforum Baden-Württemberg	Know-how-Schutz in Baden-Württemberg

Wenig untersucht ist auch das Verhältnis zwischen organisierter Kriminalität und Wirtschaftsspionage bzw. Konkurrenzausspähung. Gerade bei komplexen und gut organisierten Cyberangriffen ist zu vermuten, dass die Täter entweder Geheimdiens-

8 Vgl. *Kahle & Merkel* 2004.

9 Vgl. Sicherheitsforum Baden-Württemberg 2010.

ten fremder Staaten oder organisierten Gruppen angehören. *Pohl*, zum Beispiel, beschreibt in seinem technischen Beitrag aus dem Jahr 2008 die systematische Suche nach Sicherheitslücken in IT-Systemen, die bisweilen nicht sofort dem Hersteller gemeldet, sondern stattdessen an Mitglieder der organisierten Kriminalität verkauft worden seien.[10]

2. Abgrenzung von Wirtschaftsspionage und Konkurrenzausspähung in Deutschland

Die Begriffe Wirtschaftsspionage und Konkurrenzausspähung sind in Deutschland nicht legaldefiniert. Der Definition deutscher Behörden folgend bezeichnet Wirtschaftsspionage „die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben."[11] Konkurrenzausspähung hingegen lässt sich als das Ausforschen eines Unternehmens durch andere Unternehmen oder Einzelpersonen beschreiben.[12]

Darüber hinaus sind die Delikte in diesem Phänomenbereich regulatorisch schwer zu fassen, da weder ein expliziter Straftatbestand der Wirtschaftsspionage noch ein solcher der Konkurrenzausspähung existiert. Die Delikte sind zum einen an der Schnittstelle zwischen Staatsschutz- und Wirtschaftskriminalität angesiedelt, zum anderen überschneiden sie sich mit Delikten der Cyberkriminalität.[13] Während die Wirtschaftsspionage als Staatsschutzdelikt gem. §§ 94 ff. StGB konzipiert ist, bei dem der Schutz der nationalen Interessen der Bundesrepublik Deutschland im Mittelpunkt steht, liegt der Fokus bei der Konkurrenzausspähung auf dem Schutz eines Geschäftsgeheimnisses. Bis April 2019 war der strafrechtliche Schutz von „Geschäfts- oder Betriebsgeheimnissen" vor allem in den §§ 17 ff. UWG geregelt. Mit dem Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG)[14] im April 2019 wurde die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Knowhows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung[15] in das deutsche

---

10 Vgl. *Pohl* 2008.

11 Deutscher Bundestag 2014, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE; https://dip21.bundestag.de/dip21/btd/18/022/1802281.pdf [15.08.2019], S. 2 (BT-Drs. 18/2281).

12 Vgl. *Fleischer* 2016, S. 4–5; *Kirsch* 2014, S. 11; *Lux & Peske* 2002, S. 30.

13 Hierzu ausführlicher *Kilchling & Carl* 2016.

14 BGBl 2019, Teil I Nr. 13, S. 466 ff.

15 Richtlinie (EU) 2016/943, ABl. L 157/1 vom 15.06.2016, S. 1.

Recht umgesetzt.[16] Der strafrechtliche Schutz von Geschäftsgeheimnissen wurde aus dem bisherigen regulatorischen Kontext des UWG herausgenommen und ist nunmehr in § 23 GeschGehG geregelt, in den die weggefallenen §§ 17–19 UWG im Wesentlichen integriert wurden. Die ehemals in § 17 Abs. 4 UWG enthaltenen Regelbeispiele wurden in § 23 Abs. 4 GeschGehG durch Qualifikationstatbestände ersetzt. Eine weitere Neuerung betrifft die Legaldefinition des Geschäftsgeheimnisses in § 2 GeschGehG, mit der der deutsche Gesetzgeber die in der Praxis irrelevante Unterscheidung zwischen einem Geschäfts- und einem Betriebsgeheimnis aufgegeben hat. Zudem reicht für die Annahme eines Geschäftsgeheimnisses ein subjektiver Geheimhaltungswillen nicht mehr aus, sondern der Geheimnisinhaber muss angemessene Schutzvorkehrungen für das zu schützende Geheimnis getroffen haben.

Unabhängig von den regulatorischen Schwierigkeiten kennzeichnen Unklarheiten über behördliche Zuständigkeiten und Ermittlungsabläufe seitens betroffener Unternehmen und Organisationen das Themenfeld und erschweren die Kooperation zwischen Behörden und Betroffenen.[17] Denn während für die Prävention von Wirtschaftsspionage neben den Strafverfolgungsbehörden auch die Verfassungsschutzbehörden zuständig sind, obliegen die Prävention und strafrechtlichen Ermittlungen in Fällen von Konkurrenzausspähung ausschließlich den Strafverfolgungsbehörden. Bei der Verfolgung von Fällen der Wirtschaftsspionage ist eine Sonderzuständigkeit des Generalbundesanwaltes gem. § 142a GVG gegeben. Fälle der Konkurrenzausspähung wiederum werden von den lokalen Staatsanwaltschaften bzw. den Schwerpunkt-Staatsanwaltschaften für Wirtschaftskriminalität bearbeitet.

Tabelle 2 Überblick zu Wirtschaftsspionage und Konkurrenzausspähung in Deutschland

	Wirtschaftsspionage	**Konkurrenzausspähung**
Definition deutscher Behörden	Wirtschaftsspionage ist die *staatlich* gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Unternehmen	Konkurrenzausspähung ist die *private* Ausforschung konkurrierender Unternehmen
Ziel	Förderung der Wirtschaft eines fremden Staates	Verfolgung (eigener) kommerzieller Interessen
Täterschaft	Mitarbeiter eines fremden Geheimdienstes	Angestellter oder andere Person
strafrechtliche Kernvorschrift	geheimdienstliche Agententätigkeit (§ 99 StGB)	Verrat von Geschäftsgeheimnissen (§ 23 GeschGehG)*
Zuständigkeit	Generalbundesanwalt (§§ 142a, 74a GVG)	Staatsanwaltschaft (ggf. Schwerpunkt-StA Wirtschaftskriminalität)

* Bis April 2019: Verrat von Geschäfts- und Betriebsgeheimnissen (§§ 17–19 UWG).

---

16 Eine Synopse von § 23 GeschGehG und §§ 17–19 UWG findet sich im Anhang zur vorliegenden *Einleitung.*

17 Siehe dazu *Stieber* 2018.

3. Verbundprojekt WiSKoS

Das Forschungsprojekt WiSKoS hatte, wie einleitend beschrieben, die systematische Erfassung der Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung, der staatlichen Kontrollstrukturen sowie der innerbetrieblichen Erkennungs- und Präventionsstrategien in Deutschland, den Mitgliedsstaaten der Europäischen Union (EU) und der Schweiz zum Ziel. Im Mittelpunkt der Untersuchung standen die kleinen und mittleren Unternehmen (KMU)[18], da sie eher auf eine Kooperation mit staatlichen Behörden angewiesen sind als Großkonzerne, die insbesondere dann, wenn sie multinational aufgestellt sind, zumeist eigene Reaktionsmechanismen implementiert haben. Unternehmen werden – der Empfehlung der Europäischen Kommission[19] folgend – anhand zweier Kriterien klassifiziert. Ein Kriterium betrifft die Anzahl Beschäftigten, das andere Kriterium entweder den Jahresumsatz oder die Bilanzsumme *(Tabelle 3)*. Zur Gruppe der KMU gehören demnach Unternehmen mit bis zu 250 Beschäftigten und entweder bis zu EUR 50 Mio. Jahresumsatz oder einer Bilanzsumme bis zu EUR 43 Mio.

Tabelle 3 Definitionskriterien für die unterschiedlichen Unternehmensklassen

Klassifikation	**Beschäftigte**		**Jahresumsatz**		**Bilanzsumme**
Kleinstunternehmen	< 10		< 2 Mio. EUR		< 2 Mio. EUR
Kleine Unternehmen	< 50	und	< 10 Mio. EUR	oder	< 10 Mio. EUR
Mittlere Unternehmen	< 250		< 50 Mio. EUR		< 43 Mio. EUR
Großunternehmen	≥ 205		≥ 50 Mio. EUR		≥ 43 Mio. EUR

Quelle: IfM Bonn (undatiert): KMU-Definition der Europäischen Kommission; www.ifm-bonn.org/definitionen/kmu-definition-der-eu-kommission/.

In die Untersuchung einbezogen wurde ferner der Wissenschaftssektor, der eine Vielzahl zukunftsträchtiger und kommerziell vielversprechender Ergebnisse generiert und damit ein ebenso attraktives Angriffsziel ist wie der Unternehmenssektor. Neben einer Bestandsaufnahme des (rechtlichen) Status Quo wurden die Phänomenologie analysiert, mögliche Optimierungspotenziale identifiziert und entsprechende Empfehlungen ausgearbeitet.

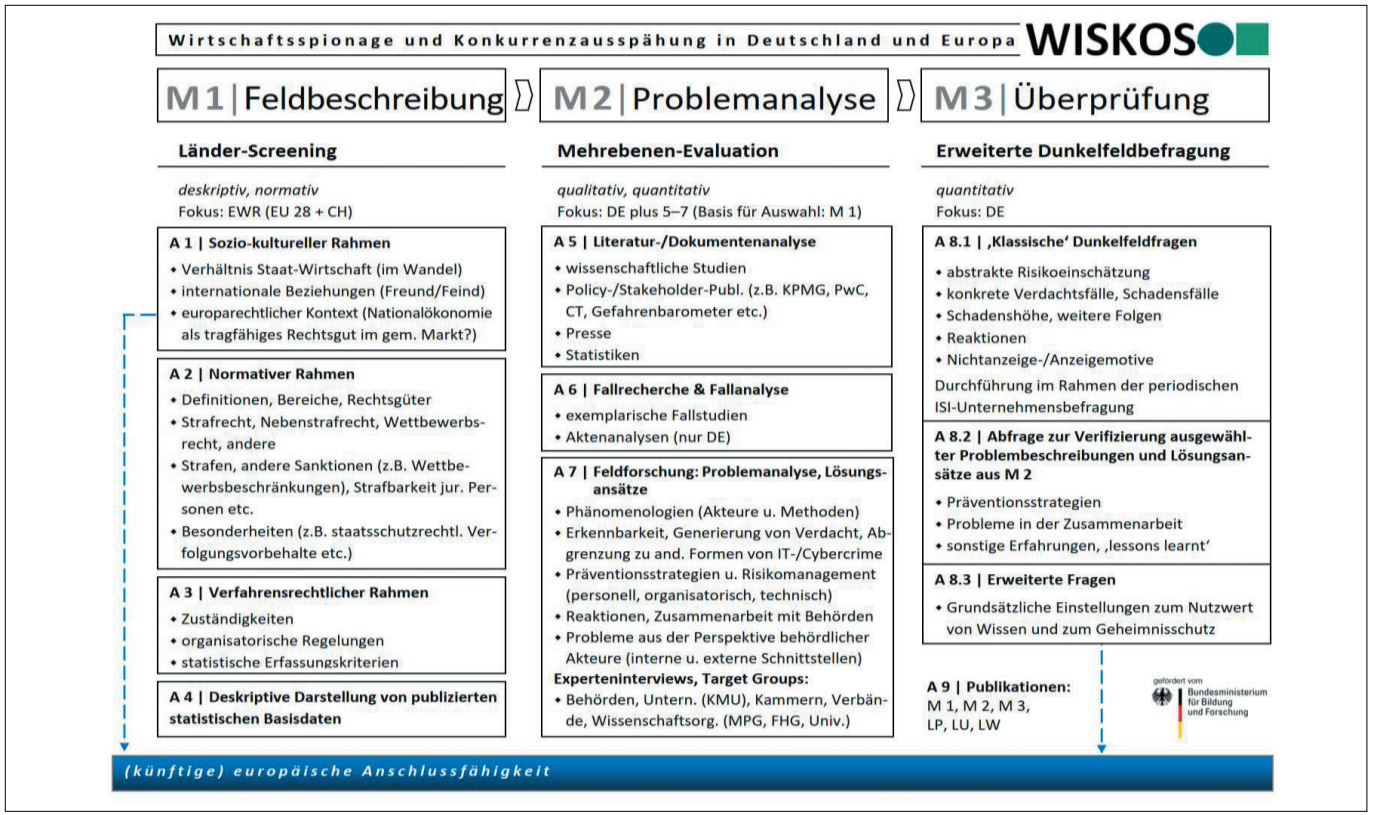
Das Projektdesign bestand aus drei – teilweise aufeinander aufbauenden – Modulen (siehe *Abbildung 1*).

---

18 Im Allgemeinen werden zu dieser Gruppe auch die Kleinstunternehmen gezählt.

19 Empfehlung der Europäischen Kommission vom 06. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG), ABl. L 124/36.

Abbildung 1 Übersicht über das Forschungsprojekt WiSKoS



3.1 Modul 1: Länder-Screening

Im Rahmen eines deskriptiv-normativ angelegten Länder-Screenings wurden zunächst vor allem die wirtschaftlich relevanten Rahmenbedingungen, die rechtlichen Regelungen zur Wirtschaftsspionage und Konkurrenzausspähung und deren Kontrolle sowie der Umfang von Wirtschaftsspionage und Konkurrenzausspähung innerhalb der EU-Staaten und der Schweiz systematisch erfasst und vergleichend analysiert. Die Ergebnisse der Arbeitspakete *A1–A4* von *Modul 1* finden sich in der Publikation *Carl & Kilchling 2018*. Zusammenfassend lassen sich für Deutschland, die weiteren Mitgliedsstaaten der EU und die Schweiz die im Folgenden dargelegten Ergebnisse festhalten.

Deutschland hat eine exportorientierte Nationalökonomie und ist eine der stärksten Volkswirtschaften innerhalb der EU, wodurch auch das Interesse anderer an deutschem Know-how hervorgerufen wird. Die strafrechtlichen Schutzvorschriften hängen von der Täterschaft ab, also davon, ob Mitarbeiter eines fremden Nachrichtendienstes oder Privatpersonen – zu eigenen Zwecken oder im Auftrag eines anderen Unternehmens – die Täter sind.[20] Der Umfang von Wirtschaftsspionage und Konkurrenzausspähung ist anhand statistischer Daten kaum zu beschreiben, da bei beiden Deliktsbereichen von einem hohen doppelten Dunkelfeld und einem verdeckten Hellfeld auszugehen ist. Zum einen werden Delikte häufig nicht entdeckt, zum anderen nicht angezeigt (doppeltes Dunkelfeld). Werden Delikte angezeigt, ist fraglich, ob sie als Konkurrenzausspähung oder Wirtschaftsspionage erkannt werden (verdecktes Hellfeld).[21] Weitere Verzerrungen in der statistischen Erfassung entstehen dadurch, dass bei der Staatsanwaltschaft angezeigte Delikte nicht in der Polizeilichen Kriminalstatistik (PKS) aufgeführt werden. Zudem sind die Daten zur Wirtschaftsspionage eingestuft und nicht öffentlich zugänglich.

Basis der vergleichenden Analyse der Wirtschafts- und Rechtssysteme der EU-Staaten und der Schweiz waren die Landesberichte von Expertinnen und Experten aus den jeweiligen Ländern, in denen die relevanten Themen ausführlich dargestellt worden sind.[22] Im Kern zeigt sich, dass unabhängig von dem jeweiligen Rechtssystem und der Wirtschaftsstruktur die (straf-)rechtlichen Regelungen zum Phänomenbereich in den europäischen Ländern uneinheitlich und fragmentarisch sind, auch wenn die Offenbarung von Geheimnissen im Geschäftsverkehr grundsätzlich strafbewehrt ist. Ebenso uneinheitlich geregelt sind die Zuständigkeiten für Prävention und Strafverfolgung, die je nach Delikt und Land bei einem Nachrichtendienst, der Polizei oder Grenzpolizei liegen, was eine grenzüberschreitende Kooperation, gegebenenfalls aber auch die Zusammenarbeit auf nationaler Ebene, erschweren

---

20 Siehe auch die von deutschen Behörden verwendete Definition von Wirtschaftsspionage und Konkurrenzausspähung sowie weitere Ausführungen zu den rechtlichen Rahmenbedingungen in *Abschnitt 2.*

21 Hierzu ausführlicher *Kilchling & Carl* 2016.

22 *Carl & Kilchling* 2018.

kann. Zur Vereinheitlichung des Schutzes von geschäftlich relevantem Know-how wurde im Juni 2016 die oben erwähnte EU-Richtlinie 2016/943 erlassen.[23] Sie enthält allerdings keine Mindestanforderungen an eine strafrechtliche Regulierung in den Mitgliedsstaaten. Ungeachtet der Vergemeinschaftung des europäischen Binnenmarktes verfolgen Mitgliedsstaaten nach wie vor (auch) die Förderung der eigenen Wirtschaft. Besonders ausgeprägt ist dies beispielsweise in Frankreich, wo das Verhältnis zwischen Staat und Wirtschaft traditionell eng ist. Seit 1997 unterhält Frankreich die „Ecole de Guerre Economique" (Wirtschaftskriegsschule), an der Absolventen nicht nur lernen, wie sie etwaigen Angriffen präventiv begegnen, sondern auch, wie Informationen über Konkurrenten erworben werden können.

Wie in Deutschland offenbaren sich auch im europäischen Ausland Defizite hinsichtlich des statistischen Datenmaterials in Bezug auf das Fallaufkommen und die verursachten Schäden. Einige Staaten führen gar keine dem Themenbereich zuordenbaren Statistiken, und selbst dort, wo statistische Daten vorliegen, ist eine Trennung von der allgemeinen Wirtschaftskriminalität und die Beurteilung ihrer quantitativen Relevanz nur schwerlich möglich oder gänzlich ausgeschlossen. Zusätzlich ergeben sich Probleme hinsichtlich der internationalen Vergleichbarkeit offizieller Kriminalstatistiken; so werden z.B. einige Statistiken als Eingangs- und andere als Ausgangsstatistiken geführt.[24]

3.2 Modul 2: Mehrebenen-Evaluation

Die Ergebnisse der drei Arbeitspakete *(A5–A7)* aus *Modul 2* sind Gegenstand der vorliegenden Publikation, die sich neben einer Beschreibung der Phänomenologie den spezifischen Problemlagen und Belangen von KMU, Wissenschaftsorganisationen und Behörden bei der Prävention und Strafverfolgung von Taten aus dem Bereich von Wirtschaftsspionage und Konkurrenzausspähung widmet. Ein spezielles Augenmerk wurde dabei auf die Kooperation zwischen (potenziellen) Opfern und den zuständigen Strafverfolgungsbehörden gelegt. An die Resultate einer umfassenden Literatur- und Dokumentenanalyse *(A5)* schließen sich verschiedene Beiträge zu den Ergebnissen einer weitreichenden Aktenanalyse für Deutschland und exemplarischen Fallstudien aus dem Ausland *(A6)* und zahlreicher qualitativer Experteninterviews im In- und Ausland *(A7)* an, die aus verschiedenen Blickwinkeln den jeweiligen Istzustand beleuchten und daraus, soweit möglich, Perspektiven für die Zukunft, insbesondere Handlungsstrategien in Deutschland, ableiten. Im Gegensatz zu *Modul 1* wurden in die Mehrebenen-Evaluation von *Modul 2* neben Deutschland nur fünf weitere Länder einbezogen (Bulgarien, Dänemark, Österreich, die Schweiz und das Vereinigte Königreich).[25]

---

23 Siehe *Fn. 15*.

24 Vergleiche stellvertretend für viele *Aebi* 2010.

25 Zu den Auswahlkriterien siehe *Abschnitt 4* in diesem Kapitel.

3.3 Modul 3: Dunkelfeldbefragung

In *Modul 3* wurden zwei quantitative Dunkelfeldbefragungen durchgeführt. Im Jahr 2015 konnte im Rahmen der durch das Fraunhofer Institut für System- und Innovationsforschung ISI alle zwei Jahre durchgeführten Befragung „Modernisierung der Produktion" ein Fragenblock zur Ausspähung von Know-how in Unternehmen integriert werden. Die Ergebnisse dieser Befragung flossen ebenso wie die Ergebnisse aus *Modul 2* in die Konzeption des Fragebogens für die erweiterte Dunkelfeldbefragung von KMU ein, die von Juni bis September 2017 stattfand. Wesentliche Kernbefunde wurden in einem von Fraunhofer ISI erstellten Ergebnisbericht publiziert, der auch online zur Verfügung steht.[26]

4. Auswahlkriterien für die Länder in Modul 2

Die Auswahl der Länder für die Vergleichsanalysen erfolgte auf der Grundlage der Landesberichte *(Modul 1)* anhand verschiedener, vor allem wirtschaftlicher und rechtlicher, Auswahlkriterien *(Tabelle 4).* Darüber hinaus wurden die geografische Lage des Landes innerhalb Europas, die Frage der Mitgliedschaft in der EU sowie Besonderheiten bei der Kooperation zwischen Behörden und Betroffenen als weitere Auswahlkriterien herangezogen. Nach einer Evaluation dieser Charakteristika wurden, um eine möglichst große Diversität im Hinblick auf die genannten Kriterien zu erzielen, Bulgarien, Dänemark, Österreich, das Vereinigte Königreich und die Schweiz für den Vergleich ausgewählt.

Tabelle 4 Übersicht über die wirtschaftlichen, rechtlichen und sonstigen Kriterien

Wirtschaftliche Kriterien	Rechtliche Kriterien	Sonstiges
• Wirtschaftskraft • Exportstärke • Innovationskraft • Verteilung der Unternehmensklassen	• Rechtskreiszugehörigkeit (Common Law oder Civil Law) • (Kodifizierte) Strafbarkeit • Strafrahmen • Behördliche Zuständigkeit • Unternehmensstrafrecht	• Mitgliedschaft in der EU • Geografische Lage • Besonderheiten bezüglich der Kooperation zwischen Behörden und Betroffenen

Im Folgenden werden die ausgewählten Länder anhand der Auswahlkriterien kurz im Vergleich dargestellt.

4.1 Wirtschaftliche Auswahlkriterien

Die wirtschaftlichen Auswahlkriterien waren die folgenden: Wirtschaftskraft, Exportstärke, Innovationskraft und die Verteilung der Unternehmensklassen (Kleinst-

26 *Bollhöfer & Jäger* 2018.

unternehmen, kleine und mittlere Unternehmen, Großunternehmen). Als wichtiger Indikator zur Einordnung der *Wirtschaftskraft* wurde das Bruttoinlandsprodukt (BIP) herangezogen. Dabei zeigte sich im Jahr 2016 bei den ausgewählten Vergleichsländern eine erhebliche Spannbreite zwischen der Schweiz mit einem BIP von EUR 72.500 pro Einwohner und Bulgarien mit einem BIP von EUR 6.880 pro Einwohner. Bei der Entwicklung des prozentualen Anteils an den *Exporten* der untersuchten EU-Länder in Drittländer im Zeitraum 2007–2016 wies Deutschland mit einem Durchschnittswert von 27,4 % kontinuierlich einen deutlich größeren Anteil an EU-Exporten in Drittländer im betrachteten Zeitraum auf. Als Indikator für die *Innovationskraft* der Wirtschaft wurden die Ausgaben für Forschung und Entwicklung (F&E) im Unternehmenssektor der untersuchten EU-Länder pro Einwohner zugrunde gelegt. Hier wies Dänemark im Jahr 2016 die höchsten innerbetrieblichen F&E-Ausgaben pro Einwohner auf, gefolgt von Österreich, Deutschland und dem Vereinigten Königreich, während Bulgarien auch bei diesem Kriterium deutlich zurücklag.

Die Wirtschaft eines jeden Staates wird auch durch die spezifische Verteilung von KMU und Großunternehmen oder Konzernen geprägt. Betrachtet man die *Unternehmensklassen* in den ausgewählten Ländern für den Teilbereich des verarbeitenden Gewerbes für das Jahr 2015, weisen Bulgarien, Dänemark, das Vereinigte Königreich und Österreich im Großen und Ganzen eine ähnliche Struktur der Unternehmenslandschaft auf, im Kontrast vor allem zur Schweiz, aber auch zu Deutschland. Besonders die Schweiz kennzeichnet ein niedrigerer Anteil an Kleinstunternehmen und ein überdurchschnittlicher Anteil an kleinen Unternehmen.

Tabelle 5 (siehe *nächste Seite*) enthält einen Überblick über die Werte der wirtschaftlichen Auswahlkriterien in den Vergleichsländern.

4.2 Rechtliche und sonstige Auswahlkriterien

Die rechtlichen Auswahlkriterien umfassten neben der Rechtskreis-Zugehörigkeit (Common Law oder Civil Law), der Frage nach dem Vorliegen einer kodifizierten Strafbarkeit von Wirtschaftsspionage und Konkurrenzausspähung sowie der Existenz eines nationalen Unternehmensstrafrechts und der Bandbreite der Strafrahmen[27] auch die behördliche Zuständigkeit bei Wirtschaftsspionage und Konkurrenzausspähung. Denn den betroffenen Unternehmen in Deutschland sind die unterschiedlichen Zuständigkeiten von Verfassungsschutz und Polizei oft unklar, was ein Einflussfaktor für das ebenfalls untersuchte Verhältnis von Behörden und Unternehmen sein kann. Im Gegensatz zu Deutschland kennen die ausgewählten

---

[27] Eine Übersicht über die Strafrahmen für die einschlägigen Delikte der Konkurrenzausspähung und Wirtschaftsspionage in den ausgewählten Ländern findet sich in *Kapitel 2* (Wirtschaftsspionage und Konkurrenzausspähung kennen keine Grenzen: eine vergleichende Analyse exemplarischer Fälle)*, Tabelle 9*.

Tabelle 5 Überblick über die Werte der wirtschaftlichen Kriterien

Kriterium	Indikator	Bulgarien	Dänemark	Vereinigtes Königreich	Österreich	Schweiz	Deutschland
Wirtschaftskraft	BIP 2016[1/2]	EUR 6.800	EUR 49.2000	EUR 36.600	EUR 40.800	EUR 72.500	EUR 38.100
Exportstärke	Anteil der EU-Exporte in Drittländer 2016[3]	0,4 %	1,9 %	11,1 %	2,3 %	*	28,6 %
Innovationskraft	Ausgaben für F&E pro Einwohner 2016[4]	EUR 38,4	EUR 998,3	EUR 414,8	EUR 898,4	*	EUR 764,5
Verteilung der Unternehmensklassen[5] im verarbeitenden Gewerbe (2015)[6]	Kleinstunternehmen	74,98 %	70,95 %	77 %	72,67 %	53,24 %	64,05 %
	kleine Unternehmen	18,45 %	21,23 %	17,13 %	19,8 %	35,66 %	25,8 %
	mittlere Unternehmen	5,64 %	6,46 %	4,81 %	5,65 %	9,27 %	8,03 %
	Großunternehmen	1,22 %	1,36 %	1,07 %	1,88 %	1,64 %	2,11 %

* Für die Schweiz, die kein Mitgliedsstaat der EU ist, liegen hierfür keine Daten vor..

[1] Gemessen in Tausend EUR pro Einwohner.

[2] Vgl. Eurostat, September 2019.

[3] Vgl. Eurostat, November 2017.

[4] Vgl. Eurostat, Juni 2019.

[5] Vgl. Eurostat Dezember 2017.

[6] Bei Eurostat wird die jährliche Unternehmensstatistik nach Größenklassen in verschiedene Gruppen unterteilt. Daten über die prozentualen Anteile der Unternehmensgrößen der KMU insgesamt liegen nicht vor. Die Wahl fiel auf die Gruppe des verarbeitenden Gewerbes, da jene auch Grundlage der in Modul 3 des Projektes WiSKoS durchgeführten Be-fragung „Modernisierung der Produktion“ war.

Vergleichsländer kein Trennungsgebot.[28] Während in Deutschland Staatsanwaltschaft und Polizei für die Strafverfolgung zuständig sind und der Verfassungsschutz sich, zusätzlich zur Polizei, um die Prävention im Bereich der Wirtschaftsspionage kümmert, ist z.B. in Österreich das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung auch für die Ermittlungen zuständig, sofern ein Geschäftsgeheimnis im Ausland verwertet oder verwendet wird (§ 6 Abs. 2 Nr. 4 Polizeiliches Staatsschutzgesetz).

Zu der Kategorie „sonstige Kriterien" gehörten die Frage nach einer EU-Mitgliedschaft, die geografische Lage eines Landes und etwaige nationale Besonderheiten, die im Rahmen der Landesberichte Erwähnung gefunden hatten. Durch die Aufnahme eines Nicht-EU-Mitgliedsstaates sollte ein Vergleich zwischen den Rechts- und Wirtschaftsordnungen der unterschiedlichen Mitgliedsstaaten der EU und eines anderen Landes ermöglicht werden. Die geografische Lage wurde als Kriterium aufgenommen, um etwaigen regionalen Unterschieden innerhalb der EU Rechnung zu tragen.

Tabelle 6 (siehe *nächste Seite*) gibt einen Überblick über die nationalen Merkmale der Vergleichsländer im Bereich der rechtlichen und sonstigen Kriterien.

4.3 Untersuchungsleitende Kurzcharakterisierung der Vergleichsländer

Die in *Modul 2* durchgeführte Mehrebenen-Analyse diente nicht nur dem Gewinn von Erkenntnissen zu den Phänomenen Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, sondern auch der Ermittlung von erfolgreichen Erfahrungen und Best Practices anderer europäischer Länder bezüglich der Erkennbarkeit, Prävention, Strafverfolgung und Kooperation verschiedener Akteure, um bei der Entwicklung von Maßnahmen in Deutschland darauf zurückzugreifen. Die in die Untersuchungen einbezogenen Länder sollten sich daher in einigen der genannten Punkte von Deutschland unterscheiden. Im Folgenden werden die Gründe für die Auswahl der Länder kurz zusammengefasst.

Bulgarien

Bulgarien spielt als ehemaliger Ostblockstaat in der Untersuchung eine besondere Rolle. Denn erst seit Beginn der 1990er-Jahre haben sich marktwirtschaftliche Strukturen entwickelt. Bis heute verfügt das Land über eine geringe Exportstärke und niedrige interne F&E-Ausgaben im Unternehmenssektor. Die Änderungen der wirtschaftlichen Rahmenbedingungen führten erst nach und nach zur Entstehung

---

28 Das deutsche Recht sieht eine Trennung zwischen Nachrichtendiensten und Polizei bezüglich der Aufgaben und Befugnisse sowie der Organisation und Datenverabeitung vor (vgl. *Thiel* 2020, § 3, Rn. 28).

Tabelle 6 Überblick über die rechtlichen und sonstigen Auswahlkriterien

		Bulgarien	Dänemark	Vereinigtes Königreich	Österreich	Schweiz	Deutschland
Rechtskreis		Civil Law	Civil Law	Common Law	Civil Law	Civil Law	Civil Law
kodifizierte Strafbarkeit*	Konkurrenzausspähung	ja**	ja	nein***	ja	ja	ja
	Wirtschaftsspionage	ja**	ja	nein***	ja	ja	ja
behördliche Zuständigkeit für Prävention und Strafverfolgung	Konkurrenzausspähung	je nach Delikt: • Ermittler (Teil des Gerichtssystems) • Polizei • Nachrichtendienst	Polizei	verschiedene Behörden, abhängig von der jeweiligen Straftat	Polizei/ Privatermittlungen****	Kantonspolizei	Polizei
	Wirtschaftsspionage		Polizei / Polizeilicher Nachrichtendienst		Bundesamt für Verfassungsschutz und Terrorismusbekämpfung	Nachrichtendienst des Bundes	Prävention: Polizei und Verfassungsschutz Strafverfolgung: Polizei
Unternehmensstrafrecht		nein	ja	strafrechtliche Verantwortlichkeit juristischer Personen	ja	ja	nein
EU-Mitgliedschaft		ja	ja	ja*****	ja	nein	ja
geografische Lage		Südosteuropa	Nordeuropa	Westeuropa	Zentraleuropa	Zentraleuropa	Zentraleuropa
Besonderheiten		–	gute Zusammenarbeit von Unternehmen und Behörden		enge Verbindungen zu osteuropäischen Ländern		

* Es existieren keine spezifischen Straftatbestände für Wirtschaftsspionage und Konkurrenzausspähung.

** Die Phänomenbereiche Konkurrenzausspähung und Wirtschaftsspionage wurden in Bulgarien, wo eine Strafbarkeit von der Art des verletzten Geheimnisses abhängt, anhand der deutschen Abgrenzungskriterien danach getrennt, ob der Geheimdienst eines fremden Staates oder ein Konkurrent der Täter ist.

*** Im Vereinigten Königreich werden Phänomene, die sprachlich der Konkurrenzausspähung und Wirtschaftsspionage zugeordnet werden, durch allgemeine Straftatbestände erfasst.

**** Im Fall von Privatanklagedelikten sind in Österreich allein die Betroffenen für die Ermittlungsarbeit zuständig.

***** Zum Zeitpunkt der Untersuchung.

von KMU. Die Notwendigkeit, sich mit Fragestellungen im Umgang mit sensiblen Geschäftsdaten auseinanderzusetzen, entsprechende Schutzsysteme zu entwickeln und eine strafrechtliche Verfolgung zu ermöglichen, ergab sich in Bulgarien daher entsprechend spät. Verglichen mit den anderen ausgewählten Ländern sind die angedrohten Strafen für Delikte der Wirtschaftsspionage und Konkurrenzausspähung verhältnismäßig hoch.

Dänemark

Dänemark ist ein nordeuropäischer Staat von mittlerer Wettbewerbsfähigkeit, der aber über eine hohe Wirtschaftskraft verfügt. Besonders auffällig sind die vergleichsweise hohen internen F&E-Ausgaben im Unternehmenssektor. Zudem hebt sich das Land durch vorhandene Hellfelddaten ab. In dem zugrunde liegenden Expertenbericht wird ausdrücklich auf die positive Beziehung und gute Kooperation zwischen Unternehmen und Behörden hingewiesen. Die Erforschung von Kooperationsmöglichkeiten und einer verbesserten Kommunikation zwischen diesen Bedarfsträgern war eine wesentliche Zielsetzung im Projekt WiSKoS und das ausschlaggebende Kriterium für die Einbeziehung Dänemarks.

Vereinigtes Königreich

Die KMU-Struktur des Vereinigten Königreichs zeichnet sich durch einen im Vergleich zu Deutschland höheren Anteil an Kleinstunternehmen aus (77 %; Deutschland: 64 %). Zudem ist das britische Rechtssystem im Gegensatz zu den anderen ausgewählten Ländern dem Common Law zuzuordnen. Für die Untersuchung war das Land somit von Interesse, um nachzuvollziehen, wie dort die infrage stehenden Tatphänomene im Gegensatz zu den kontinentaleuropäischen Rechtsordnungen rechtlich verfolgt werden. Darüber hinaus kennzeichnet das Vereinigte Königreich eine besondere geheimdienstliche Zuständigkeitsregelungen auf der Grundlage des Intelligence Service Act 1994 aus. So kann der britische Auslandsgeheimdienst (MI6) gem. Art. 1 Abs. 2 Intelligence Service Act 1994 u.a. im Interesse des wirtschaftlichen Wohlergehens des Landes tätig werden. Im Gegensatz dazu ist Wirtschaftsspionage durch den deutschen Bundesnachrichtendienst gem. § 6 Abs. 5 BND-Gesetz unzulässig.

Österreich

Trotz vieler Gemeinsamkeiten mit Deutschland unterscheidet sich Österreich im Hinblick auf die Strafverfolgung der Konkurrenzausspähung. Fälle der Konkurrenzausspähung sind hier grundsätzlich als Privatanklagedelikt geregelt. Zwar kann die Staatsanwaltschaft auch in Deutschland den Geschädigten in Fällen der Konkurrenzausspähung auf den Privatklageweg verweisen, sie ermittelt aber zunächst und kann das Verfahren, wenn sie ein öffentliches Interesse nicht verneint, zu Ende

führen. Für den österreichischen Privatankläger stellt das fehlende Ermittlungsverfahren durch staatliche Behörden ein strukturelles Hindernis dar. Hinzu kommt die Pflicht zur Kostenübernahme seitens des Geschädigten, was ein weiterer Grund für die geringe praktische Relevanz der Delikte im Hinblick auf die Verurteilungsraten in Österreich sein könnte. Auch die starke wirtschaftliche Verbindung des Landes zu Osteuropa war ein Auswahlkriterium.

Schweiz

Im Unterschied zu den anderen Ländern ist die Schweiz kein Mitgliedsstaat der EU, sondern der EFTA. Zwar ist die Schweiz durch bilaterale Verträge wirtschaftlich eng mit der EU verbunden, lehnte aber im Jahr 1992 einen Beitritt zum damals bestehenden Europäischen Wirtschaftsraum ab, um die wirtschaftliche Eigenständigkeit zu bewahren. Weitere Kriterien für die Auswahl der Schweiz waren die geografische Lage des Landes inmitten der EU sowie die Existenz starker Schlüsselindustrien (Chemie und Lebensmittel). Die schweizerische Unternehmenslandschaft verfügt, ähnlich wie Deutschland, über eine im Vergleich mit den anderen Ländern höhere Anzahl an mittleren Unternehmen (9,3 %) und geringere Anzahl an Kleinstunternehmen (53,2%). Besonderes Interesse galt aus der rechtsvergleichenden Perspektive dem Umstand, dass die Schweiz im Gegensatz zu Deutschland über ein (echtes) Unternehmensstrafrecht verfügt.

5. Überblick über den vorliegenden Band

Die Abfolge der Beiträge dieses Bandes orientiert sich an der Struktur des *Projektmoduls 2* und seinen Arbeitspaketen *A5–A7*.[29] Die Literatur- und Dokumentenanalyse (*A5*) widmete sich aus quantitativer wie auch qualitativer Sicht dem aktuellen Forschungs- und Literaturstand. Im Anschluss an eine quantitative bibliometrische Analyse der Datenbanken Scopus und Web of Science erfolgte eine qualitative Aufbereitung der Befunde (*Kapitel 1:* Der „typische" Spionagefall? Ergebnisse einer Literaturanalyse). Im Arbeitspaket *A6* wurden in Deutschland Daten aus 713 Strafverfahren erhoben, von denen ein Großteil zwischen 2009 und 2015[30] wegen eines Verstoßes gegen §§ 17–19 UWG geführt wurde. Die Ergebnisse wurden mit denjenigen der exemplarischen Fallstudien aus den genannten Vergleichsländern kontrastiert (*Kapitel 2:* Wirtschaftsspionage und Konkurrenzausspähung kennen keine Grenzen: Vergleichende Analyse exemplarischer Fälle). Das *Arbeitspaket A7* sah die Durchführung und Inhaltsanalyse von Experteninterviews mit Repräsentanten von KMU sowie Vertretern von Wissenschaftsorganisationen und Behörden vor. Die thematische Aufarbeitung

---

29 Siehe oben *Abschnitt 3.2.*

30 Vier Verfahren lagen außerhalb dieses Zeitraums (in den Jahren 2008 und 2016).

der Ergebnisse erfolgt in den vier sich anschließenden Kapiteln: Während sich *Kapitel 3* (Der nächste Angriff kommt bestimmt. Verbreitung von Maßnahmen zur Prävention gegen ungewollten Wissensabfluss von KMU) und *Kapitel 4* (Staatliche Präventionsangebote zum Schutz vor Wirtschaftsspionage und Konkurrenzausspähung) mit KMU und ihrem Schutz vor Wirtschaftsspionage und Konkurrenzausspähung befassen, werden in *Kapitel 5* (Gemeinsam gegen Wirtschafts- und Industriespionage – Erfolgsfaktoren für eine Kooperation zwischen staatlichen und privaten Akteuren) die Möglichkeiten der Kooperation zwischen Wirtschaftsunternehmen und staatlichen Akteuren thematisiert. Abschließend wird die Situation von Wissenschaftsorganisationen sowie deren Spionageschutz beschrieben (*Kapitel 6:* Spionage und Konkurrenzausspähung in deutschen Wissenschaftsorganisationen).

Literatur

Aebi, M.F. (2010): Methodological Issues in the Comparison of Police-Recorded Crime Rates, in: S.G. Shoham et al. (Hrsg.), International Handbook of Criminology. Boca Raton, S. 211–227.

Amelunxen, C. (1977): Spionage und Sabotage im Betrieb. Die Abwehraufgaben des Werkschutzes und ihre Rechtsgrundlagen. Heidelberg.

Aldoney Ramirez, R. (2009): Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen. Wiesbaden.

Ann, C. (2014): Geheimnisschutz – Kernaufgabe des Informationsmanagements im Unternehmen. Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 1, S. 12–16.

Bollhöfer, E. & Jäger, A. (2018): Wirtschaftsspionage und Konkurrenzausspähung: Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung; https://wiskos.de/files/pdf4/M3_Komplett_Online_neu.pdf [15.08.2019].

Bitkom (2018): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie; https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html [15.08.2019].

Bitkom (2016): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie; https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-Industrie.html [15.08.2019].

Bitkom (2016): Spezialstudie Wirtschaftsschutz; https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-Industrie.html [15.08.2019].

Bitkom (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter; https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-im-digitalen-Zeitalter.html [15.08.2019].

Carl, S. & Kilchling, M. (Hrsg.) (2018): Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin.

Corporate Trust (2014): Industriespionage 2014 – Cybergeddon der Deutschen Wirtschaft durch NSA & Co.?; https://www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2014_DE.pdf [15.08.2019].

Corporate Trust (2012): Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar; https://www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2012_FINAL.pdf [15.08.2019].

Detlinger, R. (2014): Spionage in Wirtschaft und Industrie. Identifikation und Auswahl von Tätern. Hamburg.

Eurostat (Juni 2019): Interne F&E-Ausgaben insgesamt nach Leistungssektor, Unternehmenssektor, Euro je Einwohner; https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do [15.08.2019].

Eurostat (Dezember 2017): Jährliche Unternehmensstatistiken nach Größenklasse für besondere Tätigkeitsaggregate (NACE Rev. 2), Unternehmen Anzahl, Verarbeitendes Gewerbe / Herstellung von Waren; http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=sbs_sc_sca_r2&lang=de [15.08.2019].

Eurostat (September 2019): Bruttoinlandsprodukt zu Marktpreisen, Euro pro Kopf, 2015; http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_pc&lang=de [15.08.2019].

Eurostat (November 2017): EU-Intrahandel und internationaler Handel nach Mitgliedstaat und nach SITC Produktgruppen; http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ext_lt_intratrd&lang=de [15.08.2019].

Fleischer, D. (2016): Wirtschaftsspionage. Phänomenologie, Erklärungsansätze, Handlungsoptionen. Wiesbaden.

Kahle, E. & Merkel, M. (2004): Fall- und Schadensanalyse bezüglich Know-how und Informationsverlusten in Baden-Württemberg ab 1995. Lüneburg.

Kilchling, M. & Carl, S. (2016): Wirtschaftsspionage im globalen Markt: Sind die Ermittlungsstrukturen in Deutschland noch zeitgemäß?, in: P. Zoche, S. Kaufmann & H. Arnold (Hrsg.), Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung. Berlin, S. 183–196.

Kirsch, S. (2014): Informationsschutz im Unternehmen – Prävention von Wissensabfluss und die Erkennung von Innentätern anhand derer Verhaltensmerkmale. Norderstedt.

KMPG (2018): Licht ins Dunkel bringen. Wirtschaftskriminalität in Deutschland 2018; https://home.kpmg/de/de/home/newsroom/press-releases/2018/07/wirtschaftskriminalitaet-in-deutschland-2018.html [15.08.2019].

KMPG (2016): Tatort Deutschland. Wirtschaftskriminalität 2016; https://assets.kpmg/content/dam/kpmg/pdf/2016/07/wirtschaftskriminalitaet-2016-2-KPMG.pdf [15.08.2019].

KPMG (2014): Wirtschaftskriminalität in Deutschland; https://assets.kpmg/content/dam/kpmg/pdf/2014/12/Wikri-Studie_2014_sec.pdf [15.08.2019].

KPMG (2012): Wirtschaftskriminalität in Deutschland; https://home.kpmg/de/de/home/themen.html [15.08.2019].

KPMG (2010a): e-Crime-Studie 2010 – Computerkriminalität in der deutschen Wirtschaft; www.kpmg.de/docs/20100810_kpmg_e-crime.pdf [15.08.2019].

KPMG (2010b): Wirtschaftskriminalität in Deutschland – Fokus: Mittelstand; www.desa-berlin.de/documents/StudieKPMG-2009-20091220_Wirtschaftskriminalitaet.pdf [15.08.2019].

Liebl, K. & Woll, H. (1987): Betriebsspionage: Begehungsformen, Schutzmaßnahmen, Rechtsfragen. Ingelheim.

Lux, C. & Peske, T. (2002): Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie. Wiesbaden.

Metzler, R. (1990): Konsequenzen neuartiger Erscheinungsformen des wirtschaftlichen Wettbewerbes für den strafrechtlichen Schutz von Geschäfts- und Betriebsgeheimnissen im Rahmen der §§ 17ff. UWG. München.

Pohl, H. (2008): Zero-Day and Less-than-Zero-Day Vulnerabilities and Exploits, in: C. Zacharias et al. (Hrsg.), Forschungsspitzen und Spitzenforschung. Heidelberg.

PwC (2017): Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2017; https://www.pwc.de/de/finanzdienstleistungen/studie-wirtschaftskriminalitaet-versicherungen-2017.pdf [15.08.2019].

PwC (2016): Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016; www.pwc.de/de/risk/studie-wirtschaftskriminalitaet-2016.pdf [15.08.2019].

PwC (2014): Wirtschaftskriminalität und Compliance – Handel und Konsumgüterindustrie 2014; www.pwc.de/de/handel-und-konsumguter/assets/pwc-studie-wirki-retail-und-consumer-2015.pdf [15.08.2019].

PwC (2012): Wirtschaftskriminalität – Versicherungsbranche; www.pwc.de/de/publikationen/paid_pubs/pwc_studie_wirtschaftskriminalitaet_versicherungen_2012.pdf [15.08.2019].

Result Group & F.A.Z.-Institut (2014): Kriminelle Risiken im Mittelstand – Gefahren, Schäden und Prävention. Frankfurt am Main.

Röder, N. (2011): Industriespionage. Risikofaktor Mensch; https://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/298 [15.08.2019].

Schaaf, C. (2009): Industriespionage. Der große Angriff auf den Mittelstand. Stuttgart.

Scherf, A. (2013): Gefahren der Wirtschaftsspionage und Auswirkungen auf das IT-Projektmanagement; http://www.pst.ifi.lmu.de/Lehre/wise-12-13/jur-pm/ausarbeitung-zum-vortrag-am-08.01.2013-a.-scherf [09.10.2015].

Sendzik, B. (2014): Der „Datendiebstahl". Hamburg.

Sicherheitsforum Baden-Württemberg (2010): SiFo-Studie 2009/2010. Know-how-Schutz in Baden-Württemberg. Stuttgart.

Stieber, B. (2018): Strategien gegen Spione; www.mpg.de/12008528/W005_Kultur_Gesellschaft_072-077.pdf [15.08.2019].

Thiel, M. (2020): Polizei- und Ordnungsrecht. Baden-Baden.

Wagner, P. (2014): Schutz vor Industriespionage. Analyse, Prävention und Abwehr des irregulären Verlustes von Know-how in Unternehmen. Hamburg.

Zwickl, J. (2015): Industriespionage im deutschen Mittelstand. Wie schützt man Know-how wirkungsvoll? Norderstedt.

Synopse von § 23 GeschGehG und §§ 17–19 UWG

§ 23 GeschGehG (in Kraft getreten am 26.04.2019)	**§§ 17–19 UWG** (weggefallen seit Inkrafttreten des GeschGehG)
§ 23 Verletzung von Geschäftsgeheimnissen (Abs. 1–8) 1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, 1. entgegen § 4[1] Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt, 2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder 3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.	**§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen (Abs. 1 u. 2)** 1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. 2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, 1. sich ein Geschäfts- oder Betriebsgeheimnis durch a. Anwendung technischer Mittel, b. Herstellung einer verkörperten Wiedergabe des Geheimnisses oder c. Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder […]

[1] § 4 GeschGehG (aufgeführt werden im Folgenden nur § 4 Abs. 1 und Abs. 2, auf die in § 23 GeschGehG verwiesen wird)

1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch
   1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
   2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer
   1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
      a. Nummer 1 oder
      b. Nummer 2 erlangt hat,
   2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
   3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.

2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.	2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, […] 2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt..
3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.	**§ 18 Verwertung von Vorlagen (Abs. 1)** 1) Wer die ihm im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte, zu Zwecken des Wettbewerbs oder aus Eigennutz unbefugt verwertet oder jemandem mitteilt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer 1. in den Fällen des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt, 2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder 3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.	**§ 17 Abs. 4** 4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe**.** Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter 1. gewerbsmäßig handelt, 2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder 3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.
5) Der Versuch ist strafbar.	**§ 17 Abs. 3; § 18 Abs. 2** Der Versuch ist strafbar.
6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.[2]	–

[2] Anmerkung der Verf.: Der neu geschaffene Strafbarkeitsausschluss für Beihilfehandlungen nach dem Vorbild des § 353b Abs. 3a StGB soll dem investigativen Journalismus Rechtssicherheit geben.

§ 23 GeschGehG	§§ 17–19 UWG
	§ 17 Abs. 6; § 18 Abs. 4; § 19 Abs. 5
7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.	§ 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.
	§ 19 Verleiten und Erbieten zum Verrat (Abs. 1–3)
Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.[3]	1) Wer zu Zwecken des Wettbewerbs oder aus Eigennutz jemanden zu bestimmen versucht, eine Straftat nach § 17 oder § 18 zu begehen oder zu einer solchen Straftat anzustiften, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. 2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs oder aus Eigennutz sich bereit erklärt oder das Erbieten eines anderen annimmt oder mit einem anderen verabredet, eine Straftat nach § 17 oder § 18 zu begehen oder zu ihr anzustiften. 3) § 31 des Strafgesetzbuches gilt entsprechend.
	§ 17 Abs. 5, § 18 Abs. 3, § 19 Abs. 4
8) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.	Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

[3] Anmerkung der Verf.: Die Strafbarkeit der versuchten Anstiftung und der Anstiftung, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt, trägt dem Gefährdungspotenzial von derartigen Vorbereitungshandlungen Rechnung; vgl. Deutscher Bundestag 2018, Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidrixger Nutzung und Offenlegung, S. 41; https://dipbt.bundestag.de/dip21/btd/19/047/1904724.pdf [15.08.2019].

Der „typische“ Spionagefall?
Ergebnisse einer Literaturanalyse

Elisa Wallwaey & Lisa Waldheim

1. Einleitung

Im vorliegenden Kapitel werden die zentralen Befunde der aktuellen wissenschaftlichen wie außerwissenschaftlichen Literatur zu Wirtschaftsspionage und Konkurrenzausspähung vorgestellt. An eine knappe Erläuterung des triangulären methodischen Vorgehens anschließend, werden die wichtigsten Ergebnisse dargestellt. Im Fokus steht dabei die Frage, ob typische Fallkonstellationen von Wirtschaftsspionage und Konkurrenzausspähung identifiziert werden können.

2. Methodisches Vorgehen

Um sowohl eine quantitative als auch eine qualitative Analyse des aktuellen internationalen Forschungsstands zum Themenbereich Wirtschaftsspionage und Konkurrenzausspähung vornehmen zu können, kamen quantitative und qualitative Methoden gleichermaßen zum Einsatz. Dabei wurde eine quantitative Bibliometrieanalyse,[1] gestützt auf die wissenschaftlichen Datenbanken Scopus und Web of Science (WoS), mit einer qualitativen Literaturanalyse mittels der Software MAXQDA kombiniert. Wird derselbe Forschungsgegenstand aus unterschiedlichen Blickwinkeln und unter Nutzung verschiedener Methoden analysiert, können diese einander ergänzen und ermöglichen die Entwicklung eines detaillierteren Gesamtbilds des Forschungsgegenstands.[2]

3. Ergebnisse

Unabhängig vom geografischen Fokus mangelt es an aktuellen wissenschaftlichen Publikationen zu Phänomenen der Wirtschaftsspionage und Konkurrenzausspä-

---

1 Aktuelle Informationen zu bibliometrischen Verfahren enthält u.a. *Ball* 2015.

2 Nähere Informationen zur Methodentriangulation finden sich z.B. bei *Bortz & Döring* 2006, pp. 365–366, 743.

hung,[3] sodass Kenntnisse, sofern sie nicht gänzlich fehlen, größtenteils veraltet sind. Erst seit wenigen Jahren kommt Ereignissen, die der Wirtschaftsspionage oder Konkurrenzausspähung zuzuordnen sind, größere Aufmerksamkeit sowohl aus der wissenschaftlichen wie auch der außerwissenschaftlichen Forschung zu.[4]

3.1 Statistische Kennzahlen und Analysekategorien

Die quantitative Bibliometrieanalyse erzielte für den untersuchten Zeitraum 2000 bis 2015 insgesamt 3.411 Literaturfunde in den beiden Datenbanken (Scopus: 2.051; WoS: 1.360), die mit Rechercheergebnissen aus einer themenbezogenen Literaturdatenbank, die das Projektteam des Max-Planck-Instituts für ausländisches und internationales Strafrecht zu Projektbeginn erstellte und anschließend laufend aktualisierte, ergänzt wurden. Bereinigt um Duplikate verblieben ca. 3.000 Artikel, die als Basis der qualitativen Analyse herangezogen wurden. Durch einen weiteren Selektionsschritt konnte die Literaturbasis auf 128 Quellen eingegrenzt werden. Diese hohe Ausschlussquote resultierte aus vier Sachverhalten:

- Die Begrenzung des geografischen Zielgebiets des Projekts auf die Europäische Union (EU) führte zum Ausschluss von Quellen aus anderen Teilen der Welt.
- Durch die Eingrenzung der verwendeten Suchbegriffe konnten relevante Literaturfunde identifiziert werden, die dem geografischen Raum des Projekts entstammen.
- Damit in Verbindung stehend, konnte eine große Bandbreite an Quellen identifiziert werden, von denen sich viele im Rahmen der qualitativen Analyse als im Projektkontext nicht relevant erwiesen.
- Die thematisch passenden Quellen sind i.d.R. veraltet und somit nur eingeschränkt nutzbar.

Zu Analysezwecken wurden fünf Kategorien gebildet:

- Branchenzugehörigkeit,
- Tat- und Täterstrukturen,
- Besonderheiten von kleinen und mittleren Unternehmen (KMU),
- Handhabung,
- Prävention.

---

3 Zur Begründung dieses Mangels vgl. *Abschnitt 3.1.*

4 Siehe z.B. *Bazzi* 2015; Bitkom 2016; CT 2014; *Fleischer* 2016; *Hofer & Weiß* 2016; Initiative Wirtschaftsschutz 2016; *Kasper* 2014; *Kirsch* 2014; *Landerer* 2014; PwC 2016; *Sule* 2006.

Diese Kategorien werden herangezogen, um sich der Antwort auf eine Frage zu nähern: Gibt es den typischen Spionagefall?

3.2 Zentrale Akteure

Als zentrale Akteure der Wirtschaftsspionage oder Konkurrenzausspähung werden regelmäßig Täter wie auch Opfer genannt.[5] Dabei kann es sich sowohl um natürliche wie auch um juristische Personen handeln.

3.2.1 Täter und Tatmotive

Unabhängig davon, ob es sich in einem konkreten Fall um Wirtschaftsspionage oder Konkurrenzausspähung handelt, können unternehmensinterne oder -externe Täter aktiv geworden sein.[6] Interne Täter sind vor allem die eigenen Mitarbeiter. Aber auch Zulieferer oder Kunden können dieser Tätergruppe zugeordnet werden, da eine vertraglich geregelte (Geschäfts-)Beziehung zum Opfer besteht. Unabhängig von der Position im Unternehmen, kann jeder – vom Topmanager bis hin zum Hausmeister oder zur aus dem Betrieb ausgegliederten und außerhalb der regulären Betriebszeiten arbeitenden Putzfrau – zum Täter werden.[7]

Externe Täter können beispielsweise Agenten eines ausländischen Geheimdienstes, Diplomaten oder Konkurrenten im Wettbewerb sein.[8] Bedingt durch den zunehmenden Umfang von Cyberspionage, sollten in diesem Kontext auch Angriffe über das Internet nicht außer Acht gelassen werden.[9]

Die idealtypische Unterteilung in interne und externe Täter liegt in der Realität allerdings häufig nicht vor. Beispielsweise werben Externe einen Mitarbeiter des Zielunternehmens an bzw. ab, sodass es zu einer Vermischung der beiden Tätergruppen kommt.[10]

---

5 Vgl. *Wolff* 2009, S. 39–76.

6 Vgl. beispielsweise BfV 2016; *Fleischer* 2016, S. 8–13; *Zwickl* 2015, S. 7–9; *Kirsch* 2014, S. 88–91; *Wagner* 2014, S. 20–22; SiFo BW 2010, S. 22; *Merkel & Kahle* 2007, S. 12; SiFo BW 2005, S. 19–20; *Nathusius* 2001, S. 60–64.

7 Als in der Literatur häufig genannter Fall von Konkurrenzausspähung kann beispielsweise jener des Managers *José Ignacio López* genannt werden (vgl. *Schaaf* 2009, S. 18; *Röder* 2011, S. 8, 27; *Wolff* 2009, S. 55–56). Ein weiteres typisches Beispiel für die Involvierung von Mitarbeitern findet sich in SiFo 2005, S. 19–21.

8 Vgl. *Lux & Peske* 2002, S. 53.

9 Vgl. BfV 2017, S. 259–266; BfV 2014b, S. 25; SiFo BW 2005, S. 39–41. Fallbeispiele aus dem Jahr 2016 finden sich in HAZ 2016 und N-TV 2016. Zu den durch Cyberspionage entstehenden Kosten siehe *Engels* 2017, S. 12–21.

10 Vgl. *Kasper* 2014, S. 58, 62; *Wagner* 2014, S. 22.

Jenseits eines finanziellen/materiellen Motivs können Innentäter durch die Unternehmenskultur im weitesten Sinne beeinflusst werden. Diese umfasst die Bindung an das Unternehmen wie auch die Zufriedenheit mit den Arbeitsaufgaben und der Stellung im Unternehmen sowie den Kontakt zu Kollegen. Nach *Lux* und *Peske* sollte die persönliche Situation (z.B. familiäre Probleme, Geldsorgen o.Ä.) ebenfalls als Einflussfaktor miteinbezogen werden.[11] Auch Erpressung oder Bedrohung durch einen Nachrichtendienst lässt sich als Einflussfaktor ausmachen.[12]

Wirtschaftsspionage und Konkurrenzausspähung zeichnen sich durch unterschiedliche Zieldimensionen aus. Während der Konkurrenzausspähung häufig ein finanzielles/materielles Motiv seitens der Wettbewerber zugrunde liegt, zeichnet sich die staatlich (an-)geleitete Wirtschaftsspionage durch das Ziel aus, die eigene Wirtschaft als Ganzes zu fördern. Das Erkenntnisinteresse wird dabei durch den Entwicklungsstand der jeweiligen nationalen Wirtschaft bedingt.[13] Einige Staaten, wie beispielsweise Russland oder China, werden besonders häufig der Wirtschaftsspionage bezichtigt.[14] Über das Ausmaß, in dem sogenannte *friendly spies,*[15] wie beispielsweise Frankreich, Großbritannien oder die USA, Spionage betreiben, lässt sich derweil nur spekulieren.[16] Mögliche Indizien dafür sind aber beispielsweise die Existenz der École *de guerre* économique (Wirtschaftskriegsschule) in Paris[17] oder die Presseberichterstattung über vermutete Fälle von Spionage unter Beteiligung der genannten Länder.[18]

3.2.2 Opfer

Die Opfer von Wirtschaftsspionage und Konkurrenzausspähung sind Unternehmen. Auch wenn sich sowohl Konzerne als auch Großunternehmen unter den Opfern befinden, sehen einschlägige wissenschaftliche und außerwissenschaftli-

---

11 Vgl. *Lux & Peske* 2002, S. 87–88.

12 Vgl. *Lux & Peske* 2002, S. 87.

13 Ist die Wirtschaft des Spionage betreibenden Staates im Vergleich zu anderen Ländern rückständig, verfolgen dessen Bemühungen das Ziel, in den Besitz von wirtschaftlichem und/oder technischem Know-how zu gelangen. Geht die Spionage jedoch von wirtschaftlich hoch entwickelten Staaten aus, zielt sie i.d.R. auf finanzielle oder wirtschaftliche Strategien (vgl. *Kurek* 2008, S. 42–43).

14 Vgl. BfV 2017, S. 258, 266–274; BfV 2008, S. 5–8; *Schaaf* 2009, S. 39–47.

15 Dieses Konzept wird z.B. ausführlich behandelt in *Schweizer* 1993.

16 Vgl. *Schaaf* 2009, S. 34–39, 47–51; *Nathusius* 2001, S. 20.

17 Vgl. www.ege.fr/ [27.06.2017].

18 Vgl. *Ashelm & Jansen* 2017 (o.S.); *O'Shea* 2016 (o.S.); *Buckley* 2015 (o.S.); *Carnegy* 2013 (o.S.); *Helm, Boffey & Hopkins* 2013 (o.S.); *Rayment* 2009 (o.S.); *Borger* 2008 (o.S.).

che Literaturquellen nach wie vor KMU in Gefahr.[19] Viktimisierte Unternehmen lassen sich anhand unterschiedlicher Kategorien klassifizieren. Beispielsweise können Unternehmensgröße oder Branchenzugehörigkeit (oder eine Kombination aus beidem) herangezogen werden. Für die Klassifikation der Unternehmensgröße bietet sich eine Kombination von Umsatz und Mitarbeiterzahl an. Folgend der EU-Empfehlung 2003/361 zur Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, werden die in *Tabelle 1* genannten Definitionskriterien angelegt.

*Tabelle 1 Definitionskriterien nach EU-Empfehlung 2003/361**

Unternehmensgröße	kleinst	klein	mittel
Beschäftigtenzahl	bis 9	10 bis 49	50 bis 249
Umsatz EUR/Jahr	bis 2 Mio.	bis 10 Mio.	bis 50 Mio.

* Die vollständige Kommissionsempfehlung kann unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:de:PDF [09.06.2017] eingesehen werden.

Obwohl KMU im Gegensatz zu Großunternehmen und Konzernen in der Regel eine weniger ausgeprägte Sicherheitsstruktur[20] und damit einhergehend ein höheres Viktimisierungsrisiko aufweisen, kommt dieser Unternehmensgruppe in den untersuchten Publikationen und Studien nicht die angemessene Aufmerksamkeit zu. Im Gegensatz zu Großunternehmen und Konzernen, die im Regelfall über ein umfassendes Sicherheitsmanagement, eine eigene Compliance-Abteilung sowie ein angemessenes Budget für Präventionsmaßnahmen verfügen, ist der Schutz bei KMU häufig verbesserungswürdig.[21] Diese Problematik wird zusätzlich durch eine überdurchschnittliche Innovationskraft der Unternehmen befeuert,[22] da innovative Forschungs- und Entwicklungsabteilungen ein beliebtes Spionageziel sind. Weiterhin können KMU in einem Nischensegment Weltmarktführer und als solche *hidden champions*[23] ein begehrenswertes Ziel für staatlich gelenkte wie auch für von Konkurrenzunternehmen gesteuerte Spionageangriffe sein.[24]

---

19 BfV 2014c, S. 6; *Kirsch* 2014, S. 48–49; CT 2012, S. 14; Spectaris 2011. Weitere Belege finden sich auch in der Berichterstattung durch die Presse. Zum Beispiel Focus Money 2013 (o.S.); *Evers* 2012 (o.S.); N-TV 2010 (o.S.).

20 Vgl. Result Group 2014, S. 6–9.

21 Vgl. *Lee* 2014, S. 2.

22 Vgl. *Engels* 2017, S. 4

23 Vgl. *Simon* 2007, S. 15.

24 Vgl. *Zwickl* 2015, S. 46.

Unabhängig von der Unternehmensgröße werden in der Literatur Branchen genannt, die als begehrte Spionageziele klassifiziert werden, sich jedoch nach unseren Analyseergebnissen[25] als nahezu irrelevant erweisen:

- Informations- und Kommunikationstechnik,[26]
- Automobil- und Maschinenbau,[27]
- Luft- und Raumfahrttechnik,[28]
- Biotechnologie und Medizin,[29]
- Chemie- und Pharmabranche,[30]
- Optoelektronik,[31]

Anhand der analysierten Quellen lassen sich neben den üblichen Tätern der Wirtschaftsspionage[32] auch einige regelmäßig viktimisierte Staaten nennen. Diese sind vorrangig Deutschland und die USA, gefolgt von Großbritannien, Schweden und Südkorea.[33]

3.3 Modi Operandi

Die Modi Operandi von Wirtschaftsspionage und Konkurrenzausspähung sind nahezu identisch,[34] weshalb sie im Folgenden gemeinsam dargestellt werden.

3.3.1 HUMINT

HUMINT steht als Abkürzung für Human Source Intelligence, also von Menschen betriebene Aufklärung.[35] Der erste Schritt besteht in der Identifikation und Anwerbung einer geeigneten Person, die die Agententätigkeit ausführen soll. Da

---

25 Erläuterungen zu den in WiSKoS als bedroht identifizierten Branchen finden sich in *Kapitel 3:* Wirtschaftsspionage und Konkurrenzausspähung kennen keine Grenzen: eine vergleichende Analyse exemplarischer Fälle

26 Vgl. *Röder* 2011, S. 13; *Kurek* 2007, S. 43; *Lux & Peske* 2002, S. 71.

27 Vgl. *Röder* 2011, S. 12; *Nathusius* 2001, S. 62.

28 Vgl. BfV 2014a, S. 23; Der Spiegel 2014; *Röder* 2011; S. 13; *Lux & Peske* 2002, S. 71.

29 Vgl. *Lux & Peske* 2002, S. 72.

30 Vgl. *Röder* 2011; *Lux & Peske* 2002, S. 192.

31 Vgl. *Lux & Peske* 2002, S. 71.

32 Besonders häufig werden Russland und China genannt (vgl. z.B. *Thorleuchter & van den Poel* 2013, S. 3433).

33 Vgl. BfV 2008, S. 4; *Crane* 2005, S. 238; zu Spionageangriffen auf südkoreanische Unternehmen siehe *Lee* 2015.

34 Vgl. *Lux & Peske* 2002, S. 83.

35 Vgl. *Zwickl* 2015, S. 54–57; *Wagner* 2014, S. 53–54.

Mitarbeiter des Zielunternehmens im Regelfall wissen, welche Informationen die „Kronjuwelen“ des Betriebs sind, und auf diese leichter zugreifen und sie an sich bringen können als Externe, wird die Anwerbung einer solchen HUMINT-Quelle angestrebt. Neben den Unternehmensmitarbeitern kommen auch Gastwissenschaftler oder Praktikanten aus dem eigenen Land zur Anwerbung infrage. Im Anschluss an eine gegebenenfalls notwendige Ausbildung oder Schulung führt der Agent unter Leitung durch einen Agentenführer den Spionageauftrag aus. Auch eine Tarnung „hauptberuflicher“ Agenten als potenzielle Kunden, Zulieferer etc. ist denkbar. [36]

Die Anwerbung erfolgt häufig über das sogenannte Social Engineering, bei dem im Anschluss an eine unverdächtige Kontaktaufnahme mit der Zielperson Informationen von dieser abgeschöpft werden.[37]

3.3.2 TECHINT

Die technische Aufklärung, kurz TECHINT, beschreibt die Informationsgewinnung unter Nutzung technischer Hilfsmittel.[38] Dazu gehören beispielsweise das Abhören und Aufzeichnen von Gesprächen, das Ausspähen von Daten, das Anfertigen und Auswerten von Fotos und Videos sowie Hacking.[39] Sie gewinnt durch die fortschreitende Digitalisierung aller Lebens- und Arbeitsbereiche zunehmend an Relevanz,[40] und es lässt sich festhalten, dass „die technischen Möglichkeiten der Informationsgewinnung […] vielfältig [sind und …] nicht nur Nachrichtendiensten, sondern in zunehmendem Maße auch Konkurrenzunternehmen zu relativ geringen Preisen zur Verfügung [stehen]“.[41]

Die Nutzung von technischen Methoden bedarf menschlicher Hilfe, sodass eine enge Verknüpfung zwischen TECHINT und HUMINT besteht.

3.3.3 OSINT

Von den beiden zuvor genannten Kategorien abzugrenzen ist die Abschöpfung offen zugänglicher Quellen, die sogenannte Open Source Intelligence (OSINT). Auch als Competitive Intelligence bekannt zeichnet sie sich dadurch aus, dass kein strafbares

---

36 Vgl. *Fleischer* 2016, S.35–42; *Zwickl* 2015, S. 54–57; *Röder* 2011, S.16–19; *Lux & Peske* 2002, S. 86, 88.

37 Nähere Informationen zu Social Engineering finden sich z.B. in *Fleischer* 2016, S. 36–42, oder im Informationsvideo „Im Visier“, siehe VBS (o.D.)..

38 Vgl. *Zwickl* 2015, S. 53–54; *Wagner* 2014, S. 55–56.

39 Weitere TECHINT-Methoden finden sich bei *Röder* 2011, S. 19–21. Für weitere Informationen empfehlen sich auch *Engels* 2017 oder Bitkom 2016.

40 Vgl. *Ashelm & Jansen* 2017 (o.S.); *Bartsch & Frey* 2017, S. 18–19; *Perlroth, Scott & Frenkel* 2017 (o.S.); *Preuss* 2016 (o.S.).

41 *Röder* 2011, S. 19.

Verhalten vorliegt. Der OSINT stehen mannigfaltige Methoden wie beispielsweise die Auswertung von Zeitungsartikeln, Pressemitteilungen, Nachrichtenbeiträgen oder dem Webauftritt des Zielunternehmens sowie Besuche des Werksgeländes oder von Messeständen zur Verfügung.[42]

Trotz des Einsatzes legaler Methoden der Informationsgewinnung ist der Übergang von OSINT zu HUMINT oder TECHINT fließend, da die Grenzen legaler Informationsbeschaffung verschwimmen.

3.4 Prävention

Ein erheblicher Anteil (40 %) der analysierten Quellen lässt sich der Oberkategorie *Prävention* zuordnen; diese kann wiederum unterteilt werden in technische, organisatorische und personelle Prävention. Auch wenn die übergeordnete Präventionsempfehlung die Entwicklung einer ganzheitlichen Sicherheitsstruktur mit Notfallmanagement ist, [43] werden im Folgenden die häufig empfohlenen Präventionsmaßnahmen idealtypisch in die drei zuvor genannten Unterkategorien eingeordnet. Vorab sei noch darauf hingewiesen, dass die Voraussetzungen eines jeden Sicherheits- und Informationsschutzkonzeptes eine Risikoanalyse und die Identifikation des essenziellen Know-hows sind.[44]

3.4.1 Personelle Prävention

Im Fokus der personellen Prävention steht der Mitarbeiter.[45] Die regelmäßig genannten Präventionsmaßnahmen sind:

- Sensibilisierung der Mitarbeiter (z.B. durch Schulungen),[46]
- Sicherheitsüberprüfung bei Neuanstellungen,[47]
- Vertraglich geregelte Verschwiegenheitserklärungen.[48]

Dennoch sollte nicht nur der Mitarbeiter im Fokus stehen, denn Akzeptanz für Präventionsmaßnahmen durch das Personal wird gefördert, wenn Manager mit gutem Beispiel vorangehen.[49]

---

42 Vgl. *Röder* 2011, S. 22–23; *Lux & Peske* 2002, S. 97–99.

43 Vgl. Bitkom 2016, S. 47; *Wagner* 2014, S. 59.

44 Vgl. *Fleischer* 2016, S. 107–110; *Kirsch* 2014, S. 98, 108; *Wagner* 2014, S. 60–63; *Schaaf* 2009, S. 173–175.

45 Vgl. Bitkom 2016, S. 58; *Wagner* 2014, S. 56–66.

46 Vgl. *Fleischer* 2016, S. 127–130; *Kirsch* 2014, S. 134.

47 Vgl. *Fleischer* 2016, S. 111–114; *Kirsch* 2014, S. 121–124.

48 Vgl. *Kirsch* 2014, S. 130.

49 Vgl. *Kirsch* 2014, S. 103.

3.4.2 Organisatorische Prävention

Die organisatorische Prävention beginnt bereits mit der Wahl von Unternehmensstandorten und bautechnischen Überlegungen.[50] Aber auch die Regelung der Beziehung zu Externen wie Kunden oder Zulieferern kann diesem Bereich zugeordnet werden.

Als beispielhafte Maßnahmen können genannt werden:

- Planung der Gebäudesicherheit, z.B. Abhör- und Sichtschutz,[51]
- Vertragliche Regelung der Beziehung zu Kunden oder Zulieferern,[52]
- Schaffung eines positiven Betriebsklimas,[53]
- Einführung eines betriebsinternen Meldesystems[54] und einer Clean-Desk-Policy.[55]

3.4.3 Technische Prävention

Maßnahmen der technischen Prävention sind vielfältig. Beispielhaft seien hier genannt:

- Zugangskontrollen, z.B. mittels Schlüsselkarten oder biometrischen Verfahren,[56]
- Regelung von Zugriffsrechten nach dem Need-to-know-Prinzip,[57]
- Verschlüsselung von Geräten und E-Mails,[58]
- Installation und Wartung von Überwachungskameras und Alarmanlagen,[59]
- regelmäßige Updates der verwendeten Softwarepakete und des Betriebssystems,[60]
- Entziehen von Zugriffsrechten und Rückforderung ausgehändigter Hardware beim Ausscheiden eines Mitarbeiters.[61]

---

50 Vgl. *Warnecke* 2010, S. 307–308; *Schaaf* 2009, S.127–138.

51 Vgl. *Kirsch* 2014, S. 115; *Röder* 2011, S. 61.

52 Vgl. *Merkel & Kahle* 2008, S. 13–14.

53 Vgl. *Kirsch* 2014, S. 120–121.

54 Vgl. *Kirsch* 2014, S. 148.

55 Vgl. *Zwickl* 2015, S. 47.

56 Vgl. *Fleischer* 2016, S. 133; *Kirsch* 2014, S. 116; *Wagner* 2014, S. 66–68.

57 Vgl. *Kirsch* 2014, S. 116, 118, 142.

58 Vgl. *Maurer* 2008, S. 69–70.

59 Vgl. *Kirsch* 2014, S. 116–119.

60 Vgl. *Fleischer* 2016, S. 123.

61 Vgl. *Röder* 2011, S. 55. Empfehlungen für geregelten Ablauf beim Ausscheiden von Mitarbeitern finden sich unter BSI (o.D.).

3.5 Kooperation

Über die gesamte Bandbreite der analysierten Literatur zeigt sich eine außerordentlich niedrige Anzeigebereitschaft seitens der viktimisierten Unternehmen. Dabei werden vielfältige Aspekte als Hemmnis zur Kooperation mit den zuständigen Behörden genannt, die sich zu drei Bereichen zusammenfassen lassen:

- Befürchtete materielle und immaterielle Folgeschäden,[62]
- Befürchteter weiterer Know-how-Abfluss während des Prozesses,[63]
- Mangelnde Kenntnis behördlicher Zuständigkeiten.[64]

Eine Verbesserung der Anzeige- und Kooperationsbereitschaft seitens der Unternehmen sollte für die Zukunft angestrebt und die Hemmnisse und Bedenken abgebaut werden.

4. Fazit

In diesem Kapitel wurden die Ergebnisse einer triangulären Literaturstudie zusammengefasst, um sich der Frage zu nähern, ob es einen typischen Spionagefall gibt. Trotz etlicher Komponenten, die bei Fällen von Wirtschaftsspionage und Konkurrenzausspähung (nahezu) identisch sind, muss das Fazit gezogen werden, dass typische Fälle nur schwer zu identifizieren sind. Es können jedoch generelle Fallcharakteristika ausgemacht werden, die das Bild prägen, u.a.:

- das Tatmotiv ist oftmals finanzieller/materieller Natur,
- Cyberspionage stellt eine zunehmende Gefahr dar,
- eine Viktimisierung ist durch Unternehmen nur schwer zu erkennen,
- gleichzeitig ist die Anzeigebereitschaft sehr gering,
- behördliche Zuständigkeiten sind für betroffene Unternehmen häufig unklar.

Diese gehäuft auftretenden Charakteristika können als Ausgangspunkt für die Entwicklung neuer Maßnahmen der Prävention wie auch der Repression dienen.

---

62 Für den Bereich der Cyberspionage vgl. *Engels* 2017, S. 12–16. Weitere Informationen finden sich beispielsweise in *Merkel & Kahle* 2008, S. 8–18.

63 Vgl. *Kasper* 2014, S. 80.

64 Vgl. *Kasper* 2014, S. 75.

Literatur

Ashelm, M. & Jansen, J. (2017): Cyberspione nehmen deutsche Mittelständler ins Visier. Frankfurter Allgemeine, 07.06.2017; www.faz.net/aktuell/wirtschaft/unternehmen/cyber-spione-nehmen-mittelstaendler-ins-visier-15051022.html [26.06.2017].

Ball, R. (2015): Bibliometrie im Zeitalter von Open und Big Data – das Ende des klassischen Indikatorenkanons. Wiesbaden.

Bartsch, M. & Frey, S. (2017): Cyberstrategien für Unternehmen und Behörden – Maßnahmen zur Erhöhung der Cyberresilienz. Wiesbaden.

Bazzi, C. (2015): Internationale Wirtschaftsspionage. Eine Analyse des strafrechtlichen Abwehrdispositivs der Schweiz. Züricher Studien zum Strafrecht 81. Zürich.

BfV, siehe Bundesamt für Verfassungsschutz.

Bitkom, siehe Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Borger, J. (2008): British trade official accused of espionage by Russians. The Guardian, 11.06.2008; www.theguardian.com/politics/2008/jul/11/british.russian.espionage [27.06.2017].

Bortz, J. & Döring, N. (2006): Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. 4., überarb. Aufl. Heidelberg.

BSI, siehe Bundesamt Sicherheit in der Informationstechnik.

Buckley, C. (2015): China Formally Arrests U.S. Citizen Accused of Spying. The New York Times, 22.09.2015; www.nytimes.com/2015/09/23/world/asia/china-detains-us-citizen-sandy-phan-gillis.html [27.06.2017].

Bundesamt für Sicherheit in der Informationstechnik (o.D.): Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern, Stand 2013; www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03006.html [26.06.2017]; zit.: BSI (o. D.)

Bundesamt für Verfassungsschutz (2017): Verfassungsschutzbericht 2017; www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2017/vsb-2016.pdf?__blob=publicationFile [05.07.2017]; zit.: BfV 2017.

Bundesamt für Verfassungsschutz (2016): Flyer „Gefahr durch Innentäter"; www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-geheim-sabotage-und-wirtschaftsschutz/faltblatt-2016-03-sicherheitsluecke-mensch [09.06.2017]; zit.: BfV 2016.

Bundesamt für Verfassungsschutz (2014a): Elektronische Angriffe mit nachrichtendienstlichem Hintergrund; www.verfassungsschutz.de/de/download-manager/_broschuere-2014-07-elektronische-angriffe-mit-nachrichtendienstlichem-hintergrund.pdf [12.06.2017]; zit.: BfV 2014a.

Bundesamt für Verfassungsschutz (2014b): Spionage – Ihre Ziele, ihre Methoden; www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2014-05-spionage-ihre-ziele-ihre-methoden [13.06.2017]; zit.: BfV 2014b.

Bundesamt für Verfassungsschutz (2014c): Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung; www.verfassungsschutz.de/de/download-manager/_broschuere-2014-07-wirtschaftsspionage.pdf [05.07.2017]; zit.: BfV 2014c.

Bundesamt für Verfassungsschutz (2008): Spionage gegen Deutschland – Aktuelle Entwicklungen. Köln; zit.: BfV 2008.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2016): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie; www.bitkom.

org/noindex/Publikationen/2016/Studien/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-Industrie/161110-Studie-Wirtschaftsschutz.pdf [02.06.2017]; zit.: Bitkom 2016.

Carl, S., Kilchling, M., Knickmeier, S. & Wallwaey, E. (2017): Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa. Eine rechtsvergleichende Betrachtung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, forschung aktuell – research in brief 49. Freiburg i.Br.

Carnegy, H. (2013): France, a master at espionage, under few illusions on US spying. Financial Times, 01.11.2013; www.ft.com/content/e86fdad0-42d9-11e3-9d3c-00144feabdc0?mhq5j=e1 [27.06.2017].

Corporate Trust (2014): Studie Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co?; www.corporate-trust.de/wp-content/uploads/ 2016/06/CT-Studie-2014_DE.pdf [27.06.2017]; zit.: CT 2014.

Corporate Trust (2012): Studie Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar; www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2012_FINAL.pdf [27.06.2017]; zit.: CT 2012.

Crane, A. (2005): In the company of spies – When competitive intelligence gathering becomes industrial espionage. Business Horizons 48, S. 233–240.

CT, siehe Corporate Trust.

Der Spiegel (2014): Spähangriff auf Deutsches Zentrum für Luft- und Raumfahrt. Ausgabe 16/2014; www.spiegel.de/netzwelt/web/dlr-mit-trojanern-von-geheimdienst-ausgespaeht-a-964099.html [12.06.2017].

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (o.D.): „Im Visier". Informationsvideo des Schweizer Nachrichtendienstes des Bundes (NDB 2016); www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.html [28.06.2017]; zit.: VBS (o.D.).

Engels, B. (2017): Wirtschaftliche Kosten der Cyberspionage für deutsche Unternehmen – Cybersicherheit als Grundvoraussetzung der digitalen Transformation, in: Institut der deutschen Wirtschaft Köln (Hrsg.), Aktuelle politische Debattenbeiträge (IW policy paper 6/2017); www.iwkoeln.de/fileadmin/publikationen/2017/341100/IW-policy-paper_2017_6_Cyberspionage.pdf [27.06.2017].

Evers, M. (2012): Kopiert und nachgebaut – Spionage trifft Mittelstand. Braunschweiger Zeitung, 04.09.2012; www.braunschweiger-zeitung.de/wirtschaft/article150748845/Kopiert-und-nachgebaut-Spionage-trifft-Mittelstand.html [05.07.2017].

Fleischer, D. (2016): Wirtschaftsspionage – Phänomenologie, Erklärungsansätze, Handlungsoptionen. Wiesbaden.

Focus-Money (2013): Mittelstand besonders gefährdet – Wirtschaftsspionage kostet Industrie 50 Milliarden. Artikel vom 28.08.2013; www.focus.de/finanzen/news/unternehmen/mittelstand-besonders-gefaehrdet-wirtschaftsspionage-kostet-industrie-50-milliarden_aid_1083974.html [05.07.2017].

Hannoversche Allgemeine (2016): Hacker programmieren Viren gegen Unternehmen; www.haz.de/Nachrichten/Wirtschaft/Deutschland-Welt/Spionage-Hacker-programmieren-Viren-gegen-Unternehmen [13.06.2017]; zit.: HAZ 2016.

HAZ, siehe Hannoversche Allgemeine.

Helm, T., Boffey, D. & Hopkins, N. (2013): Snowden spy row grows as US is accused of hacking China. The Guardian, 22.06.2013; www.theguardian.com/world/2013/jun/22/edward-snowden-us-china [27.06.2017].

Hofer, A. & Weiß, M. (2016): Wirtschafts- und Industriespionage – Informationsgewinnung, Management, Kompetenz. Wiesbaden.

Initiative Wirtschaftsschutz (2016): Leitfaden Wirtschaftsschutz; www.bdsw.de/images/broschueren/Leitfaden-Wirtschaftsschutz_web.pdf [06.06.2017].

Kasper, K. (2014): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes, Ergebnisbericht einer Sekundäranalyse. Bundeskriminalamt; www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Wirtschaftsschutzallgemein/SpioForschung_lang.pdf?__blob=publicationFile&v=3 [02.06.2017].

Kirsch, S. (2014): Informationsschutz im Unternehmen – Prävention von Wissensabfluss und die Erkennung von Innentätern anhand derer Verhaltensmerkmale. Norderstedt.

Knickmeier, S. & Wallwaey, E. (2018): Introduction, in: S. Carl & M. Kilchling (Hrsg.), Economic and industrial espionage in Germany and Europe. Vol. 1: History, developments and present legislative frameworks. Berlin, S. 3–14.

Kurek, H. (2007): Wirtschaftsspionage – Herausforderung für den Verfassungsschutz, in: Bundesamt für Verfassungsschutz (Hrsg.), Bedrohung der Wirtschaft im Zeitalter der Globalisierung – Publikation der Vorträge des 6. Symposiums des Bundesamtes für Verfassungsschutz am 3. Dezember 2007, S. 40–49; www.verfassungsschutz.de/de/download-manager/_tagungsband-2008-07-symposium-2007.pdf [06.06.2017].

Landerer, L. (2014): Das Risiko der Wirtschaftsspionage – Mögliche Schutzmaßnahmen gegen Spionage. Hamburg.

Lee, C.-M. (2015): Criminal profiling and industrial security. Multimedia Tools and Applications 74/5, S. 1689–1696.

Lux, C. & Peske, T. (2002): Competitive Intelligence und Wirtschaftsspionage – Analyse, Praxis, Strategie. Wiesbaden.

Maurer, M. (2008): Geheimschutz in der Wirtschaft – Vorbild für den Schutz von Unternehmensgeheimnissen?, in: Bundesamt für Verfassungsschutz (Hrsg.), Bedrohung der Wirtschaft im Zeitalter der Globalisierung – Publikation der Vorträge des 6. Symposiums des Bundesamtes für Verfassungsschutz am 3. Dezember 2007, S. 64–77; www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-symposium/tagungsband-2008-07-symposium-2007 [09.06.2017].

Merkel, W. & Kahle, E. (2007): Wettbewerb um Know-how – Schaden durch Know-how-Verlust, in: Bundesamt für Verfassungsschutz (Hrsg.), Bedrohung der Wirtschaft im Zeitalter der Globalisierung – Publikation der Vorträge des 6. Symposiums des Bundesamtes für Verfassungsschutz am 3. Dezember 2007, S. 8–18; www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-symposium/tagungsband-2008-07-symposium-2007 [09.06.2017].

Nathusius, I. (2001): Wirtschaftsspionage – Gefahren, Strukturen und Bekämpfung. Heidelberg.

N-TV (2016): Datenklau in unbekanntem Ausmaß – Hacker brechen bei Thyssenkrupp ein; www.n-tv.de/wirtschaft/Hacker-brechen-bei-Thyssenkrupp-ein-article19279586.html [13.06.2017].

N-TV (2010): Abgehört und ausgespäht – Spione bedrohen Mittelstand; www.n-tv.de/wirtschaft/Spione-bedrohen-Mittelstand-article1497096.html [05.07.2017].

O'Shea, G. (2016): Suspected British spy arrested in Iran after country announces clampdown on foreign espionage networks. The Sun, 17.08.2016; www.thesun.co.uk/news/1624488/

suspected-british-spy-arrested-in-iran-after-country-announces-clampdown-on-foreign-espionage-networks/ [27.06.2017].

Perlroth, N., Scott, M. & Frenkel, S. (2017): Cyberattack hits Ukraine, then spreads internationally. The New York Times, 27.06.2017; www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [28.06.2017].

Preuss, M. (2016): Neue Generation der Cyberattacken – Erpressung, Spionage, Hacks: Welche Gefahren 2016 im Netz auf Sie lauern. Focus Online, 17.01.2016; www.focus.de/digital/internet/neue-generation-der-cyberattacken-erpressung-spionage-hacks-das-koennte-uns-2016-alles-bluehen_id_5202588.html [28.06.2017].

PricewaterhouseCoopers (2016): Wirtschaftskriminalität in der analogen und digitalen Wirtschaft; www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf [02.06.2017]; zit.: PwC 2016.

PwC, siehe PricewaterhouseCoopers.

Rayment, S. (2009): Britain under attack from 20 foreign spy agencies including France and Germany. The Telegraph, 07.02.2009; www.telegraph.co.uk/news/uknews/defence/4548753/Britain-under-attack-from-20-foreign-spy-agencies-including-France-and-Germany.html [27.06.2017].

Result Group GmbH Global Risk and Crisis Management (2014): Kriminelle Risiken im Mittelstand – Gefahren, Schäden, Prävention; www.vdr-service.de/fileadmin/der-verband/fachthemen/studien/ResultGroup_KriminelleRisikenMittelstand.pdf [14.06.2017]; zit.: Result Group.

Röder, N. (2011): Industriespionage – Risikofaktor Mensch. Unveröffentlichte Masterarbeit. Hochschule Hannover, Fakultät IV – Abteilung Betriebswirtschaft.

Schaaf, C. (2009): Industriespionage – Der große Angriff auf den Mittelstand. Stuttgart.

Schweizer, P. (1993): Friendly Spies – How America's Allies are using Economic Espionage to steal our Secrets. New York.

Sicherheitsforum Baden-Württemberg (2010): SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg; www.sicherheitsforum-bw.de/pb/site/sifo/get/documents/IV.Dachmandant/Sifo/PDF/SiFo-Studie%202009-10%20-%20Know-how-Schutz%20in%20Baden-W%C3%BCrttemberg.pdf [09.06.2017]; zit.: SiFO BW 2010.

Sicherheitsforum Baden-Württemberg (2005): Mit Sicherheit erfolgreich – Erfolgsfaktor Know-how-Schutz; www.sicherheitsforum-bw.de/pb/site/sifo/get/documents/IV.Dachmandant/Sifo/PDF/SiFo%20Mit%20Sicherheit%20erfolgreich.pdf [09.06.2017]; zit.: SiFO BW 2005.

SiFO BW, siehe Sicherheitsforum Baden-Württemberg.

Simon, H. (2007): Hidden Champions des 21. Jahrhunderts – Die Erfolgsstrategien unbekannter Weltmarkführer. Frankfurt am Main.

Spectaris (2011): Wirtschaftsspionage – Risiken für den Mittelstand. Spectaris Infoletter 02/2011; www.spectaris.de/index.php?id=2846 [05.07.2017]; zit.: Spectaris 2011.

Sule, S. (2006): Spionage – völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage. Baden-Baden.

Thorleuchter, D. & Van den Poel, D. (2013): Protecting research and technology from espionage. Expert Systems with Applications 40, S. 3432–3440.

Wagner, P. (2014): Schutz vor Industriespionage – Analyse, Prävention und Abwehr des irregulären Verlusts von Know-how in Unternehmen. Hamburg.

Warnecke, G. (2010): Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage, in: C. Fussan (Hrsg.), Managementmaßnahmen gegen Produktpiraterie und Industriespionage. Wiesbaden, S. 249–332.

Wolff, D. (2009): Wirtschafts- und Industriespionage im deutschen Wirtschaftsraum – eine analytische Betrachtung von Akteuren, Methoden und Gefahren. Arbeitspapiere zur Internationalen Politik und Außenpolitik (AIPA) 3/2009; www.ssoar.info/ssoar/bitstream/handle/document/21817/ssoar-2009-wolff-wirtschafts_und_industriespionage_im_deutschen.pdf?sequence=1.

Zwickl, J. (2015): Industriespionage im deutschen Mittelstand. Wie schützt man Know-How wirkungsvoll? Norderstedt.

Wirtschaftsspionage und Konkurrenzausspähung kennen keine Grenzen

Eine vergleichende Analyse exemplarischer Fälle[1]

Susanne Knickmeier

1. Einleitung

Im Jahr 2013 erhielten deutsche Strafverfolgungsbehörden einen Hinweis, dass mittels einer Schadsoftware versucht worden war, in verschiedenen Ländern – u.a. Deutschland und Norwegen – Daten, zu denen auch Geschäftsgeheimnisse gehören sollten, auszuspähen, um diese unbefugten Dritten zur Verfügung zu stellen. Die Tatverdächtigen konnten nicht identifiziert werden, sodass die Verfahren eingestellt wurden.[2] In einem anderen Fall erstellte ein chinesischer Delegierter bei einem Betriebsrundgang auf dem Gelände der in Bayern ansässigen Firma Rieder,[3] einem der weltweit führenden Unternehmen im Bereich Faserbeton, mit einer an seinem Gürtel befestigten digitalen Minikamera heimlich Filmaufnahmen von Betriebsabläufen, obwohl Filmaufnahmen ausdrücklich untersagt waren. Er wurde auf frischer Tat ertappt und vom Landgericht München II zu einer Freiheitsstrafe von 18 Monaten, die zur Bewährung ausgesetzt wurde, verurteilt. Zudem zahlte er eine Entschädigung in Höhe von 80.000 Euro.[4]

Die Bandbreite möglicher Delikte der Wirtschaftsspionage und Konkurrenzausspähung sowie die Vielfältigkeit der Gruppe potenzieller Täter sind groß und auch die Möglichkeit einer Tatbegehung ist nicht regional beschränkt. Betroffen sein kann

---

1 Herrn Ass. iur. *Nikolai Anstatt* danke ich für die Anfertigung eines Gutachtens zu den strafprozessualen Herausforderungen im Fall der Firma AMSC Windtech, das er während der Wahlstation seines juristischen Vorbereitungsdienstes am Max-Planck-Institut für ausländisches und internationales Strafrecht erstellte.

2 Vgl. *Fall 119* Deutschland. Die zitierten Fälle stammen aus einer Analyse von 713 Strafverfahren in Deutschland. Weitere Informationen zur Datenerhebung finden sich im *Abschnitt 2.3*.

3 Informationen zu Fällen, die namentlich erwähnt werden, stammen aus frei zugänglichen Quellen.

4 Vgl. *Tsolkas & Wimmer* 2013, S. 28.

der lokale Handwerksbetrieb, dessen (ehemaliger) Mitarbeiter unerlaubt Kundendaten verrät, ebenso wie ein sogenannter Hidden Champion, der in seinem Tätigkeitsbereich Weltmarktführer ist und dessen Produktionsdaten von Geheimdienstmitarbeitern eines fremden Staates (z.B. über Cyberangriffe) ausspioniert werden. Die wirtschaftlichen Folgen eines unzulässigen Know-how-Abflusses können für das betroffene Unternehmen existenzbedrohend sein.[5] Mit der seit einigen Jahrzehnten zunehmenden Globalisierung haben der grenzüberschreitende Handel und Wettbewerb weiter zugenommen.[6] Um im internationalen Wettbewerb bestehen zu können, weckt gerade das Know-how führender Hochtechnologieländer wie Deutschland, in denen viel Geld in die Forschung und Entwicklung investiert wird,[7] das Interesse (ausländischer) konkurrierender Unternehmen oder fremder Staaten, die die eigene Wirtschaft fördern wollen. So verpflichtet zum Beispiel Russland seinen Auslandsgeheimdienst (SWR), Wirtschaftsspionage zu betreiben, um die nationale Wirtschaft voranzubringen.[8] Auch im Vereinigten Königreich kann der Geheimdienst im Interesse des nationalen wirtschaftlichen Wohlergehens aktiv werden (Art. 1 Intelligence Service Act 1994). Die Handlungen können sich vom Wortlaut des Gesetzes her trotz der (noch) bestehenden Zugehörigkeit zum europäischen Binnenmarkt auch gegen andere Mitgliedsstaaten der Europäischen Union (EU) richten.

Betrachtet man die Kriminalstatistiken europäischer Staaten, scheinen Wirtschaftsspionage und Konkurrenzausspähung quantitativ keine große Rolle zu spielen.[9] Der im Hellfeld bekannte Umfang ist gering und strafrechtliche Verurteilungen sind selten.[10] Im Gegensatz zu diesen Zahlen stehen die Ergebnisse einer im Rahmen des Projektes WiSKoS im Jahr 2017 in Deutschland durchgeführten Dunkelfeldbefragung, in der 45 % der befragten kleinen und mittleren Unternehmen (KMU) mit dem Schwerpunkt „Produktion“ und „Dienstleistung“ angaben, in den letzten fünf Jahren einen illegalen Wissens-, Informations- und/oder Datenabfluss konkret erlebt zu haben oder die eine solche Betroffenheit vermuteten.[11] Von ähnlichen Dunkelziffern ist in anderen Ländern auszugehen.

---

5 Siehe dazu auch *Bollhöfer & Jäger* 2018, S. 41, 42.

6 Vgl. WTO 2017, S. 122, 123.

7 Nach einer Erhebung des Essener Stifterverbands für die Deutsche Wissenschaft investierte die deutsche Wirtschaft im Jahr 2017 68,6 Mrd. Euro in die eigene Forschung und Entwicklung (vgl. dpa 2018, Deutsche Wirtschaft gibt mehr für Forschung aus; Wirtschaftswoche, 12.11.2018; www.wiwo.de/technologie/forschung/studie-zeigt-deutsche-wirtschaft-gibt-mehr-fuer-forschung-aus/23621868.html [12.07.2019]).

8 Vgl. Verfassungsschutzbehörden des Bundes und der Länder 2014, S. 8.

9 Vgl. dazu die Landesberichte zum *Modul 1* des WiSKoS-Projektes in *Carl & Kilchling* 2018.

10 In der deutschen Polizeilichen Kriminalstatistik wurden im Jahr 2017 nur 322 Fälle (im Jahr 2016: 397 Fälle) wegen Verstoßes gegen § 17 UWG registriert.

11 Vgl. *Bollhöfer & Jäger* 2018, S. 31.

Der Schutz von Know-how wirft nicht nur die Frage auf, mit welchen technischen, organisatorischen oder personellen Maßnahmen Unternehmen und Wissenschaftsorganisationen ihre Geschäftsgeheimnisse schützen können, sondern auch, welche rechtlichen Möglichkeiten den Betroffenen nach einem erfolgreichen Angriff zur Verfügung stehen. Neben zivil- oder arbeitsrechtlichen Konsequenzen kann ein (erfolgreicher) Angriff, wenn er entdeckt wird, strafrechtlich verfolgt werden. Die (grenzüberschreitende) Verfolgung von Straftaten, besonders aus dem Bereich der Cyberkriminalität, stellt Strafverfolgungsbehörden und Gerichte jedoch immer wieder vor rechtliche und strafprozessuale Herausforderungen wie den Strafklageverbrauch, Beweisschwierigkeiten oder das Fehlen eines Strafantrags sowie vor die Frage nach den Grenzen des Strafrechts bei der Regulierung des unzulässigen Know-how-Abflusses.

Der vorliegende Beitrag behandelt auf der Grundlage exemplarischer Fallstudien aus Bulgarien, Dänemark, Österreich, der Schweiz und dem Vereinigten Königreich[12] sowie einer Analyse von über 700 Strafverfahren in Deutschland Fragen der Phänomenologie von Konkurrenzausspähung, die strafrechtliche Verfolgungspraxis sowie Herausforderungen der Strafverfolgung bei Delikten der Konkurrenzausspähung und Wirtschaftsspionage.

2. Methodisches Vorgehen

Während der Schwerpunkt des Projektes WiSKoS bei den KMU lag,[13] wurden in die Analyse deutscher Strafverfahren und exemplarischer Fallstudien aus dem Ausland neben den eine untergeordnete Rolle spielenden Wissenschaftsorganisationen auch große Unternehmen einbezogen. Die durch die Auswertung der Strafverfahren aus Deutschland gewonnenen Ergebnisse wurden mit den Ergebnissen der exemplarischen Fallstudien verglichen.

2.1 Theoretischer Rahmen

Die Untersuchung beruht auf den Annahmen der Rational-Choice-Theorie. Dieser Ansatz geht vom Leitbild des neoklassischen Homo oeconomicus aus, wonach ein Mensch in seiner Willensbildung frei ist und die Kosten einer Straftat gegen die Vorteile einer geplanten kriminellen Handlung rational abwägt.[14] Überwiegt der Nut-

---

12 Die Kriterien, nach denen die Auswahl der Vergleichsländer erfolgte, sind in der *Einleitung* zum vorliegenden Band (Wirtschaftsspionage und Konkurrenzausspähung in Theorie und Praxis)*, Abschnitt 4*, dargelegt.

13 Vgl. auch die Ausführungen dazu in der *Einleitung* zum vorliegenden Band (Wirtschaftsspionage und Konkurrenzausspähung in Theorie und Praxis).

14 Vgl. Gabler Wirtschaftslexikon (o.D.): Homo oeconomicus; http://wirtschaftslexikon.gabler.de/Archiv/8004/homo-oeconomicus-v12.html [12.07.2019]; *Spirgath* 2013, S. 11 m.w.N.

zen aus einer Straftat ihre Kosten, entscheidet sich der Täter für die Begehung der unerlaubten Handlung.[15] Dem folgend wird angenommen, dass sich Täter bewusst für den Verrat von Geschäftsgeheimnissen entscheiden, um einen wirtschaftlichen Vorteil (für sich oder Dritte) zu erlangen. Präventiv kann nach den auf dem Rational-Choice-Ansatz beruhenden Abschreckungstheorien durch externe Faktoren auf den potenziellen Straftäter eingewirkt werden, indem die Kosten für die Begehung von Straftaten erhöht werden und die Begehung selbst erschwert wird.[16] Zur Herstellung von Normkonformität stützen sich kriminalpolitische Strategien daher vor allem auf verstärkte Kontrollmaßnahmen, um das Entdeckungsrisiko zu erhöhen, sowie auf Strafgesetze, auf deren Basis für den Fall eines Gesetzesverstoßes eine Strafe angedroht wird, die bei einem Verstoß verhängt und vollstreckt wird.[17]

Anhand der Ergebnisse der ausgewerteten deutschen Strafverfahren und der auf die Vergleichsländer bezogenen Fallstudien wird daher analysiert, welche Faktoren zur Aufdeckung der Taten führten, wo die Unternehmen das Entdeckungsrisiko erhöhen sollten und inwieweit die strafrechtlichen Regelungen in der Praxis geeignet sind, um potenzielle Täter von der Tatbegehung abzuschrecken.

2.2 Dokumentenanalysen und ihre Grenzen

Die Analyse von Strafverfahrensakten (Dokumentenanalyse) ermöglicht die Beschreibung eines Deliktsbereichs im Hellfeld.[18] Eine Beantwortung der Forschungsfragen jedoch ist gerade bei Delikten, bei denen – wie im Bereich der Wirtschaftsspionage und Konkurrenzausspähung – von einem hohen Dunkelfeld auszugehen ist, nur beschränkt möglich.[19] Wirtschaftsspionage und Konkurrenzausspähung sind durch ein doppeltes Dunkelfeld und ein verdecktes Hellfeld charakterisiert. Teilweise bemerken betroffene Unternehmen nicht, dass unerlaubt auf geschützte Informationen zugegriffen wurde (absolutes Dunkelfeld). Selbst wenn ein Vorfall bemerkt wird, erstatten viele Unternehmen keine Strafanzeige, sodass die Strafverfolgungsbehörden keine Kenntnis von einem solchen Vorfall erlangen (relatives Dunkelfeld). Werden Vorfälle angezeigt, kann wiederum ein verdecktes Hellfeld vorliegen, und zwar dann, wenn ein Vorfall nicht als Verrat eines Geschäftsgeheimnisses erkannt wird.[20] Zum Beispiel liegt bei der Wegnahme eines Laptops dem ersten Anschein nach ein

---

15 Vgl. *Roxin* 1997, S. 50.

16 Vgl. *Becker* 1968, S. 207, 208.

17 Vgl. *Feuerbach* 1801, § 157; *Roxin* 1997, S. 48.

18 Vgl. *Kersting & Erdmann* 2015, S. 11.

19 Vgl. *Kersting & Erdmann* 2015, S. 28.
Um sich dem Phänomen möglichst umfassend zu nähern, wurde daher im Projekt WiSKoS in *Modul 3* eine Dunkelfeldbefragung durchgeführt. Die Ergebnisse der Dunkelfeldbefragung sind veröffentlicht in *Bollhöfer & Jäger* 2018.

20 Vgl. *Kilchling & Carl* 2016, S. 189.

Diebstahl vor. Inwieweit der Täter möglicherweise weniger an dem Gerät als an den auf dem Laptop gespeicherten Informationen interessiert war, womit ein Verrat von Geschäfts- oder Betriebsgeheimnissen gem. §§ 17–19 UWG[21] (Konkurrenzausspähung) oder eine geheimdienstliche Agententätigkeit gem. § 99 StGB (Wirtschaftsspionage) vorläge, bleibt möglicherweise unaufgeklärt.[22]

Die im Folgenden dargestellten Ergebnisse aus den untersuchten Strafverfahren können aus diesen Gründen nur die entdeckten Vorfälle bei anzeigewilligen Unternehmen widerspiegeln, bei denen die Staatsanwaltschaft wegen eines Deliktes aus dem Phänomenbereich der Konkurrenzausspähung oder Wirtschaftsspionage Ermittlungen angestrengt hat.

2.3 Zugang zu den Strafverfahrensakten

Die Erhebung der Daten aus Deutschland erfolgte durch eine standardisierte Auswertung von Strafverfahren, die wegen des Verrats von Geschäft- oder Betriebsgeheimnissen gem. §§ 17 ff. UWG geführt und abgeschlossen wurden. Die Strafverfahren enthielten z.T. Verstöße gegen weitere Delikte, wobei der Schwerpunkt des Verfahrens immer auf einem Verstoß gegen §§ 17 ff. UWG lag. Ein Zugang zu Strafverfahrensakten aus dem Bereich der Wirtschaftsspionage war nicht möglich, da sie als Staatsschutzverfahren geführt werden und als vertraulich eingestuft sind. Zur Untersuchung der Konkurrenzausspähung wurden 54 Staatsanwaltschaften in Deutschland gebeten, die bei ihnen geführten, infrage kommenden Strafverfahren aus dem Zeitraum 2010–2015 zur Verfügung zu stellen. Um eine möglichst breite geografische Abdeckung Deutschlands zu erreichen, erfolgte die Auswahl der Staatsanwaltschaften nach Bundesländern, dort nach Generalstaatsanwaltschaften und innerhalb des Bezirks einer Generalstaatsanwaltschaft, sofern möglich, nach den Schwerpunktstaatsanwaltschaften für Wirtschaftsstrafrecht. In die Datenerhebung konnten 713 Verfahren von insgesamt 43 Staatsanwaltschaften aus dem erweiterten Zeitraum 2008–2016 aufgenommen werden.

Bei der Auswahl der insgesamt 50 exemplarischen Fallstudien aus den Vergleichsländern waren Fälle mit internationalen Verflechtungen sowie außergewöhnlichen rechtlichen oder tatsächlichen Strafverfolgungsproblemen von besonderem Interesse. Die Auswahl der Fälle aus Bulgarien, Dänemark und dem Vereinigten Königreich erfolgte durch Länderexperten und im deutschsprachigen Raum durch die Autorin. Durch die Beteiligung lokaler Experten waren die notwendigen Kenntnisse

---

21 Nach Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) im April 2019 sind die Vorschriften der §§ 17 bis 19 UWG weggefallen und in § 23 GeschGehG geregelt. Im Folgenden wird auf die zum Zeitpunkt der Untersuchung (2016–2017) geltende Rechtslage abgestellt.

22 Gesetze ohne Angabe eines Landes, die nicht im Kontext eines der untersuchten Länder stehen, beziehen sich auf Deutschland.

des nationalen Strafrechts, Strafprozessrechts, der behördlichen Zuständigkeiten und nicht zuletzt der Sprache sichergestellt. Wie in Deutschland konnten auch in Bulgarien, Österreich[23] und der Schweiz nur Fälle, die in dem jeweiligen Land der Konkurrenzausspähung zugeordnet sind, einbezogen werden, da Fälle der Wirtschaftsspionage – als vertraulich eingestuft – nicht zu wissenschaftlichen Zwecken eingesehen werden konnten. Trotz größter Bemühungen gelang es in Dänemark und dem Vereinigten Königreich nicht, Zugang zu Strafakten zu erhalten, sodass auf Fälle aus öffentlich zugänglichen Quellen von Strafverfolgungs- und Ermittlungsbehörden und Geheimdiensten sowie auf (entsprechende) Presseberichte zurückgegriffen werden musste.

Allgemeingültige Aussagen über den Status Quo der Phänomenologie von Wirtschaftsspionage und Konkurrenzausspähung und über Best Practices bei der Tataufdeckung, Strafverfolgung und Prävention in den ausgewählten Ländern lassen sich aus der geringen Anzahl der analysierten Fallstudien nicht herleiten.

2.4 Inhaltsanalytische Auswertung

Die Auswertung der aufs Ausland bezogenen Fallstudien und deutschen Strafverfahren erfolgte anhand einer Inhaltsanalyse mit dem Ziel der systematischen Erhebung und Aufbereitung der Dokumenteninhalte.[24] Mithilfe eines Erhebungsrasters wurden standardisiert Informationen zu den Tätern (z.B. Beziehung zum Unternehmen, Zusammenarbeit von Tätern), den Geschädigten, dem Vorfall, der Tätigkeit von Behörden und dem Strafverfahren erfasst. In jeder Kategorie konnten Informationen als Freitext hinzugefügt werden, um keine nicht antizipierte Information zu verlieren. Die ausformulierte Zusammenfassung jedes einzelnen Verfahrens ermöglichte die qualitative Ausarbeitung etwaiger Besonderheiten einzelner Fälle, die durch die standardisierte Abfrage von Informationen nicht erfasst wurden. Die erhobenen Informationen wurden nach ihrer Häufigkeit ausgewertet (sog. Frequenzanalyse).[25] Die analysierten Kategorien betrafen u.a. folgende Fragestellungen:

Phänomenologie

- Wie war das Verhältnis von Täter und Unternehmen? (siehe *4.1*)
- Was waren die treibenden Faktoren und wer hat profitiert? (siehe *4.2*)
- Wo lag der Tatort? (siehe *4.3*)
- Wie gelangten die Täter an die geschützten Informationen? (siehe *4.4*)

---

23 In Österreich galt die Beschränkung nur für die Fälle, in denen ein fremder Nachrichtendienst Täter war (§ 256 StGB).

24 Vgl. *Häder* 2015, S. 327.

25 Vgl. *Häder* 2015, S. 333.

- Welche Informationen sind auf welche Weise abgeflossen? (siehe *4.5*)
- Was war das Angriffsziel? (siehe *4.6*)
- Wie wurde die Tat aufgedeckt? Gab es besonders vielversprechende Mechanismen? (siehe *4.7*)

Strafverfahren

- Wie unterscheiden sich die rechtlichen Grundlagen der Wirtschaftsspionage und Konkurrenzausspähung in den ausgewählten Ländern? (siehe *5.1*)
- Welche strafprozessualen Entscheidungsmöglichkeiten stehen in den ausgewählten Ländern zur Verfügung und mit welchen Konsequenzen? (siehe *5.2*)
- Wodurch wurden die Ermittlungen ausgelöst? (siehe *5.3*)
- Mit welchen Entscheidungen endeten die Ermittlungsverfahren? (siehe *5.4*)
- Mit welchen Rechtsfolgen endeten die Strafverfahren? (siehe *5.5*)
- Welchen strafprozessualen und/oder praktischen Herausforderungen standen die Strafverfolgungsbehörden – besonders bei Cyberangriffen und der grenzüberschreitenden Verfolgung von Straftaten – gegenüber? (siehe *5.6*)

3. Abgrenzung von Wirtschaftsspionage und Konkurrenzausspähung in den ausgewählten Ländern

Die beiden Phänomenbereiche Wirtschaftsspionage und Konkurrenzausspähung sind weder in Deutschland noch in den ausgewählten Ländern legaldefiniert oder zumindest einheitlich definiert.[26] Sie sind dennoch voneinander abzugrenzen, da die juristische Unterscheidung der beiden Phänomenbereiche zu unterschiedlichen behördlichen Zuständigkeiten[27] und rechtlichen Konsequenzen führt (siehe *Tabelle 9* in *Abschnitt 5.5*).

Während in Deutschland, ähnlich wie auch in Dänemark,[28] Wirtschaftsspionage und Konkurrenzausspähung nach allgemeiner Ansicht danach abgegrenzt werden, ob der Täter im Auftrag des Geheimdienstes eines fremden Staates oder zugunsten seiner selbst bzw. eines anderen Unternehmens handelt,[29] hängt die Unterscheidung

---

26 Siehe auch die *Einleitung* zum vorliegenden Band (Wirtschaftsspionage und Konkurrenzausspähung in Theorie und Praxis), *Abschnitt 2*.

27 Vgl. *Carl et al.* 2017, S. 110, 111.

28 Vgl. *Afsah* 2018.

29 Vgl. Bundestags-Drucksache 18/2281, S. 2.

Tabelle 1 Abgrenzung von Wirtschaftsspionage und Konkurrenzausspähung

	Abgrenzungs-merkmal	Wirtschaftsspionage	Konkurrenzausspähung
Bulgarien	Geheimnis	Staatsgeheimnis, Wirtschaftsgeheimnis, Privatgeheimnis	
Dänemark	Täterschaft	fremder Nachrichten-dienst	natürliche oder juristische Person, z.B. Angestellter oder (konkurrie-rendes) Unternehmen
Deutschland	Täterschaft	fremder Nachrichten-dienst	natürliche Person, z.B. Angestell-ter oder für ein (konkurrierendes) Unternehmen handelnd
Österreich	Täterschaft	fremder Nachrichtendienst oder natürliche oder juristische Person, die ein Geheimnis zugunsten des Nicht-EU-Auslands auskundschaftet	natürliche oder juristische Person aus dem EU-Inland, z.B. Ange-stellter oder (konkurrierendes) Unternehmen
Schweiz	Täterschaft	fremder Staat oder eine ausländische natürliche oder juristische Person	natürliche oder juristische Person, z.B. Angestellter oder (konkurrie-rendes) Unternehmen
Vereinigtes Königreich	keine einheitliche Verwendung der Begriffe Wirtschaftsspionage und Konkurrenz-ausspähung im allgemeinen Sprachgebrauch und bei den Rechtsvorschriften		

der Delikte in den Vergleichsländern zum Teil von anderen Merkmalen ab (siehe *Tabelle 1*).

In der Schweiz werden in das Deliktsfeld Wirtschaftsspionage nicht nur Fälle einbezogen, in denen der Täter für einen fremden Staat gehandelt hat, sondern auch die Vorfälle, bei denen ein Unternehmen/Mitarbeiter eines Unternehmens aus dem Ausland der Täter war. Die Konkurrenzausspähung ist hier demzufolge auf Täter aus dem eigenen Land beschränkt.[30] In Österreich wiederum ist das Ausspähen von Geschäftsgeheimnissen durch ausländische Täter nicht eindeutig einer Definition zugeordnet. Während das „Handbuch Know-How-Schutz für die österreichische Wirtschaft", der deutschen Terminologie entsprechend, Wirtschaftsspionage als die Ausforschung von Unternehmen „durch ausländische, staatlich gelenkte Nachrichtendienste" bezeichnet,[31] wird in der Studie „Wirtschafts- und Industriespionage in österreichischen Unternehmen" Wirtschaftsspionage, ähnlich wie in der Schweiz, als „die gezielte Ausforschung von Geschäfts- und Betriebsgeheimnissen (Wirtschaftsgeheimnissen) inländischer Unternehmen und Forschungseinrichtungen zur Stärkung der Wirtschaft anderer Staaten" definiert.[32] Im Unterschied zu Deutschland und der Schweiz, wo Delikte der Wirtschaftsspionage als Staatsschutzdelikte

30 Vgl. *Konopatsch et al*. 2018.

31 FH Campus Wien 2011, S. 15.

32 *Körmer & Langer* 2015, S. 20.

behandelt werden, sind Verstöße gegen § 124 StGB („Auskundschaften von Geschäfts- und Betriebsgeheimnissen zugunsten des Auslands") kein klassisches Staatsschutzdelikt. Ein solches liegt nur vor, wenn fremde Staaten österreichische Wirtschaftsunternehmen ausspähen (§ 256 StGB). Das österreichische Bundesamt für Verfassungsschutz und Terrorismusbekämpfung hat zwar gem. § 6 Abs. 2 Nr. 4 Polizeiliches Staatsschutzgesetz für Verstöße gegen § 124 StGB eine Ermittlungszuständigkeit, aber im Gegensatz zu den klassischen Staatsschutzdelikten sind die Strafvorschriften wegen des Auskundschaftens von Geschäfts- und Betriebsgeheimnissen im Strafgesetzbuch systematisch nicht bei den Staatsschutzdelikten, sondern im Abschnitt „Verletzung der Privatsphäre und bestimmter Berufsgruppen" nach den Delikten der Konkurrenzausspähung eingeordnet.[33] Zudem sind die Strafverfahren im Gegensatz zu Verstößen gegen § 256 StGB nicht als vertraulich eingestuft. Im vorliegenden Beitrag wird der herrschenden Meinung in Österreich folgend das Auskundschaften eines Geschäftsgeheimnisses zugunsten des Auslands (§ 124 StGB) der Wirtschaftsspionage zugeordnet.

Im Vereinigten Königreich tauchen die Begriffe *industrial espionage* und *economic espionage* zwar im Sprachgebrauch auf, werden aber nicht einheitlich für jeweils einen Deliktsbereich verwendet und können auch nicht durch eine rechtliche Abgrenzung, wie in den anderen untersuchten Ländern, erklärt werden.[34] Auch in Bulgarien werden Wirtschaftsspionage und Konkurrenzausspähung im Sprachgebrauch nicht als unterschiedlich definierte Begriffe verwendet. Die Strafvorschriften, die die Deliktsbereiche Konkurrenzausspähung und Wirtschaftsspionage umfassen, werden anhand des betroffenen Geheimnisses (Staatsgeheimnis, Wirtschaftsgeheimnis, Privatgeheimnis) abgegrenzt.[35]

4. Ausgewählte phänomenologische Ergebnisse

Im Mittelpunkt der ausgewählten phänomenologischen Ergebnisse stehen das Verhältnis der Täter zum geschädigten Unternehmen, die Motivation für ihre Handlungen, der Tatort, betroffene Unternehmensgeheimnisse und -branchen, die unterschiedlichen Formen des Zugangs zu und des Abflusses von geschützten Informationen sowie Möglichkeiten der Tataufdeckung. Letztere sind eine Voraussetzung für die Einleitung eines Strafverfahrens, das in *Abschnitt 5* (Strafverfolgungspraxis in Fällen von Konkurrenzausspähung und Wirtschaftsspionage) behandelt wird. Erkenntnisse über die Täter und Modi Operandi des Informati-

---

33 In dem Landesbericht zu Österreich von *Konopatsch & Lehmkuhl* 2018 finden sich weitere Ausführungen zum Rechtsstreit über die Einordnung von § 124 StGB.

34 Vgl. *Button et al.* 2018.

35 Vgl. *Petrova et al*. 2018.

onsabflusses wiederum spielen bei der Entwicklung präventiver Maßnahmen eine große Rolle.

4.1 Verhältnis der Täter zum geschädigten Unternehmen

Ein besonderes Interesse gilt der Frage nach dem Verhältnis der Täter zum geschädigten Unternehmen. Gerade für die Entwicklung präventiver Maßnahmen ist es für die Geschädigten von Bedeutung, ob der Täter eher der (unbekannte) Angreifer von außen oder der eigene Mitarbeiter ist.

Im deutschen Sample lag die Zahl der Innentäter bei 43 %, die der Außentäter bei 32 % und 23 % der Täter sicherten sich die Daten als Innentäter und verwerteten sie als Außentäter. Von den Innentätern waren knapp über 80 % länger als ein Jahr in dem Unternehmen beschäftigt, 44,4 % von ihnen gehörten dem Unternehmen schon über fünf Jahre als Mitarbeiter an.[36] Auch in den Fallstudien zu den Vergleichsländern kam die Mehrzahl der Täter aus dem eigenen unternehmerischen Umfeld. Das Verhältnis der Taten, die von Einzeltätern begangen werden, und solchen, bei denen es Mittäter gibt, hielt sich im deutschen Sample die Waage.

Innentäter können langjährige (unzufriedene) Beschäftigte sein, aber durchaus auch neu eingestellte Mitarbeiter oder Praktikanten. Jedoch können gerade langjährige Mitarbeiter den Wert von geschützten Informationen besser einschätzen, da sie über gute Einblicke in das Unternehmen und seine Strukturen verfügen, und – gegebenenfalls auch über einen längeren Zeitraum unentdeckt – das Unternehmen nachhaltig schädigen. Neben den bewusst vorgehenden Innentätern kann es zudem auch Mitarbeiter geben, die unabsichtlich zum Täter werden, zum Beispiel durch Social Engineering oder als Opfer von Phishing-E-Mails. Social Engineering umfasst verschiedene Methoden der manipulativen Beeinflussung von Mitarbeitern eines Unternehmens mit dem Ziel, an vertrauliche Geschäftsgeheimnisse zu gelangen.[37]

Im Bereich der Cyberkriminalität, gerade wenn von außen auf ein Unternehmen zugegriffen wird, kann die Identifizierung eines Täters oder auch das Bekanntwerden eines Falles schwierig sein oder sogar vom Zufall abhängen. Ein unbekannter Täter wiederum kann ein Grund für die Nichtanzeige eines Vorfalls sein, der damit nicht in das Hellfeld gelangt.[38]

---

36 Diese Angaben erfassen nur Fälle, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete.

37 Vgl. *Tsolkas & Wimmer* 2013, S. 38.

38 Zu der Problematik nicht angezeigter Fälle und zu den Hemmnissen einer Kooperation von Unternehmen mit Behörden vgl. *Bollhöfer & Jäger* 2018, S. 57, 60.

4.2 Treibende Faktoren

Von den Taten profitieren in den meisten Fällen entweder die Täter selbst oder ein anderes Unternehmen. Die Motive der Täter sind vielfältig, wobei beim deutschen Sample die eigene Bereicherung und die Sicherung von Wettbewerbsvorteilen den Schwerpunkt bildeten. So verschafften sich Mitarbeiter zum Beispiel durch den Verkauf oder die Mitnahme und weitere Nutzung von Kundendaten finanzielle Vorteile. In anderen Fällen verhalf die Weitergabe von Produktdaten oder technischem Know-how, die die Herstellung eines Produkts ohne eigene Investitionskosten ermöglichte, Konkurrenzunternehmen zu einem Marktvorteil. Weitere Motive waren Rache oder Unzufriedenheit mit dem Arbeitgeber.

Tabelle 2 gibt einen Überblick über die im deutschen Sample festgestellten Motive. Der Kategorie „ideelle Motive" sind Fallkonstellationen zugeordnet, die an der Grenze zum (straffreien) Whistleblowing stehen. Handlungsleitend waren hier also nicht finanzielle oder wettbewerbliche Vorteile, sondern der Verrat von Geschäftsgeheimnissen sollte auf Missstände aufmerksam machen. Die Kategorie „Sonstiges" umfasst verschiedene Fallkonstellationen. So wollten sich bisweilen Täter mit unbefugt mitgenommenen Daten den Einstieg bei einem neuen Arbeitgeber erleichtern oder Startvorteile bei einer geplanten Selbstständigkeit verschaffen. Auch kam es vor, dass sich ein Täter zur Sicherung seiner privaten Daten bei der Beendigung seines Arbeitsverhältnisses ein komplettes Laufwerk kopierte, auf dem neben eigenen Daten auch geschützte Geschäftsgeheimnisse lagen.

Tabelle 2 Motive für den Verrat von Geschäftsgeheimnissen (deutsches Sample)

Motiv	
einem Konkurrenzunternehmen einen Wettbewerbsvorteil verschaffen	45,8 %
sich selbst oder einem anderen einen finanziellen Vorteil verschaffen, z.B. durch den Verkauf von Kundendaten oder den Verrat eines Geschäftsgeheimnisses	34,4 %
Rache oder Unzufriedenheit im Unternehmen	10,9 %
ideelle Motive	1,0 %
Sonstiges	7,8 %

n = 194; Mehrfachnennung möglich, ohne Fälle mit nicht feststellbaren Motiven. Es wurden nur Fälle aufgenommen, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete.

4.3 Tatorte im In- oder Ausland

In den meisten auslandsbezogenen Fallstudien war, ebenso wie in einem Großteil der Fälle des deutschen Samples, der Tatort innerhalb eines Unternehmens im Inland. In Deutschland lagen fast 95 % der Tatorte im Inland und nur knapp 2 % im

Ausland.[39] Eine Ausnahme bildeten die Fallstudien aus Dänemark, in denen die Täter auch außerhalb des jeweiligen Unternehmens und im Ausland aktiv waren. Begründet ist dieses Ergebnis durch die Aufnahme von Fällen, die das dänische Centre for Cyber Security veröffentlicht hat. Vergleichbare Fälle in Bulgarien, Deutschland, Österreich und der Schweiz wurden als vertraulich eingestuft, sodass für diese Länder keine Fallbeispiele dieser Art bekannt wurden.

4.4 Zugang der Täter zu geschützten Informationen

Der Zugang zu Geschäftsgeheimnissen ist auf vielfältige Weise auf physischem, elektronischem oder persönlichem Wege möglich (siehe *Tabelle 3*). In *Kapitel 2* (Der „typische" Spionagefall? Ergebnisse einer Literaturanalyse) werden die unterschiedlichen Modi Operandi in Form von HUMINT – Informationsbeschaffung über Menschen – oder TECHINT – Informationsgewinnung unter Nutzung technischer Hilfsmittel – ausführlicher beschrieben.[40]

Tabelle 3 Zugang der Täter zu geschützten Informationen (deutsches Sample)

Zugangsart	
Aushorchen von Mitarbeitern	1,0 %
Kenntnisnahme oder Kopie von (z.B. in Aktenordnern enthaltenen) Informationen	24,4 %
Zugriff auf elektronisch gespeicherte Daten	48,8 %
Nutzen von Sicherheitslücken im IKT-System	0,5 %
Zugang über Schadsoftware-Infiltration	0,5 %
Zugang über mobile Kommunikationsgeräte	1,0 %
Zugang über private Kommunikationsgeräte von Mitarbeitern	1,5 %
Angriff auf IT-System, z.B. durch Manipulation	2,0 %
Sonstiges	20,5 %

n = 205; Mehrfachnennung möglich. Es wurden nur Fälle aufgenommen, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete.

In den untersuchten deutschen Strafverfahren verschafften sich im Untersuchungszeitraum 48,8 % der Täter Zugang zu Geschäftsgeheimnissen über den Zugriff auf Datenträger. Die Zahl verwundert nicht, da in vielen Unternehmen die Korrespondenz und Datenarchivierung weitestgehend elektronisch verläuft. Trotz der elektronischen

---

39 Die Prozentzahlen beziehen sich auf n = 181 Fälle. Eine Mehrfachnennung war möglich. Einbezogen wurden nur die Fälle, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete. Bei den übrigen ca. 3 % der Fälle war der Tatort nicht feststellbar.

40 Siehe dazu auch *Zwickl* 2015, S. 54–57.

Speicherung von Daten darf der Faktor „Mitarbeiter“ bei dem Zugriff auf Datenträger innerhalb eines Unternehmens nicht unterschätzt werden. Cyberangriffe auf IT-Systeme von Unternehmen, hinter denen unbekannte Dritte vermutet werden, spielten in den untersuchten Strafverfahren eine untergeordnete Rolle. Die niedrige Zahl kann dadurch begründet sein, dass von einer Anzeige abgesehen wurde, weil kein Täter ausgemacht werden konnte oder kein Schaden entstanden war, Geschäftsgeheimnisse nicht als Ziel des Angriffs identifiziert wurden oder der Vorfall erfolgreich abgewehrt wurde.

Eine weitere Form des Zugangs zu geschützten Informationen innerhalb von Unternehmen, ohne dass der Täter ein Mitarbeiter sein musste, war die Kenntnisnahme oder Kopie von z.B. in Aktenordnern enthaltenen Informationen (24,4 %). In die Kategorie „Sonstiges“ fallen einzelne Vorkommnisse wie das Fotografieren von Maschinen oder Produktionsanlagen in einem Unternehmen (siehe den eingangs beschriebenen Fall der Firma Rieder) oder das Anfertigen von Video- oder Tonaufnahmen.

4.5 Informationsabfluss

Auch wenn in vielen Fällen der Zugriff auf ein Geschäftsgeheimnis und der Informationsabfluss eng zusammenhängen, wurde der Datenabfluss im Hinblick auf zu entwickelnde präventive Maßnahmen einer gesonderten Betrachtung unterzogen (siehe *Tabelle 4)*.

Tabelle 4 Abfluss von Informationen (deutsches Sample)

Art des Informationsabflusses	
Mitnahme von Datenträgern (USB-Sticks, CDs etc.)	32,5 %
Versenden von Daten (z.B. per E-Mail, über eine Cloud)	21,2 %
Mitnahme kopierter und/oder fotografierter Dokumente	14,3 %
Mitnahme von Dokumenten in Papierform (Originale)	13,3 %
Entwenden von Daten auf elektronischem Weg von außen (ohne interne Beteiligung)	1,0 %
Sonstiges	4,4 %
nicht feststellbar	13,3 %

n = 203; Mehrfachnennung möglich. Es wurden nur Fälle aufgenommen, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete.

Ein Großteil der geschützten Geschäftsgeheimnisse aus dem deutschen Sample floss auf elektronischem Wege ab, zum Beispiel über die Mitnahme von Speichermedien wie USB-Sticks, CDs oder externen Laufwerken (32,5 %), das Versenden als Anhang einer E-Mail oder Speichern in einer Cloud (21,2 %). Aber auch im digitalen Zeitalter wurden Dokumente, die Geschäftsgeheimnisse enthielten, in Papierform entwendet (13,3 %) oder kopiert bzw. fotografiert (14,3 %). Das elektronische Entwenden von Daten, bei denen der Zugriff von außen erfolgte, war in den deutschen

Strafverfahren von untergeordneter Bedeutung (1 %). Außentäter, die mit Innentätern kooperierten, sind in der Kategorie „Entwenden von Daten auf elektronischem Wege von außen“ nicht erfasst. Die Kategorie „Sonstiges“ umfasst Fälle, in denen zum Beispiel Laptops oder Aktenordner mitgenommen oder Accounts nach Verlassen des Unternehmens weiter genutzt wurden.

Bei den Fallstudien aus Österreich, der Schweiz und Bulgarien erfolgte der Abfluss von Geschäftsgeheimnissen oftmals aus dem Unternehmen heraus durch das Versenden von Daten, während in den dänischen Fällen mehrfach elektronisch von außen auf Unternehmensdaten zugegriffen wurde. In einem Fall erfolgte der Zugang zum Firmennetzwerk über eine virenverseuchte E-Mail, die ein Mitarbeiter geöffnet hatte und die es den Hackern ermöglichte, Daten auf elektronischem Wege zu entwenden.[41]

4.6 Betroffene Unternehmensgeheimnisse und -branchen

Von besonderem Interesse waren für die Täter aller untersuchten Fälle im In- und Ausland Kundendaten, die für ein Unternehmen von erheblichem Wert sein können. Typische Konstellationen waren, dass Versicherungsvertreter Kundendaten ihres ehemaligen Arbeitgebers nutzten, um Kunden für den neuen Arbeitgeber abzuwerben. In ähnlicher Weise waren kleine Dienstleistungsbetriebe betroffen. Jene können sogar in ihrer Existenz bedroht sein, wenn ein ehemaliger Mitarbeiter einen eigenen Betrieb gründet und mithilfe der Kundendaten große Teile der Stammkundschaft „übernimmt“.[42] Aber auch Vertragsunterlagen, Unternehmensstrategien und technische Daten bzw. Know-how zur Produktentwicklung waren bei den untersuchten Fällen in Deutschland und in den anderen Ländern beliebte Angriffsziele.

Im Gegensatz zu der im Vorfeld der Untersuchung angenommenen Betroffenheit von Unternehmen mit einem hohen Forschungs- und Entwicklungsaufwand oder Unternehmen des Technologiesektors war im deutschen Sample vor allem der Dienstleistungsbereich (mit insgesamt 46,2 %) betroffen, wobei die Branchen „Versicherung, Finanzen, Immobilien“ über ein Drittel ausmachten. Dies kann darauf zurückzuführen sein, dass diese Branchen (überwiegend) wissensintensiv sind und gerade Kundendaten, wie erwähnt, einen hohen Wert haben können. Gründe dafür, dass bestimmte Branchen unterrepräsentiert waren, könnten sein, dass Unternehmen effektive Präventionsmaßnahmen implementiert hatten, (erfolgreiche)

---

41 Vgl. *Fall 1* Dänemark.

42 Strafrechtlich relevant sind solche Fälle dann, wenn der ausscheidende Mitarbeiter die von ihm betreute Kundschaft unter Nutzung der dem ehemaligen Unternehmen gehörenden Kundendatei für sein neues Unternehmen akquiriert, nicht aber, wenn er frei zugängliche Informationsquellen, wie z.B. das örtliche Telefonbuch, nutzt.

Angriffe nicht entdeckt wurden, ein Angriff nicht dem Phänomenbereich der Konkurrenzausspähung zugeordnet oder auf eine Strafanzeige verzichtet wurde.

4.7 Aufdecken von Vorfällen

Für die Entwicklung zielgerichteter Präventionskonzepte in Unternehmen sind jedoch nicht nur Kenntnisse über den Zugang zu oder Abfluss von geschützten Informationen wesentlich, sondern auch darüber, wie die Taten aufgedeckt werden. So wurde in der Untersuchung ein Augenmerk auch darauf gerichtet, ob es in einem der Vergleichsländer möglicherweise besonders vielversprechende Mechanismen der Tataufdeckung gab (siehe *Tabelle 5*).

Tabelle 5 Aufdeckung der Taten (deutsches Sample)

Tataufdeckung	
Hinweis von Dritten mit Kontakt zum geschädigten Unternehmen (z.B. Kunden, Lieferanten, externe Mitarbeiter)	23,1 %
Hinweis von Mitarbeiter	13,7 %
Beobachtung einer auffälligen Verhaltensänderung bei einem Mitarbeiter oder in der Entwicklung eines Mitarbeiters über den gesamten Zeitraum seiner Zugehörigkeit zum Unternehmen	7,9 %
Hinweis von Dritten ohne Bezug zum geschädigten Unternehmen	5,7 %
routinemäßige Kontrolle der Datenströme und Rechneraktivitäten	5,3 %
überraschende Kündigung eines Mitarbeiters	4,0 %
Registrierung verschwundenen (physischen) Materials (inkl. Datenträger)	2,2 %
Entdecken eines Produktes (z.B. bei einer Messe), das eine hohe Ähnlichkeit mit dem Produkt des ausgespähten Unternehmens hat	2,2 %
Meldung durch ein IT-Tool (Intrusion-Detection-Systeme, Firewall-Aktivitäten, unerwartete Rechneraktivitäten, hohe Datenvolumina, Datenströme an externe E-Mail-Accounts etc.)	1,3 %
Entdeckung durch den Datenschutzbeauftragten/Sicherheitsbeauftragten	0,9 %
stichprobenartige Kontrolle von Taschen oder technischen Geräten	0,4 %
Sonstiges	24,9 %
nicht feststellbar	8,0 %

n = 225; Mehrfachnennung möglich. Es wurden nur Fälle aufgenommen, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete.

Die Analyse der deutschen Strafverfahren zeigte, dass der Faktor Mensch nicht nur bei der Tatbegehung, sondern auch bei der Aufdeckung von Straftaten eine wichtige Rolle spielte. Denn ein Großteil der Taten wurde durch menschliche Beobachtungen entdeckt. Dabei waren Dritte mit Kontakt zu dem geschädigten Unternehmen, zum Beispiel Kunden, Lieferanten oder externe Mitarbeiter, besonders wichtig. Aber

auch die eigenen Mitarbeiter, die Hinweise gaben, indem sie z.B. Verhaltensauffälligkeiten bei Kollegen beobachtet hatten, fungierten als wichtige Hinweisgeber bei der Tataufdeckung. Die routinemäßige Kontrolle von Datenströmen und Rechneraktivitäten war für die Entdeckung von Cyberangriffen von Bedeutung. Sehr selten kam es bei einem Cyberdelikt zur Aufdeckung einer Tat durch einen Hinweis von außen (Kategorie „Sonstiges"). So wurde z.B. in Dänemark ein Cyberangriff dadurch bekannt, dass sich ein amerikanisches Unternehmen für Cybersicherheit an das dänische Centre for Cyber Security wandte, nachdem es dänische Dokumente auf einem amerikanischen Server gefunden hatte.[43] In einem anderen Fall war z.B. ein Landesdatenschutzbeauftragter in Deutschland von einem Außenstehenden informiert worden.[44]

Die Ergebnisse der Fallstudien in den Vergleichsländern ähneln jenen der Analyse der deutschen Akten. Bekannt wurden die meisten Fälle entweder durch Hinweise von Mitarbeitern oder Dritten mit oder ohne Kontakt zu dem geschädigten Unternehmen sowie durch die routinemäßige Kontrolle von Datenströmen und Rechneraktivitäten.

In den Bereich „Sonstiges" fallen – neben den genannten Hinweisen von außen – verschiedene Konstellationen, in denen die Tat zufällig durch das geschädigte Unternehmen oder einen Dritten bemerkt wurde oder bei der sich der Täter nachlässig verhielt. In einem Fall entdeckte ein Finanzinstitut fehlerhafte Abbuchungen und informierte das geschädigte Unternehmen.[45] In einem weiteren Fall hatte der Täter bei der Verwendung eines unerlaubt genutzten Formulars vergessen, die Kontaktdaten zu ändern, sodass die geschädigte und nicht die neue Firma des Täters kontaktiert wurde.[46] Immer wieder vergaßen Täter, unerlaubt vervielfältigte Dokumente aus einem Kopiergerät zu entfernen. In dem bereits erwähnten Spionagefall, der im Jahr 2007 die Formel-1-Szene bewegte, wurden zwar keine unerlaubt kopierten Dokumente gefunden, aber der Mitarbeiter eines englischen Copyshops hatte die Ehefrau von *McLarens* Chefdesigner *Mike Coughlan* beim Vervielfältigen von geheimen technischen Informationen von Ferrari beobachtet, die *Nigel Stepney* im Vorfeld an *Mike Coughlan* weitergegeben hatte.[47]

Eine besonders vielversprechende Methode zur Aufdeckung von Fällen konnte allerdings in keinem der Vergleichsländer festgestellt werden. Die Vorgehensweisen waren hier ebenso vielfältig wie die Art des Zugangs der Täter zu geschützten Geschäftsgeheimnissen und der Informationsabfluss.

---

43 Vgl. *Fall 1* Dänemark.

44 Vgl. *Fall 526* Deutschland.

45 Vgl. *Fall 183* Deutschland.

46 Vgl. *Fall 51* Deutschland.

47 Vgl. FiA 2007; *Goren & Noble* 2007.

5. Strafverfolgungspraxis in Fällen von Konkurrenzausspähung und Wirtschaftsspionage

Der folgende Abschnitt widmet sich zunächst den Fragen, wie Wirtschaftsspionage und Konkurrenzausspähung in den untersuchten Ländern reguliert sind, welche strafrechtlichen Konsequenzen jeweils drohen und welche in der Praxis tatsächlich folgten. Dazu werden auch die mit der Verfahrensentscheidung zusammenhängenden Fragen, ob es sich bei dem jeweiligen Delikt um ein Offizial- oder Antragsdelikt handelt oder ob die Möglichkeit des Verweises auf den Privatklageweg besteht, herangezogen. Die Herausforderungen, denen Strafverfolgungsbehörden in nationalen und internationalen Strafverfahren – vor allem bei der (grenzüberschreitenden) Beweiserhebung – gegenüberstehen, werden abschließend diskutiert.

5.1 Rechtsgrundlagen des strafrechtlichen Geheimnisschutzes

Weder in Deutschland noch in den Vergleichsländern existiert ein Straftatbestand der Wirtschaftsspionage oder ein solcher der Konkurrenzausspähung, sodass die Phänomenbereiche jeweils durch unterschiedliche strafrechtliche Normen mit unterschiedlich hohen Strafrahmen geschützt werden. Zwar sind seit dem Inkrafttreten der EU-Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen der Begriff „Geschäftsgeheimnis“ und der entsprechende Schutzbereich innerhalb der EU einheitlich definiert, aber die Strafvorschriften und die Strafrahmen in Fällen von sowohl Wirtschaftsspionage als auch Konkurrenzausspähung unterscheiden sich weiterhin in den einzelnen Mitgliedsstaaten,[48] da das materielle Strafrecht innerhalb der EU nicht harmonisiert ist. Die mit dem Vertrag von Lissabon in Art. 83 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) vereinbarte Möglichkeit, Richtlinien mit Mindestvorschriften zur Festlegung von Straftaten und Strafen zu erlassen, ist auf besonders schwere, grenzüberschreitende Kriminalität, wie z.B. Menschenhandel oder Terrorismus, beschränkt. Die EU-Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen sieht daher, konsequenterweise, keine strafrechtlichen Regelungen vor, sodass der nationale Gesetzgeber zuständig bleibt.

In den in die Untersuchung einbezogenen Ländern können in den fraglichen Phänomenbereichen jeweils verschiedene Straftatbestände aus dem jeweiligen Strafgesetzbuch oder aus strafrechtlichen Nebengesetzen verwirklicht sein. Aus diesem Grund sind in *Tabelle 6* nur die Strafvorschriften angegeben, die den Hauptanwendungsbereich von Wirtschaftsspionage und Konkurrenzausspähung in dem jeweils betroffenen Land abdecken. Zur Abgrenzung von Wirtschaftsspionage und Konkurrenzausspähung wird in der Tabelle gemäß der Handhabung in der Mehrheit der

---

48 Landesberichte zu den Rechtsgrundlagen von Wirtschaftsspionage und Konkurrenzausspähung in allen Mitgliedsstaaten der EU und der Schweiz finden sich in *Carl & Kilchling* 2018.

*Tabelle 6 Übersicht über die Straftatbestände in den untersuchten Ländern (außer Vereinigtes Königreich)**

Land	Phänomen	Strafvorschrift**	Kennzeichen
Bulgarien	Wirtschaftsspionage	Art. 104 StGB	Staatsgeheimnis, das auch einen ökonomischen Bezug haben kann, wird einem fremden Staat oder einer fremden Organisation verraten
	Konkurrenzausspähung	Art. 224 StGB	geschützte Information betrifft ein Wirtschafts- oder Geschäftsgeheimnis
		Art. 284 StGB	geschützte Information wird durch einen Beamten oder einen Mitarbeiter des öffentlichen Dienstes, eines Unternehmens oder einer Organisation offengelegt
Dänemark	Wirtschaftsspionage	§ 107 StGB	Offenlegung eines Geheimnisses, das im dänischen Interesse geheim bleiben sollte, durch oder für den Mitarbeiter eines fremden Nachrichtendienstes oder einer ausländischen Organisation
	Konkurrenzausspähung	§§ 37 Abs. 5, 23 Marketing Practice Act	Offenlegung eines Geschäftsgeheimnisses durch einen Mitarbeiter oder Vertragspartner
		§§ 263 Abs. 3,. 264 Abs. 2 StGB	Offenlegung eines Geschäftsgeheimnisses durch eine natürliche oder juristische Person
Deutschland	Wirtschaftsspionage	§ 99 StGB	Agententätigkeit für einen fremden Staat
	Konkurrenzausspähung	§§ 17–19 UWG (seit April 2019: § 23 GeschGehG)	Verrat eines Geschäftsgeheimnisses durch eine andere Person
Österreich	Wirtschaftsspionage	§ 256 StGB	Agententätigkeit eines fremden Nachrichtendienstes; Tatgegenstand kann auch ein Geschäfts- oder Betriebsgeheimnis sein
		§ 124 StGB	Verwertung eines Geschäfts- oder Betriebsgeheimnisses im Ausland***
	Konkurrenzausspähung	§§ 122–123 StGB	Verletzung eines Geschäfts- oder Betriebsgeheimnisses durch Dritte oder Bedienstete
		§§ 11, 12 UWG	Verletzung eines Geschäfts- oder Betriebsgeheimnisses durch einen Bediensteten
Schweiz	Wirtschaftsspionage	Art. 273 StGB	Zugänglichmachung eines Fabrikations- oder Geschäftsgeheimnisses für einen fremden Staat, ein ausländisches Unternehmen oder eine Organisation
	Konkurrenzausspähung	Art. 162 StGB	Verrat eines Fabrikations- oder Geschäftsgeheimnisses, das infolge einer gesetzlichen oder vertraglichen Pflicht bewahrt werden soll
		Art. 23 UWG	Verwertung oder Mitteilung eines unrechtmäßig ausgekundschafteten Fabrikations- und Geschäftsgeheimnisses

* Eine ausführliche Beschreibung der Straftatbestände findet sich in *Carl & Kilchling* 2018. Vgl. dort zu Bulgarien *Petrova et al.*, zu Dänemark *Afsah*, zu Deutschland *Knickmeier et. al.*, zu Österreich *Konopatsch & Lehmkuhl* und zur Schweiz *Konopatsch et al*.

** Aufgeführt sind die zum Zeitpunkt der Datenerhebung (2016/2017) geltenden Rechtsvorschriften.

*** Der Begriff „Ausland" umfasst nach österreichischem Recht nur Staaten, die nicht Mitglied in der EU sind; vgl. *Bertel et al.* 2018, S. 163.

Vergleichsländer auf die Täterschaft abgestellt. Da in Bulgarien die Tatbestände, wie zuvor beschrieben, nach dem verletzten Geheimnis unterschieden werden, wurden dort die Rechtsvorschriften ausgewählt, bei denen das betroffene Geheimnis den Hauptanwendungsbereich von Wirtschaftsspionage und Konkurrenzausspähung (nach dem in den anderen Ländern üblichen Verständnis) umfasst. Im Vereinigten Königreich wird bei den in die Phänomenbereiche gehörenden Delikten auf unterschiedliche Rechtsakte – zum Beispiel zur Strafbarkeit des Betrugs, Diebstahls, Verrats von Staatsgeheimnissen oder des unerlaubten Zugriffs auf Computer – zurückgegriffen, die sich nicht in die Kategorien von Wirtschaftsspionage und Konkurrenzausspähung einordnen lassen und deshalb in der Tabelle nicht aufgeführt werden.

5.2 Antrags- und Offizialdelikt, Privatklageverfahren

Ob ein strafrechtlich relevanter Vorfall angezeigt wird, kann ebenso wie der Ausgang eines Ermittlungsverfahrens davon abhängen, inwieweit die Strafvorschrift als Antragsdelikt oder Offizialdelikt ausgestaltet ist. Delikte aus dem Bereich der Wirtschaftsspionage sind in allen untersuchten Ländern Offizialdelikte. Bei den Delikten aus dem Bereich der Konkurrenzausspähung ist die rechtliche Einordnung diffiziler.

Während in Deutschland Strafverfolgungsbehörden aufgrund des Legalitätsprinzips (§ 152 Abs. 2 StPO) bei einem Offizialdelikt ein Ermittlungsverfahren einleiten müssen, sobald der Anfangsverdacht einer Straftat vorliegt, ist bei einem Antragsdelikt der Strafantrag des Geschädigten erforderlich, damit die Staatsanwaltschaft tätig wird. Bei relativen Antragsdelikten kann die Staatsanwaltschaft jedoch nach Kenntnisnahme des Falles ohne einen Strafantrag des Geschädigten das öffentliche Interesse bejahen und ein Ermittlungsverfahren einleiten. Der Geschädigte wiederum kann einen Strafantrag in jedem Stadium des Verfahrens zurücknehmen, mit der Folge, dass die Staatsanwaltschaft das Verfahren einstellen muss, sofern sie bei relativen Antragsdelikten das öffentliche Interesse nicht bejaht. Eine Rücknahme des Strafantrags erfolgt regelmäßig nach einer zivil- oder arbeitsgerichtlichen Einigung, da in diesen Fällen der Rechtsfrieden auch ohne eine Entscheidung des Strafgerichts wiederhergestellt ist. Straftaten, denen ein Verrat von Geschäfts- oder Betriebsgeheimnissen gem. §§ 17 ff. UWG zugrunde liegt, sind relative Antragsdelikte.

Die österreichische Rechtsordnung kennt neben den Offizialdelikten, bei denen die Staatsanwaltschaft tätig werden muss, Ermächtigungsdelikte (§ 92 StPO) und Privatanklagedelikte (§ 71 StPO). Ermächtigungsdelikte ähneln den deutschen Antragsdelikten, da die Staatsanwaltschaft erst tätig wird, wenn der Betroffene eine Ermächtigung erteilt. Privatanklagedelikte können hingegen ausschließlich durch den Betroffenen als Privatankläger, nicht aber durch die Staatsanwaltschaft verfolgt werden. Straftaten wegen der Verletzung von Geschäfts- oder Betriebsgeheimnissen (gem. § 122 und § 123 StGB sowie § 11 und § 12 UWG) sind Privatanklagedelikte. Sofern das Geschäfts- oder Betriebsgeheimnis jedoch im Nicht-EU-Ausland ver-

wertet, verwendet oder sonst ausgewertet wird (§ 124 StG), liegt ein Offizialdelikt vor.[49]

In der Schweiz sind Straftaten wegen des Verrats eines Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB) oder wegen der Verwertung oder Mitteilung eines unrechtmäßig ausgekundschafteten Fabrikations- oder Geschäftsgeheimnisses (Art. 23 UWG) Antragsdelikte. Während bei Verstößen gegen Art. 162 StGB nur die verletzte Person einen Antrag stellen kann (Art. 30 Abs. 1 StGB), können bei Verstößen gegen Art. 23 UWG alle gem. Art. 9 und Art. 10 UWG zur Zivilklage Berechtigten, z.B. neben dem (potenziell) Verletzten auch Berufs- oder Wirtschaftsverbände oder Kunden, einen Antrag stellen. Zudem hat der Bund gem. Art. 23 Abs. 3 UWG die Rechte eines Privatklägers.

In Bulgarien sind auch die Strafvorschriften, die in den Bereich der Konkurrenzausspähung fallen, als Offizialdelikt ausgestaltet.

Bei einigen Antragsdelikten, wie dem Verrat von Geschäfts- und Betriebsgeheimnissen (Konkurrenzausspähung), kann die geschädigte Person in verschiedenen Ländern (z.B. in Deutschland, Österreich und der Schweiz) auf den Privatklageweg verwiesen werden. Im Gegensatz zu einem von der Staatsanwaltschaft betriebenen Strafverfahren führt in einem Privatklageverfahren oder Privatanklageverfahren, wie es in Österreich heißt, der Geschädigte das Verfahren, was für ihn einen erheblich höheren Aufwand als bei einem von der Staatsanwaltschaft geführten Strafverfahren bedeutet sowie ein hohes Kostenrisiko birgt, da der Geschädigte die Verfahrenskosten zunächst selbst zu tragen hat. Die Ausgestaltung eines Straftatbestandes als Antragsdelikt zeigt ebenso wie die Möglichkeit, den Geschädigten auf den Privatklageweg zu verweisen, die kriminalpolitisch geringe Bedeutung, die dem strafrechtlich relevanten Verhalten beigemessen wird. Privatklageverfahren sind in diversen Rechtsordnungen bekannt. Sie wurden für Delikte der einfachen Kriminalität, die kaum über das Schutzinteresse des Einzelnen hinausgehen und kein gegenwärtiges Anliegen der Allgemeinheit betreffen, eingeführt,[50] z.B. für Beleidigungen oder einfache Körperverletzungen. Der Wirtschaftsspionage kommt in ihrer Einordnung als Offizialdelikt eine andere Bedeutung zu. Führt man sich jedoch vor Augen, welche Werte bei Unternehmen betroffen sein können und welche Folgen der Verrat eines Unternehmensgeheimnisses auch für den nationalen Wirtschaftsstandort haben kann, ist die Frage zu stellen, ob in Fällen der Konkurrenzausspähung tatsächlich nur die Schutzinteressen des Einzelnen betroffen sind. Gemessen daran, dass in der Schweiz und Österreich Straftaten, bei denen Geschäftsgeheimnisse ins Ausland bzw. Nicht-EU-Ausland abfließen, als Offizialdelikte eingeordnet sind, ist in Deutschland zudem die Frage zu stellen, ob es sinnvoll ist, die Wertigkeit eines

---

49 Zu der Diskussion über die Einordnung von § 124 StGB (Österreich) als Wirtschaftsspionage oder Konkurrenzausspähung siehe *Abschnitt 3*.

50 Vgl. für das deutsche Recht Nr. 86 II RiStBV.

Deliktes davon abhängig zu machen, ob ein fremder Geheimdienst oder ein Konkurrent als Täter in Betracht kommt.

5.3 Gründe für die Einleitung von Ermittlungsverfahren

Wirtschaftsspionage und Konkurrenzausspähung sind, wie beschrieben, durch ein doppeltes Dunkelfeld und verdecktes Hellfeld gekennzeichnet. Dieser Charakterisierung entspricht auch das Ergebnis der im Rahmen des Projektes WiSKoS durchgeführten Dunkelfeldbefragung, in der nur 22 % der befragten Unternehmen angaben, einen verdächtigen Sachverhalt bei der Polizei angezeigt zu haben.[51] Dabei sind Konkurrenzausspähung und Wirtschaftsspionage klassische Anzeigedelikte. In knapp 93 % der deutschen Verfahren zur Konkurrenzausspähung löste eine Strafanzeige die Ermittlungen aus.[52] Ähnlich sieht es in den untersuchten Vergleichsländern aus. Diese Ergebnisse zeigen die funktionale Bedeutung von Strafanzeigen für die Einleitung von Strafverfahren.

5.4 Erledigung der Ermittlungsverfahren in Fällen der Konkurrenzausspähung

Die im Folgenden beschriebenen Ergebnisse deutscher Strafverfahren beziehen sich ausschließlich auf Fälle aus dem Phänomenbereich der Konkurrenzausspähung. Die 713 deutschen Strafverfahren wurden gegen insgesamt 1.085 Beschuldigte geführt und enthielten 1.132 Verfahrensentscheidungen.[53] Da einige Verfahren gegen mehr als einen Beschuldigten geführt wurden, ist die Anzahl der Beschuldigten höher als die der Strafverfahren. Die höhere Anzahl der Verfahrensentscheidungen ist dadurch begründet, dass gegen einen Beschuldigten mehrere Entscheidungen ergangen sein können, z.B. eine Anklage und eine Teileinstellung gem. § 154 StPO, wenn der Beschuldigte mehr als ein Delikt verwirklicht hat.[54]

---

51 Vgl. *Bollhöfer & Jäger* 2018, S. 4, 5.
Zu den Voraussetzungen für eine Kooperation mit Behörden, zu denen auch das Anzeigeverhalten gehört, siehe *Bollhöfer & Jäger* 2018, S. 55–58.

52 Weitere Faktoren für die Auslösung von Ermittlungsverfahren waren Erkenntnisse aus anderen Ermittlungsverfahren (5,6 %) sowie in Einzelfällen Vorermittlungen, Weiterleitungen durch Behörden oder Zufallsfunde.

53 Die Verfahrensentscheidungen enthalten nicht nur Entscheidungen bzgl. Verstößen gegen §§ 17 ff. UWG. In einigen Fällen wurde neben einem Verstoß gegen §§ 17 ff. UWG auch wegen anderer Delikte ermittelt. Dabei kann es zu unterschiedlichen Entscheidungen wegen der betroffenen Delikte gekommen sein.

54 Entscheidungen, bei denen die Staatsanwaltschaft eine Einstellung gem. § 152 Abs. 2 StPO oder §§ 170 Abs. 2 und 374 StPO angegeben hatte, wurden in der Auswertung als eine Entscheidung gem. § 152 Abs.2 StPO oder eine Entscheidung nach § 374 StPO geführt.

5.4.1 Abschluss der Ermittlungsverfahren

Von den in die Untersuchung aufgenommenen Ermittlungsverfahren wegen Verstoßes gegen §§ 17 ff. UWG endeten 65,4 % mit einer Einstellung (siehe *Tabelle 7*). Die Einstellungsquote liegt damit über der von der Staatsanwaltschaftsstatistik ausgewiesenen Einstellungsquote von 31,4 %, die sich auf alle staatsanwaltschaftlichen Verfahrenserledigungen bezieht und das gesamte Spektrum an in Deutschland begangenen Straftaten enthält.[55] Während 10,6 % der Ermittlungsverfahren des deutschen Samples mit dem Antrag auf Erlass eines Strafbefehls oder einer Anklage endeten, lag die Quote bei allen staatsanwaltschaftlichen Verfahrenserledigungen im Jahr 2017 bei 19,6 %.

Tabelle 7 Ermittlungsverfahren in Deutschland: Gegenüberstellung aller staatsanwaltschaftlicher Erledigungen (2017) mit jenen des Samples (2008–2016)*

Verfahrenserledigung	**insgesamt (2017)**	**im Sample (2008–2016)**
keine Aufnahme von Ermittlungen; Einstellung wegen fehlenden Tatverdachts oder Verweises auf den Privatklageweg	31,4 %	65,4 %
Einstellung ohne Auflagen	26,0 %	14,0 %
Einstellung mit Auflagen	3,5 %	8,7 %
Strafbefehl	10,9 %	7,1 %
Anklageerhebung	8,7 %	3,5 %
Sonstiges	19,5 %	1,5 %
	N = 4.858.212	n = 1.132

* Vgl. Statistisches Bundesamt 2018, S. 26.

In den untersuchten exemplarischen Fallstudien der Vergleichsländer wurde ein Großteil der Täter angeklagt. In Bezug auf Österreich ist jedoch zu berücksichtigen, dass dort überwiegend Privatanklagen erhoben wurden, in denen die Staatsanwaltschaft nicht ermittelt hatte. Wie in Deutschland, überwogen in der Schweiz die Einstellungsentscheidungen. Der sich ansonsten von den Ergebnissen der untersuchten Fälle aus Deutschland unterscheidende Ausgang der Ermittlungsverfahren beruht vor allem auf der Auswahl der exemplarischen Fallstudien, die bestimmten Kriterien unterlag (siehe *Abschnitt 2.3*).

5.4.2 Einstellungsentscheidungen im deutschen Sample

Tabelle 8 enthält einen Überblick über die unterschiedlichen Gründe für die Einstellungsentscheidungen der Staatsanwaltschaft zum Abschluss des Ermittlungsverfah-

55 Vgl. Statistisches Bundesamt 2018, S. 26.

rens im deutschen Sample. Bei den in die Untersuchung einbezogenen Strafverfahren hat die Staatsanwaltschaft in 7,5 % der Ermittlungsverfahren gem. § 152 Abs. 2 StPO von der Durchführung von Ermittlungen abgesehen, da der vorgetragene Sachverhalt kein strafrechtlich relevantes Verhalten enthielt. Auch wenn querulatorische Verfahren[56] im Vorfeld der Untersuchung erwartet wurden, überraschte die verhältnismäßig hohe Anzahl der Einstellungsentscheidungen nach § 152 Abs. 2 StPO. Eine mögliche Erklärung kann sein, dass versucht wurde, einer zivil- oder arbeitsgerichtlichen Auseinandersetzung mit einem Strafantrag (erfolglos) Nachdruck zu verleihen. Insgesamt ca. 30 % der Beschuldigten waren parallel in ein privatrechtliches Verfahren involviert. 13,5 % der Beschuldigten waren neben dem Strafverfahren an einem zivilgerichtlichen Verfahren und 17,5 % der Beschuldigten an einem arbeitsgerichtlichen Verfahren beteiligt. Auch wenn es rechtlich nicht ausgeschlossen ist, dass ein Beschuldigter gleichzeitig arbeits- und zivilrechtlich verklagt wird, kann davon ausgegangen werden, dass entweder ein arbeitsgerichtliches oder ein zivilgerichtliches Verfahren geführt wurde.

Tabelle 8 Einstellungsentscheidungen der Staatsanwaltschaft am Ende des Ermittlungsverfahrens (deutsches Sample)

Einstellungsentscheidung	**Anzahl**
keine Ermittlungen aufgenommen gem. § 152 Abs. 2 StPO	85 (7,5 %)
Einstellung wegen fehlenden hinreichenden Tatverdachts gem. § 170 Abs. 2 StPO oder Verweis auf den Privatklageweg gem. § 374 StPO	655 (57,6 %)
Einstellung wegen Geringfügigkeit gem. § 153 SPO	118 (10,4 %)
Einstellung nach Erfüllung von Auflagen gem. § 153a StPO	98 (8,7 %)
anderes Ergebnis, z.B. Einstellung nach § 154, § 153d oder § 205 StPO	57 (5,0 %)
n = 1.132 Verfahrensentscheidungen	

Insgesamt knapp 58 % der Ermittlungsverfahren des deutschen Samples wurden wegen fehlenden hinreichenden Tatverdachts gem. § 170 Abs. 2 StPO eingestellt oder das geschädigte Unternehmen wurde auf den Privatklageweg (gem. § 374 StPO) verwiesen. Während einige Staatsanwaltschaften das Verfahren gem. § 170 Abs. 2 StPO einstellten und den Geschädigten auf den Privatklageweg verwiesen, basierten die Entscheidungen anderer Staatsanwaltschaften ausschließlich auf einem Verweis auf den Privatklageweg (§ 374 StPO). Daher wurden die Einstellungen nach § 170 Abs. 2 StPO und die nach § 374 StPO in einer Kategorie zusammengefasst. Der Verweis auf den Privatklageweg erfolgte in unterschiedlichen Stadien des Ermittlungsverfahrens. Während manche Staatsanwälte im Wege der Sachverhaltsaufklä-

---

56 Ein querulatorisches Verfahren war z.B. die Strafanzeige wegen Verstoßes gegen § 17 UWG gegen einen Einzelhändler, bei dem die als Sonderangebot angepriesenen XXL-Packungen Spinat bereits ausverkauft waren (vgl. *Fall 98* Deutschland).

rung gem. § 160 StPO zunächst konkrete Ermittlungen durchführten und am Ende ihrer Ermittlungen den Geschädigten auf den Privatklageweg verwiesen, da kein öffentliches Interesse erkennbar war, nutzten andere Staatsanwälte die Möglichkeit zum Verweis auf den Privatklageweg, bevor sie Ermittlungsmaßnahmen einleiteten. Beide Möglichkeiten sind rechtlich vertretbar und können inhaltlich geboten sein. Sie können aber auch dazu führen, dass dem geschädigten Unternehmen zusätzliche Hürden auferlegt werden, indem es selbst Beweise vorlegen muss, ohne über dieselben Eingriffsmöglichkeiten in Rechte der Beschuldigten wie die Staatsanwaltschaft zu verfügen. Eine einheitliche Linie war beim Verweis auf den Privatklageweg nicht erkennbar. Inwieweit Geschädigte den Privatklageweg tatsächlich beschritten haben, konnte nicht ermittelt werden.[57] Aufgrund des beschriebenen höheren Aufwands und Kostenrisikos ist von einer geringen Zahl auszugehen.

Die eingestellten Verfahren betrafen nicht nur Fälle, in denen ein Täter – z.B. nach einem Hackerangriff – nicht ermittelt oder die Tat nicht nachgewiesen werden konnte oder der Betroffene auf den Privatklageweg verwiesen wurde, sondern auch solche Konstellationen, in denen ein Strafantrag nach einer Einigung im arbeits- oder zivilgerichtlichen Verfahren zurückgenommen wurde. So war in manchen Strafverfahren in Deutschland und den Vergleichsländern zwar der Ärger eines Unternehmens über einen (ehemaligen) Mitarbeiter groß, aber die entwendeten Daten waren entweder nicht geheim gewesen oder aufgrund einer erteilten Einwilligung legal auf einem anderen Datenträger gesichert worden, sodass keine Strafbarkeit gegeben war.

In 10,4 % der Ermittlungsverfahren entschied die Staatsanwaltschaft, das Verfahren wegen Geringfügigkeit gem. § 153 StPO ohne Auflagen einzustellen. Insgesamt 8,7 % der eingeleiteten Verfahren endeten mit einer Einstellung gegen Zahlung einer Geldauflage gem. § 153a StPO. Andere Ergebnisse umfassten zum Beispiel eine Teileinstellung gem. § 154 StPO, das Absehen von der Verfolgung bei Staatsschutzdelikten wegen überwiegender öffentlicher Interessen gem. § 153d StPO oder eine Einstellung des Verfahrens wegen eines vorübergehenden Hindernisses gem. § 205 StPO.

5.5 Strafrahmen und Ausgang der Strafverfahren

Mangels eines harmonisierten Strafrechts in der EU unterscheiden sich nicht nur die Strafrahmen von Wirtschaftsspionage und Konkurrenzausspähung innerhalb eines Landes, sondern zudem die Strafrahmen der Vergleichsländer untereinander (siehe *Tabelle 9*). Dabei fällt der Wirtschaftsspionage mit einer höheren Strafandrohung eine größere Bedeutung zu als der Konkurrenzausspähung, die zudem oft in strafrechtlichen Nebengesetzen geregelt ist (so in Dänemark, Deutschland, Österreich, der Schweiz).

---

57 Die als Privatklage geführten Verfahren werden bei den zuständigen Gerichten unter einem anderen Aktenzeichen als die vorangegangenen Ermittlungsverfahren bei der Staatsanwaltschaft geführt.

*Tabelle 9 Strafrahmen bei Wirtschaftsspionage und Konkurrenzausspähung (in den untersuchten Ländern außer dem Vereinigten Königreich)**

Land	Phänomen	Strafvorschrift	Strafrahmen**
Bulgarien	Wirtschaftsspionage	Art. 104 StGB	10 bis 20 Jahre oder lebenslängliche Freiheitsstrafe
	Konkurrenzausspähung	Art. 224 StGB	Geldstrafe oder bis zu 5 Jahren Freiheitsstrafe
		Art. 284 StGB	bis zu 2 Jahren Freiheitsstrafe
Dänemark	Wirtschaftsspionage	§ 107 StGB	bis zu 16 Jahren Freiheitsstrafe
	Konkurrenzausspähung	§ 37 Abs. 5, § 23 Marketing Practices Act	Geldstrafe oder bis zu 18 Monaten Freiheitsstrafe
		§§ 263, 264 StGB	bis zu sechs Jahren Freiheitsstrafe
Deutschland	Wirtschaftsspionage	§ 99 StGB	Geldstrafe oder bis zu 5 Jahren Freiheitsstrafe
	Konkurrenzausspähung	§§ 17–19 UWG (seit April 2019: § 23 GeschGehG)	Geldstrafe oder bis zu 3 Jahren Freiheitsstrafe
Österreich	Wirtschaftsspionage	§ 256 StGB	Geldstrafe oder bis zu 3 Jahren Freiheitsstrafe
		§ 124 StGB	Geldstrafe oder bis zu 3 Jahren Freiheitsstrafe
	Konkurrenzausspähung	§§ 122–123 StGB	Geldstrafe oder bis zu 6 Monaten (§ 122 StGB) bzw. 2 Jahren (§ 123 StGB)
		§ 11 UWG	Geldstrafe oder bis zu 3 Monaten Freiheitsstrafe
Schweiz	Wirtschaftsspionage	§ 273 StGB	Geldstrafe oder bis zu 3 Jahren Freiheitsstrafe
	Konkurrenzausspähung	§ 162 StGB, § 23 UWG	Geldstrafe oder bis zu 3 Jahren Freiheitsstrafe

* Aufgeführt sind die zum Zeitpunkt der Datenerhebung (2016/2017) geltenden Rechtsvorschriften.

** Die Strafrahmen enthalten die Mindest- und Höchstandrohung des Grunddelikts und beziehen sich nicht auf schwere Fälle mit einer erhöhten Mindest- oder Höchstandrohung.

Bei der Wirtschaftsspionage reichen die Strafrahmen von mindestens einer Geldstrafe (Deutschland, Österreich, Schweiz) bis zu lebenslänglicher Freiheitsstrafe (Bulgarien).[58] Bei der Konkurrenzausspähung ist die Mindeststrafe in allen untersuchten Ländern eine Geldstrafe; die Höchststrafen rangieren zwischen fünf Jahren Freiheitsstrafe in Bulgarien und drei Monaten Freiheitsstrafe in Österreich. Neben einer Geld- und Freiheitsstrafe für den Täter können nach den Rechtsordnungen in Däne-

58 Die Einteilung der bulgarischen Straftatbestände in die Kategorien Wirtschaftsspionage und Konkurrenzausspähung erfolgte nach der in Deutschland gebräuchlichen Definition.

mark, Österreich, der Schweiz und dem Vereinigten Königreich die Unternehmen als juristische Personen strafrechtlich zur Verantwortung gezogen werden. Auch wenn in Deutschland kein Unternehmensstrafrecht existiert, können gegen Unternehmen Geldstrafen nach dem Ordnungswidrigkeitenrecht verhängt werden.[59] In Bulgarien können Verwaltungsbehörden neben der Kriminalstrafe durch die Strafgerichtsbarkeit zusätzlich Verwaltungsstrafen in Form von Geldstrafen verhängen.[60]

5.5.1 Ausgang der Strafverfahren (Deutschland)

Die Strafverfahren des deutschen Samples (Fälle der Konkurrenzausspähung), bei denen ein Gericht an der Entscheidung beteiligt war (Einstellung gem. § 153a StPO, Strafbefehl, angeklagte Taten), endeten am häufigsten mit einer Geldauflage gem. § 153a StPO (11,0 % aller Verfahrensentscheidungen) oder einer Geldstrafe (4,9 % aller Verfahrensentscheidungen). Die Geldauflagen gem. § 153a StPO reichten von EUR 150 bis EUR 45.000. Am häufigsten wurden Geldauflagen i.H.v. EUR 500 (17 Fälle), EUR 1.000 (15 Fälle), EUR 1.500 (12 Fälle) und EUR 2.000 (12 Fälle) verhängt. In keinem einzigen Fall wurde eine Freiheitsstrafe ohne Bewährung verhängt und in nur fünf Fällen, also in 0,4 % aller Verfahrensentscheidungen, wurde der Täter zu einer Freiheitsstrafe verurteilt, die zur Bewährung ausgesetzt wurde (siehe *Tabelle 10*). In einem dieser Fälle beschränkte man sich durch eine Verständigung zwischen den Prozessbeteiligten und dem Gericht in der Hauptverhandlung gem. § 257c StPO bei der Verurteilung auf die neben dem Verrat von Geschäfts- oder Betriebsgeheimnissen angeklagten Delikte des Diebstahls und der Unterschlagung.

Tabelle 10 Rechtskräftige Entscheidungen (deutsches Sample)

Rechtsfolge	**Anzahl der Verfahren**	**Anteil an allen Verfahrensentscheidungen (n = 1.132)**
Geldauflage, gem. § 153a StPO	124	11,0 %
Verwarnung mit Strafvorbehalt	3	0,3 %
Geldstrafe	55	4,9 %
Freiheitsstrafe mit Bewährung	5	0,4 %
Freispruch	11	1,0 %
andere Ergebnisse	16	1,4 %

5.5.2 Ausgang der Strafverfahren (Vergleichsländer)

Ähnliche Rechtsfolgen hatten die in den Vergleichsländern geführten Strafverfahren in Fällen der Konkurrenzausspähung. In Österreich wurde ein Großteil der Ver-

59 Vgl. *Hellmann* 2018, S. 364.

60 Vgl. *Petrova et al.* 2018.

fahren, in denen der Täter angeklagt wurde, eingestellt, z.B. nach der Rücknahme von Privatanklagen. In einem Fall wurde der Täter in Österreich neben einer Bewährungsstrafe zu Schadensersatz verurteilt. Wie im deutschen Adhäsionsverfahren können in Österreich in einem Strafverfahren privatrechtliche Ansprüche geltend gemacht werden (§ 67 StPO). Bei einer Verurteilung des Täters fällt das Gericht zugleich eine Entscheidung über jene. In Bulgarien wurde zudem von der rechtlichen Möglichkeit Gebrauch gemacht, eine Verwaltungsstrafe oder eine Geld- neben einer Bewährungsstrafe zu verhängen. Die in der Schweiz bestehende und in den dortigen Fällen gern gewählte Nichtanhandnahmeverfügung gem. Art. 310 StPO ergeht, wenn das Ermittlungsergebnis das Verfahren erfolglos erscheinen lässt. Die Nichtanhandnahmeverfügung kommt einem Freispruch gleich.[61] Nur in zwei Fällen des dänischen Samples, die allerdings dem Bereich der Wirtschaftsspionage zuzuordnen sind, wurden die Täter zu einer Freiheitsstrafe ohne Bewährung verurteilt.

5.6 Ausgewählte Herausforderungen für Strafverfolgungsbehörden in Ermittlungsverfahren wegen Konkurrenzausspähung und Wirtschaftsspionage

Die hohe Zahl an Verfahrenseinstellungen und die geringe Verurteilungsquote können in Deutschland, Österreich und der Schweiz zum Teil auf die Möglichkeit des Verweises auf den Privatklageweg/die Privatanklage zurückgeführt werden. In den anderen Fällen ist jedoch fraglich, ob der erhobene Vorwurf haltlos oder nicht substantiiert war oder ob die zulässigen Beweismittel an ihre (nationalen) Grenzen stießen oder unverhältnismäßig gewesen wären. Im Folgenden werden Schwierigkeiten bei der Strafverfolgung, z.B. bei der grenzüberschreitenden Zusammenarbeit von Strafverfolgungsbehörden oder Strafverfolgungsbehörden mit ausländischen Unternehmen, Beweisschwierigkeiten und die Herausforderungen bei der Ermittlung im Fall von Cyberangriffen diskutiert.

5.6.1 Grenzüberschreitende Kooperation von Strafverfolgungsbehörden

Auch wenn sich die Annahme im Vorfeld der Untersuchung, dass der Phänomenbereich für grenzüberschreitende Straftaten prädestiniert ist, in dem untersuchten deutschen Sample und den Fallstudien des verglichenen Auslands nicht bestätigt hat,[62] stehen Ermittlungen mit Auslandsbezug regelmäßig vor rechtlichen oder praktischen Hürden.

In einem wirtschaftlich interessanten Fall von Konkurrenzausspähung mit einer mutmaßlich hohen Schadenssumme wurden die Ermittlungen unter Verweis auf den

---

61 Vgl. *Omlin* 2010, Art. 310 StPO, Rn. 6, 7.

62 Nur 6,4 % der Fälle des deutschen Samples hatten einen Auslandsbezug.

Privatklageweg eingestellt, nachdem Zuständigkeitsstreitigkeiten nicht abschließend geklärt werden konnten.[63] Die geschädigte Firma hatte durch ein (zivilgerichtliches) selbstständiges Beweisverfahren gem. §§ 485 ff. ZPO Beweise gesichert, bevor sie den Vorfall bei einer deutschen Staatsanwaltschaft anzeigte. Diese wiederum hielt eine Staatsanwaltschaft in Österreich für zuständig, da die Beschuldigten Österreicher waren, das geschädigte Unternehmen seinen Hauptsitz in Österreich hatte und ein Tatort in Deutschland nicht sicher ausgemacht werden konnte. Die österreichische Staatsanwaltschaft lehnte eine Übernahme des Verfahrens ab, da der angezeigte Vorfall in Österreich ein Privatanklagedelikt sei, bei dem die Staatsanwaltschaft nicht ermittle. Die deutsche Staatsanwaltschaft stellte daraufhin das Verfahren ein, ohne eigene Ermittlungen durchzuführen, und verwies das geschädigte Unternehmen auf den Privatklageweg. Zwar ist dieses Ergebnis rechtlich nicht zu beanstanden, aber in vergleichbaren, sich ausschließlich auf nationaler Ebene abspielenden Fällen waren Ermittlungen der Staatsanwaltschaft erfolgt.

Die Kooperation mit ausländischen Behörden kann (zeit-)aufwendig sein, sodass sich die Frage nach dem Kosten-Nutzen-Verhältnis stellt. In einem Fall hatten sich die Beschuldigten vor ihrem durch eigene Kündigung veranlassten Ausscheiden für das Unternehmen existenzwichtige Daten kopiert, die sie bei ihrem neuen Arbeitgeber, einem im Ausland sitzenden und sich im Aufbau befindlichen Konkurrenten, verwendeten.[64] Das Verfahren wurde letztendlich wegen der schwierigen Beweislage nach drei Jahren aus verfahrensökonomischen Gründen mit dem Erlass eines Strafbefehls beendet, in dem eine hohe Geldstrafe verhängt wurde. Eine ähnliche Möglichkeit zur Lösung von Fällen mit Auslandsbezug, in denen die notwendigen Ermittlungen mit viel Aufwand verbunden und eher wenig erfolgsversprechend sind oder die Durchführung der Hauptverhandlung aufgrund von aus dem Ausland zu ladenden Zeugen langwierig werden kann, ist eine Verständigung zwischen dem Gericht und den Verfahrensbeteiligten gem. § 257c StPO.[65]

Das Fehlen bilateraler Kooperationsabkommen kann die grenzüberschreitende Strafverfolgung erschweren oder sogar unmöglich machen. So kann zum Beispiel die Auslieferung eines Verdächtigen aus dem Ausland, die Verurteilung von im Ausland befindlichen Tätern nach nationalem Recht oder die Anerkennung von im Ausland gewonnener Beweise vor nationalen Gerichten ausgeschlossen sein.

Der Fall der österreichischen Firma AMSC Windtech, eines Tochterunternehmens des US-amerikanischen Konzerns American Superconductor, verdeutlich in dem Zusammenhang nicht nur, was für schwerwiegende Folgen der Verrat von Geschäftsgeheimnissen für ein Unternehmen und seine Mitarbeiter haben kann, sondern auch strafpro-

---

63 Vgl. *Fall 48* Deutschland.

64 Vgl. *Fall 567 & 568* Deutschland.

65 Von den Strafverfahren in Deutschland, die vor Gericht verhandelt wurden, endeten ca. 20 % (aus unterschiedlichen Gründen) mit einer solchen Verständigung.

zessuale Grenzen auf internationaler Ebene. Das chinesische Unternehmen Sinovel, ein langjähriger Kunde von AMSC Windtech, bot im Jahr 2011 einem AMSC Windtech-Mitarbeiter eine Zahlung von EUR 15.000 und einen hoch dotierten Job bei einem Tochterunternehmen von Sinovel an.[66] Im Gegenzug erhielt Sinovel den Quellcode einer Steuerungssoftware, die es dem Unternehmen ermöglichte, Windkrafträder selbst zu bauen und in Betrieb zu nehmen, ohne weiter die teuren Lizenzgebühren zahlen zu müssen. Bei AMSC Windtech brachen durch den Wegfall des wichtigsten Kunden die Gewinne ein. In der Folge mussten weltweit über 700 Stellen des Unternehmens abgebaut werden und der Aktienkurs hat sich bis heute nicht von dem Vorfall erholt.[67] Der Täter wurde in Österreich zu einer dreijährigen Haftstrafe und zudem EUR 200.000 Schadensersatz[68] verurteilt.[69] Die Firma Sinovel wurde im Jahr 2018 wegen Datendiebstahls und Betrugs von einem amerikanischen Gericht zu einer Geldstrafe von USD 1,5 Millionen verurteilt.[70] Die Täter aus China blieben straflos, da weder nach österreichischem noch nach amerikanischem Recht eine Verurteilung *in absentia* möglich ist. Gegen den in Österreich verurteilten Täter erging in den Vereinigten Staaten aufgrund seiner Abwesenheit ebenfalls kein (weiteres) Urteil. Die Durchführung eines Strafverfahrens in den Vereinigten Staaten und eine erneute Verurteilung des Täters wegen derselben Tat wären jedoch möglich gewesen, weil Österreich und die Vereinigten Staaten einen etwaigen Strafklageverbrauch rechtlich nicht geregelt haben. Da der Grundsatz *ne bis in idem* (Strafklageverbrauch) jedoch in Art. 6 des Auslieferungsabkommens zwischen Österreich und den Vereinigten Staaten von Amerika geregelt ist, wurde der in Österreich rechtskräftig verurteilte Täter nicht an die Vereinigten Staaten ausgeliefert.[71]

In einem weiteren Fall hatte ein Chinese in einem börsennotierten deutschen Unternehmen während seiner Zeit als Mitarbeiter Informationen gesammelt, die den Nachbau von Produkten in China ermöglichten.[72] Nach der Durchsuchung seiner Wohn- und Geschäftsräume reiste der Verdächtige „fluchtartig" nach China. Die Fahndung verlief erfolglos, das Verfahren musste aufgrund eines Verfahrenshindernisses (Abwesenheit des Beschuldigten) gem. § 205 StPO analog[73] vorläufig und nach Eintritt der Verjährung gem. § 170 Abs. 2 StPO eingestellt werden.

---

66 Vgl. *Budras* 2014.

67 Vgl. US Department of Justice 2018a.

68 Da das geschützte Geschäftsgeheimnis im Nicht-EU-Ausland verwertet wurde, lag gem. § 124 StGB (Österreich) kein Privatanklagedelikt, sondern ein Offizialdelikt vor.

69 Vgl. *Zirm* 2013.

70 Vgl. US Department of Justice 2018a; US Department of Justice 2018b.

71 Sollte der in Österreich verurteilte Täter in die Vereinigten Staaten von Amerika reisen, wäre ein erneuter Strafprozess grundsätzlich möglich.

72 Vgl. *Fall 369* Deutschland.

73 *Fall 369* Deutschland stammt aus dem Jahr 2008, als § 154f StPO, der in solchen Fällen für die Einstellung einschlägig ist, noch nicht in die StPO eingeführt worden war und § 205 StPO analog angewendet wurde.

In Deutschland wurde bei Verstößen wegen des Verrats von Geschäfts- und Betriebsgeheimnissen auf (internationalen) Messen, bei denen ein Haftbefehl unverhältnismäßig gewesen wäre, zum Teil eine Sicherheitsleistung einbehalten, um zu verhindern, dass ausländische Täter straflos ausreisen.[74] Wenn der Täter dann in sein Heimatland zurückreiste, wurde das Verfahren gegen eine Geldauflage (in Höhe der Sicherheitsleistung) nach § 153a StPO eingestellt.

5.6.2 Grenzüberschreitende Kooperation zwischen Strafverfolgungsbehörden und ausländischen Unternehmen

Sofern zwischen zwei Staaten ein Rechtshilfeabkommen besteht, auf dessen Grundlage z.B. Zugang zu Beweismitteln in anderen Staaten möglich ist, kann die Bearbeitung eines förmlichen Rechtshilfeersuchens aufgrund des aufwendigen Verfahrens Monate dauern. Während dieser Zeit laufen andere Fristen, z.B. die von Unternehmen zu wahrenden Speicherfristen für Daten, weiter und gegebenenfalls ab. Da bei der Speicherung von Daten berechtigte Interessen Dritter betroffen sind, stehen Staaten gerade in Zeiten weltweit möglicher Cyberangriffe vor der Herausforderung, sich auf Verfahren für eine zeitnahe Umsetzung von Ermittlungsmaßnahmen in Strafsachen zu einigen.

Der folgende Fall verdeutlicht die Folgen der (notwendigerweise) befristeten Speicherung von Daten, wenn trotz aller Bemühungen die Ermittlungen länger dauern, als Daten gespeichert werden. Bei einem Cyberangriff gegen ein in Deutschland ansässiges börsennotiertes Unternehmen versuchte jenes erfolglos, den Täter selbst zu identifizieren, indem es zum Schein an von ihm angebotenen Kundendaten Interesse zeigte.[75] Für seine Aktivitäten nutzte der Täter eine E-Mail-Adresse über einen Provider in Israel und einen Messenger-Dienst mit Sitz in Luxemburg. Die ermittelnde Staatsanwaltschaft bat diesen um die Bekanntgabe der Benutzerdaten des Anrufers. Diesem Antrag konnte nicht entsprochen werden, da der Täter einen sogenannten Displaynamen nutzte. Als die Staatsanwaltschaft den Benutzernamen, den der Täter zur Registrierung bei diesem Dienst angegeben hatte,[76] ermittelt und daraufhin die E-Mail-Adresse des Täters erhalten hatte, war ein Rechtshilfeersuchen zur Datenabfrage in Israel nicht mehr möglich, da die Taten mehr als sechs Monate zurücklagen und die Daten nicht mehr gespeichert waren.

---

74 Vgl. z.B. *Fall 269* Deutschland.

75 Vgl. *Fall 12* Deutschland.

76 Im vorliegenden Fall entsprach der Displayname, der anderen Benutzern angezeigt wird, nicht dem Benutzernamen, mit dem sich der Täter bei dem Messenger-Dienst registriert hatte.

5.6.3 Beweisschwierigkeiten

Sofern in den untersuchten Strafverfahren Ermittlungen durchgeführt wurden, ergriffen die Strafverfolgungsbehörden die ihnen zur Verfügung stehenden strafprozessualen Ermittlungsmaßnahmen, wie die Vernehmung von Zeugen und Beschuldigten, die Durchsuchung von Wohn- und/oder Geschäftsräumen sowie die Beschlagnahme von technischen Geräten und in anderer Form gespeicherten Informationen. In der Gesamtschau der untersuchten Strafverfahren konnte festgestellt werden, dass, sofern Schwierigkeiten der Beweisführung aktenkundig waren, diese selten auf das Verbot bestimmter Beweiserhebungsmethoden zurückgeführt werden konnten. Im Ergebnis konnte nicht in jedem Fall bei Abschluss der Ermittlungen ein Täter festgestellt oder die einem mutmaßlichen Täter vorgeworfene Straftat bewiesen werden. Gründe dafür waren z.B. der Ablauf von Speicherfristen (siehe *Abschnitt 5.6.2*).

Bei einigen eingestellten Verfahren stellte sich die Frage, ob mit den gegenwärtig zulässigen Beweiserhebungsmethoden kein Nachweis möglich gewesen oder ob die verdächtige Person wirklich unschuldig war. So gab es im deutschen Sample z.B. den Fall einer Organisation, die vermutete, dass über eine Mitarbeiterin während ihres Auslandsaufenthaltes geschützte Daten abgeflossen waren.[77] Obwohl die digitalforensische Untersuchung des Mobiltelefons ohne Hinweis auf eine Straftat blieb, war man sich auf Grundlage der Gesamtumstände des Falles nicht sicher, ob der Verdacht nicht doch begründet war. Da es jedoch an dem für eine Anklage erforderlichen hinreichenden Tatverdacht fehlte, wurde das Verfahren gem. § 170 Abs. 2 StPO eingestellt.

Eine wesentliche Beweisfrage ist in Fällen, in denen der Verdacht der Wirtschaftsspionage besteht, ob der Täter tatsächlich Mitarbeiter eines ausländischen Geheimdienstes war oder ein Geschäftsgeheimnis für das Nicht-EU-Ausland auskundschaftete – ein Tatbestandsmerkmal, das schwer zu beweisen ist. Wie zuvor erläutert, sind in den untersuchten Ländern die Strafandrohungen höher, wenn ein fremder Staat hinter der Tat steckt oder das Geheimnis für das Nicht-EU-Ausland ausgekundschaftet wird. Gerade bei aus China stammenden Tätern wird zwar oft vermutet, dass sie im Auftrag ihres Staates tätig sind, aber der Beweis dafür ist kaum zu führen. Fehlt es in Deutschland an einem hinreichenden Tatverdacht der Agententätigkeit i.S.d. § 99 StGB, wird aus einem Delikt der Wirtschaftsspionage konsequenterweise ein Delikt der Konkurrenzausspähung mit einer niedrigeren Strafandrohung, und in einigen Ländern folgt daraus die Notwendigkeit eines Strafantrags sowie die Möglichkeit, den Geschädigten auf den Privatklageweg zu verweisen.

---

77 Vgl. *Fall 652* Deutschland.

5.6.4 Ermittlungsprobleme bei Cyberangriffen

Die erste Herausforderung bei Cyberdelikten ist die Entdeckung des Angriffs. In den analysierten Fällen wurde ein solcher entweder im Zuge interner Kontrollen oder von Mitarbeitern registriert, die interne Vorgänge genau beobachteten und entsprechende Hinweise gaben.

Ist der Angriff entdeckt, stellt sich zunächst die Frage nach seiner konkreten Ausgestaltung und seinem tatsächlichen Schadenspotenzial. Die Möglichkeiten einer eigenen, technisch umfangreichen Ermittlung, deren Ausgang ungewiss ist, haben vor allem kleinere KMU oft nicht, da ihnen häufig die Ressourcen für die Aufarbeitung von Cyberangriffen fehlen. Das folgende Beispiel zeigt exemplarische Probleme bei Ermittlungen im Fall von Hackerangriffen. Ein Unternehmen in Deutschland, das als Verschlusssache eingestufte Produkte herstellte, zeigte einen Angriff via Phishing-E-Mails sowie das Einschleusen von Schadsoftware in das Unternehmensnetzwerk an.[78] Aufgrund des Geheimhaltungsinteresses an den Produkten wurde von den Strafverfolgungsbehörden gem. § 100g Abs. 1 StPO eine Maßnahme zur Erhebung von Verkehrsdaten eingerichtet. Sie wurde jedoch nicht aktiviert, nachdem die Behörden ermittelt hatten, dass die Schadsoftware nicht konkret auf das Unternehmen zugeschnitten war, was eine besondere Gefährdung bedeutet hätte. Inwieweit die Phishing-E-Mails, die nicht in erkennbarem Zusammenhang mit der Schadsoftware standen, Inhalt eines mehrstufigen Hackerangriffs waren, wurde seitens der Behörden nicht weiterermittelt, da über die Phishing-E-Mails kein Zugang erfolgt war.

Der Prozess, ein entdecktes Datenleck zu beheben, kann viel Zeit in Anspruch nehmen, sodass Daten weiter ungehindert abfließen können. Für die Täter in Fällen professioneller Cyberattacken ist es oft genug ein Leichtes, ihre Spuren so zu verwischen, sodass sie nicht identifiziert werden können, gerade wenn die Angriffe auf Unternehmensnetzwerke von Orten außerhalb der EU gesteuert werden. Solange ein konkreter Täter nicht ermittelt werden kann, werden die „gegen Unbekannt" geführten Verfahren gem. § 170 Abs. 2 StPO (vorläufig) eingestellt.[79]

Das (erfolgreiche) Verwischen von Spuren kann sogar dazu führen, dass Unschuldige fälschlicherweise unter Verdacht geraten und unter Umständen schwerwiegenden strafprozessualen Maßnahmen ausgesetzt sind. In einem der untersuchten deutschen Verfahren informierte die amerikanische Bundespolizei (FBI) ein in Deutschland ansässiges Unternehmen darüber, dass auf einem vom FBI überwachten Server in Amerika vertrauliche Daten des Unternehmens entdeckt worden waren und mög-

---

78 Vgl. *Fall 251* Deutschland.

79 Bei vorläufig eingestellten Verfahren können bis zum Ablauf der Verfolgungsverjährung die Ermittlung jederzeit wieder aufgenommen werden. Ist eine Verjährung eingetreten, bevor ein Täter ermittelt wurde, wird das Verfahren gem. § 170 Abs. 2 StPO endgültig eingestellt.

licherweise unter Mitwirkung des Täters von einem chinesischen Mitbewerber eingesehen werden konnten.[80] Verdächtigt wurde der Mitarbeiter eines externen Dienstleisters des geschädigten Unternehmens. Während des Ermittlungsverfahrens wurden seine Wohn- und Geschäftsräume durchsucht und er saß wegen Fluchtgefahr sechs Wochen in Untersuchungshaft. Nachdem sich der Verdacht erhärtete, dass ein unbekannter Dritter den Account des Beschuldigten unbefugt genutzt hatte, wurde das Verfahren gegen den Beschuldigten gem. § 170 Abs. 2 StPO eingestellt. Der unbekannte Hacker konnte nicht ermittelt werden, während der ursprünglich verdächtigte externe Mitarbeiter während des laufenden Ermittlungsverfahrens erhebliche Einschränkungen seiner persönlichen Freiheit und seines Rechts auf die Unverletzlichkeit der Wohnung hinnehmen musste.

Falsche Verdächtigungen sind nur eine der möglichen Fehlerquellen der digitalen Beweiserhebung. Zur Gewährleistung der Einhaltung fundamentaler Grundsätze eines fairen Strafverfahrens sind Beweismittel unter Einhaltung rechtsstaatlicher Vorschriften verwertbar vor das zuständige Gericht zu bringen, das im Falle von unzulässigen Beweiserhebungen einen Beweisantrag gem. § 244 StPO ablehnen muss bzw. unzulässig erhobene Beweismittel nicht verwerten darf. Die Beweiserhebung im Cyberspace und die Sicherung elektronischer Beweise stehen dabei vor rechtlichen und tatsächlichen Herausforderungen, z.B. durch die Gefahr der Manipulation, Vernichtung oder Beseitigung von Beweismitteln.[81] Bei grenzüberschreitend agierenden Tätern kann die Verwertung von Beweismitteln, die in anderen Ländern erhoben wurden, umstritten sein, wenn in dem beweiserhebenden Land andere strafprozessuale Vorschriften bei der Beweiserhebung und -verwertung gelten als in dem Land, in dem der Strafprozess durchgeführt wird. Auch stellen Schwierigkeiten beim Zugriff auf Beweismittel bei Anbietern von Online-Diensten (z.B. von sozialen Netzwerken), die aufgrund unterschiedlicher strafrechtlicher und strafprozessualer Regelungen in den EU-Mitgliedsstaaten uneinheitlich geregelt sind, ein grundsätzliches Problem dar.

Im April 2018 schlug die Europäische Kommission dem Europäischen Parlament und Rat daher die – in der rechtswissenschaftlichen Literatur umstrittene – „Verordnung über eine europäische Herausgabeanordnung und Sicherungsanordnung für elektronische Beweismittel in Strafsachen“[82] sowie flankierend die (ebenfalls umstrittene) „Richtlinie zur Festlegung einheitlicher Regeln zum Zwecke der Beweiserhebung in Strafverfahren“[83] vor. Beide zielen vor allem darauf ab, dass der

---

80 Vgl. *Fall 32* Deutschland.

81 Vgl. *Momsen & Hercher* 2013, S. 178 ff.

82 Europäische Kommission COM/2018/225 final – 2018/0108 (COD): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen.

83 Europäische Kommission: Vorschlag für eine Richtlinie des Europäischen Rates und des Europäischen Parlaments zur Festlegung einheitlicher Regeln für die Bestellung von

grenzüberschreitende Zugang zu elektronischen Beweismitteln beschleunigt wird und Ermittlungsbehörden Zugang zu Beweismitteln, die Diensteanbieter mit Sitz innerhalb oder außerhalb der EU gespeichert haben, erhalten. Kritik erfahren die Vorschläge besonders im Hinblick auf Defizite im Grundrechtsschutz, den gerichtlichen Rechtsschutz der von der Datenübermittlung betroffenen Person im Vollstreckungsstaat sowie den gerichtlichen Rechtsschutz des Service-Providers im Ausstellungsstaat der Herausgabeanordnung.[84]

6. Resümee und Ausblick

Die ausgewählten phänomenologischen Ergebnisse sollen als Grundlage für die Entwicklung evidenzbasierter Maßnahmen dienen, vor allem mit dem Ziel der Prävention gegen den unerlaubten Abfluss von Geschäftsgeheimnissen. Ein weiteres Ziel ist die Einrichtung von Mechanismen, die eine frühzeitige Entdeckung erfolgreicher (Cyber-)Angriffe auf ein Unternehmen ermöglichen. Dabei waren der Zugang der Täter zu geschützten Geschäftsgeheimnissen sowie der Abfluss von Know-how ebenso vielfältig wie die Aufdeckungsmethoden, ohne dass sich in einem der untersuchten Länder eine besonders vielversprechende Methode identifizieren ließ. Konzepte zur Tataufdeckung sollten unter Berücksichtigung der Ergebnisse Maßnahmen enthalten, die sowohl personelle als auch technische Ebenen einbeziehen. Auf personeller Ebene ist besonders die Gefahr potenzieller Innentäter zu bedenken sowie der Umstand, dass im deutschen Sample knapp 27 % der Taten, bei denen das Ermittlungsverfahren mit einer Einstellung gem. § 153a StPO, einem Antrag auf Erlass eines Strafbefehls oder einer Anklage endete, auf Hinweise von aufmerksamen Mitarbeitern oder Dritten mit Kontakt zu dem geschädigten Unternehmen zurückzuführen sind. Eine Sensibilisierung der eigenen Angestellten für etwaige Möglichkeiten des Zugriffs auf Geschäftsgeheimnisse und potenzielle Fallkonstellationen des unerlaubten Know-how-Abflusses kann nicht nur bei der Entdeckung, sondern auch bei der Verhinderung erfolgreicher Angriffe zweckmäßig sein. Auf technischer Ebene sollten sich Präventionsmaßnahmen, unter Berücksichtigung der Ergebnisse bezüglich des Zugangs zu und Abflusses von Geschäftsgeheimnissen, vor allem auf den Schutz vor einem Zugang zu (elektronisch gespeicherten) Geschäftsgeheimnissen beziehen. Neben einem umfassenden IT-Schutzkonzept, dem routinemäßigen Sperren von Rechnern und Wegschließen von Aktenordnern bietet es sich im Hinblick auf potenzielle Innentäter an, Zugangsberechtigungen zu Daten (elektronisch oder in Akten gespeichert) auf diejenigen zu beschränken, die mit den Geschäftsgeheimnissen arbeiten müssen.

Vertretern zu Zwecken der Beweiserhebung in Strafverfahren COM/2018/226 final – 2018/0107 (COD).

84 Vgl. dazu *Böse* 2019, S. 144, 146.

Die rechtliche Reaktion auf den unerlaubten Know-how-Abfluss umfasst neben zivil- und arbeitsrechtlichen Konsequenzen auch die strafrechtliche Verfolgung. Dabei sind die Ergebnisse von Ermittlungsverfahren, wie in *Abschnitt 5.4,* sowie Rechtsfolgen des Strafverfahrens, wie in *Abschnitt 5.5* beschrieben, für die betroffenen Unternehmen wenig zufriedenstellend. Während einem Unternehmen bei einem erfolgreichen Angriff starke Einschränkungen und finanziellen Schäden drohen, riskieren die Täter, sofern ihr Angriff überhaupt entdeckt wird und sie ermittelt werden, selten strafrechtliche Konsequenzen. Zum einen wird nur ein Bruchteil der Delikte angezeigt und der strafrechtlichen Verfolgung unterworfen, zum anderen werden Strafverfahren aus den aufgeführten unterschiedlichen Gründen regelmäßig eingestellt oder sie enden teilweise nach einer prozessualen Absprache lediglich mit der Verurteilung zu einer Geldstrafe. Die geringe Wahrscheinlichkeit einer Verurteilung der Täter kann wiederum ein Grund für eine geringe Anzeigebereitschaft der Unternehmen sein.

Auch für die Strafverfolgungsbehörden, die teilweise umfangreiche personelle und damit auch finanzielle Ressourcen in Ermittlungsverfahren investieren, kann gegebenenfalls ein hoher Aufwand einem geringen „Ertrag“ gegenüberstehen. Das Ermittlungsverfahren dient dem Zweck, das Vorliegen einer Straftat zu überprüfen, aber gerade bei Cyberangriffen kann die Beweisführung, sei es technisch oder rechtlich, schwierig sein. Rechtliche Schwierigkeiten betreffen vor allem den Zugang zu möglichen Beweismitteln im Ausland, z.B. zu Daten, die auf den Servern ausländischer Provider gespeichert sind. Soweit es bilaterale Abkommen mit dem entsprechenden Land gibt, können Rechtshilfeverfahren viel Zeit in Anspruch nehmen, sodass vor Abschluss der Ermittlungen Fristen für die Speicherung der gewünschten Daten ablaufen können. Weitere Schwierigkeiten betreffen die Sicherung und Herausgabe elektronischer Beweismittel. Die Europäische Kommission hat für beide Problemfelder eine Richtlinie bzw. Verordnung vorgeschlagen, die zurzeit kontrovers diskutiert werden. Fehlende Rechtshilfeabkommen können dazu führen, dass Straftäter nicht ausgeliefert oder Beweismittel nicht zugänglich gemacht werden.

Eine Schwierigkeit bei der strafrechtlichen Verfolgung von Wirtschaftsspionage stellt der Nachweis der Tätigkeit für einen fremden Nachrichtendienst dar. Dieses Tatbestandsmerkmal begründet im deutschen Recht eine Strafbarkeit wegen geheimdienstlicher Agententätigkeit gem. § 99 StGB (Wirtschaftsspionage) mit der sachlichen Zuständigkeit des Generalbundesanwaltes gem. § 142a GVG. Kann nicht bewiesen werden, dass der Täter für einen ausländischen Geheimdienst tätig war, entfällt eine Strafbarkeit als Wirtschaftsspionage, die als Offizialdelikt verfolgt wird und für die ein höherer Strafrahmen vorgesehen ist. Die Möglichkeit, das Delikt durch die Landesstaatsanwaltschaft wegen eines Verstoßes gegen § 23 GeschGehG[85] (Konkurrenzausspähung) zu verfolgen, bleibt jedoch bestehen. Vor

---

[85] Bis April 2019: §§ 17–19 UWG.

denselben Schwierigkeiten stehen die Strafverfolgungsbehörden auch in Bulgarien, Dänemark, Österreich und dem Vereinigten Königreich, wo Straftaten, bei denen ein fremder Nachrichtendienst aktiv oder ein Staatsgeheimnis betroffen war, mit einer höheren Strafe bedroht sind.

Die Konkurrenzausspähung ist in Deutschland, Österreich und der Schweiz als Antragsdelikt ausgestaltet. Das geschädigte Unternehmen kann somit in Deutschland und der Schweiz auf den Privatklageweg verwiesen werden, in Österreich obliegt gem. § 71 StPO (Österreich) im Privatanklageverfahren dem Geschädigten die Durchführung des Verfahrens, ohne dass die Staatsanwaltschaft tätig wird. Aufgrund der möglichen hohen Schäden, die der unerlaubte Zugriff auf geschützte Geschäftsgeheimnisse für Unternehmen und damit den gesamten Wirtschaftsstandort verursachen kann, erscheint es zielführend, die Konkurrenzausspähung ebenfalls als Offizialdelikt auszugestalten. Die dadurch entfallende Möglichkeit des Verweises auf den Privatklageweg könnte dazu führen, dass es in mehr Verfahren zu einer strafrechtlichen Verfolgung kommt. Dies könnte möglicherweise wiederum die Anzeigebereitschaft betroffener Unternehmen steigern. Mit der Ausgestaltung der Konkurrenzausspähung als Offizialdelikt entfiele zudem die Möglichkeit der Rücknahme eines Strafantrags, wodurch gegebenenfalls die Anzahl der Verfahren, die ohne einen ersichtlichen strafrechtlichen Vorwurf lediglich zur Unterstützung eines zivil- oder arbeitsgerichtlichen Verfahrens eingeleitet wurden, reduziert werden könnte. Bei dem im April 2019 in Deutschland in Kraft getretenen Gesetz zum Schutz von Geschäftsgeheimnissen hat der Gesetzgeber an der Einordnung der Konkurrenzausspähung als Antragsdelikt und der Möglichkeit des Verweises auf den Privatklageweg (zunächst) jedoch nichts geändert. In seiner jetzigen Form und im Hinblick auf den Ausgang der Strafverfahren scheint die generalpräventive Wirkung der Vorschriften zum Schutz von Geschäftsgeheimnissen daher eher gering.

Zusammenfassend lässt sich festhalten, dass sich die phänomenologischen Ergebnisse in den untersuchten Ländern kaum voneinander unterscheiden. Ebenso steht jedes der Länder vor rechtlichen und tatsächlichen Herausforderungen bei der Strafverfolgung, vor allem bei der Ermittlung und Beweisführung in Fällen von (grenzüberschreitender) Cyberkriminalität, ohne dass sich in einem Land eine besonders vielversprechende rechtliche Lösung abgezeichnet hat. Grundsätzlich zu überdenken ist die diskutierte Einordnung von Delikten der Konkurrenzausspähung als Antragsdelikt.

Literatur

Afsah, E. (2018): Country Report: Denmark, in: S. Carl & M. Kilchling (Hrsg.), Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin, S. 141–164.

Becker, G.S. (1968): Crime and punishment: an economic approach. Journal of Political Economy vol. 78, S. 169–217.

Bertel, C., Schwaighöfer, K. & Venier, A. (2018): Österreichisches Strafrecht Besonderer Teil I (§§ 75 bis 168b StGB). 14. Aufl. Wien.

Bollhöfer, E. & Jäger A. (2018): Wirtschaftsspionage und Konkurrenzausspähung – Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Freiburg i.Br.

Böse, M. (2019): Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe? Kriminalpolitische Zeitschrift 03/2019, S. 140–147.

Budras, C. (2014): Der Feind sitzt im Büro nebenan. Frankfurter Allgemeine Zeitung, 23.05.2014; www.faz.net/aktuell/wirtschaft/wirtschaftsspionage-frustrierte-mitarbeiter-sind-ein-risiko-12944343.html [12.07.2019].

Button, M., Wakefield, A. & Larkins, K. (2018): Country Report: United Kingdom, in: S. Carl & M. Kilchling (Hrsg.), Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin, S. 597–612.

Carl, S. & Kilchling, M. (Hrsg.) (2018): Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin.

Centre for Cyber Security (2017): The cyber threat against the maritime sector; https://fe-ddis.dk/cfcs/CFCSDocuments/The_Cyber_Threat_to_the_Maritime_Sector_march.pdf [24.07.2019].

Feuerbach, P.J.A. von (1801): Lehrbuch des gemeinen in Deutschland geltenden Peinlichen Rechts; www.deutschestextarchiv.de/feuerbach_recht_1801 [24.07.2019].

FH Campus Wien, Fachbereich Risiko- und Sicherheitsmanagement (2011): Wirtschafts- und Industriespionage. Handbuch Know-How-Schutz für die österreichische Wirtschaft; www.bvt.gv.at/401/files/Handbuch_WIS.pdf; zit.: FH Campus Wien 2011.

FiA (Fédération Internationale de l´Automobile) (2007): World Motor Sport Council Decision. Re: Article 151(c) International Sporting Code – Vodafone McLaren Mercedes, 13.09.2007; https://web.archive.org/web/20071022060508/http://www.fia.com/resources/documents/17844641__WMSC_Decision_130907.pdf [12.07.2019].

Goren; B. & Noble, J. (2007): Spy case court hearing adjourned. autosport 10.07.2007; www.autosport.com/f1/news/60690/spy-case-court-hearing-adjourned [12.07.2019].

Häder, M. (2015): Empirische Sozialforschung – eine Einführung. 3. Aufl. Wiesbaden.

Hellmann, U. (2018): Wirtschaftsstrafrecht. 5. Aufl. Stuttgart.

Kersting, S. & Erdmann, J. (2015): Analyse von Hellfelddaten – Darstellung von Problemen, Besonderheiten und Fallstricken anhand ausgewählter Praxisbeispiele, in: S. Eifler & D. Pollich (Hrsg.), Empirische Forschung über Kriminalität. Wiesbaden, S. 9–29.

Kilchling, M. & Carl, S. (2016): Wirtschaftsspionage im globalen Markt: Sind die Ermittlungsstrukturen in Deutschland noch zeitgemäß? In: P. Zoche, S. Kaufmann & H. Arnold (Hrsg.), Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung. Berlin, S. 183–196.

Konopatsch, C., Rentsch, M., Stocker, P. & Lehmkuhl, M. (2018): Country Report: Switzerland, in: S. Carl & M. Kilchling (Hrsg.), Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin, S. 577–596.

Konopatsch, C. & Lehmkuhl, M. (2018): Country Report: Austria, in: S. Carl & M. Kilchling (Hrsg.), Economic and Industrial Espionage in Germany and Europe: History, De-

velopments and Present Legislative Frameworks in a Comparative Perspective. Berlin, S. 17–36.

Körmer, C., Langer, M. (FH Campus Wien) (Dezember 2015): Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015; www.bvt.gv.at/401/files/StudieWirtschafts-undIndustriespionageinoesterreichischenUnternehmen2015.pdf; zit.: Körmer & Langer 2015.

Momsen, C. & Hercher, N. (2013): Digitale Beweismittel im Strafprozess – Eignung, Gewinnung, Verwertung, Revisibilität; www.strafverteidigervereinigungen.org/Material/Themen/Technik%20&%20Ueberwachung/37_momsen.pdf [12.07.2019].

Omlin, E. (2010): Art. 310 StPO, in: M. A. Niggli, M. Heer & H. Wiprächtiger (Hrsg.), Basler Kommentar zur Schweizerischen Strafprozessordnung, Jugendstrafprozessordnung. Basel.

Petrova, T., Yordanova, D., Petrov, S. & Boyadjiyski, P. (2018): Country Report: Bulgaria, in: S. Carl & M. Kilchling (Hrsg.), Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin, S. 61–90.

Roxin, C. (1997): Strafrecht Allgemeiner Teil - Grundlagen. Der Aufbau der Verbrechenslehre. 3. Aufl. München.

Spirgath, T. (2013): Zur Abschreckungswirkung des Strafrechts – eine Metaanalyse kriminalstatistischer Untersuchungen. Berlin.

Statistisches Bundesamt (2018): Rechtspflege – Staatsanwaltschaften 2017, Fachserie 10, Reihe 2.6. Wiesbaden.

Tsolkas, A. & Wimmer, F. (2013): Wirtschaftsspionage und Intelligence Gathering. Wiesbaden.

US Department of Justice (2018a): Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets, Pressemitteilung, 24.01.2018; www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets [12.07.2019].

US Department of Justice (2018b): Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets, Pressemitteilung, 06.07.2018; www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets [12.07.2019].

Verfassungsschutzbehörden des Bundes und der Länder (2014): Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung; www.verfassungsschutz.de/embed/broschuere-2014-07-wirtschaftsspionage.pdf [12.07.2019].

World Trade Organisation (2017): World Trade Statistical Review 2017; www.wto.org/english/res_e/statis_e/wts2017_e/wts2017_e.pdf [12.07.2019].

Zirm, J. (2013): Spionage: „Das war versuchter Firmenmord". Die Presse, 22.08.2013; https://diepresse.com/home/wirtschaft/international/1444292/Spionage_Das-war-versuchter-Firmenmord [12.07.2019].

Zwickl, J. (2015): Industriespionage im deutschen Mittelstand. Wie schützt man Know-how wirkungsvoll? Norderstedt.

Der nächste Angriff kommt bestimmt

Verbreitung von Maßnahmen zur Prävention gegen ungewollten Wissensabfluss bei kleinen und mittleren Unternehmen (KMU)

Esther Bollhöfer

1. Situation der KMU

Eine der zentralen Fragen im Kontext von Wirtschaftsspionage und Konkurrenzausspähung ist die nach dem Schutz der Informationen. Diese Aufgabe ist für ein Unternehmen nicht neu, jedoch ist mit der Digitalisierung die Menge an digital erfassten und verfügbaren Informationen gestiegen, bei einer gleichzeitigen Vervielfachung der Kommunikationsprozesse. Zugleich entstehen neue Potenziale für Wirtschaftsspionage und Konkurrenzausspähung: Ein Beispiel ist das *condition monitoring*, die Grundlage für die zustandsbasierte Wartung von Maschinen und Anlagen. Dabei werden Betriebsdaten wie Temperatur, Lasten und Systemzustände protokolliert und kontinuierlich an den Hersteller bzw. einen externen Dienstleister zur Auswertung übermittelt. Im Gegenzug erhält das Unternehmen die Informationen, wann welche Bauteile idealerweise zu ersetzen sind, damit es nicht zu einem Ausfall oder Produktionsstillstand kommt. Diese aggregierten Daten erlauben in der Hand von unberechtigten Dritten zum Beispiel Rückschlüsse auf die Auslastung der Produktionslinie und damit auf die Auftragslage des Unternehmens[1] – und können damit für einen Kunden in Vertragsverhandlungen von enormer Bedeutung sein. Dabei ist das Ende der Digitalisierung noch nicht erreicht: Wie der Innovationsindikator 2017 zeigt, liegt Deutschland im Digitalisierungsbereich abgeschlagen auf Platz 17[2] und hat hier großen Nachholbedarf. Im Bereich der Spionage zieht die Digitalisierung eine Änderung der Modi Operandi nach sich: Waren in der Vergangenheit noch aufwendige Vorbereitungen nötig, um zum Beispiel eine Person im Zielunternehmen zu positionieren, hat sich das Tatvorgehen zum Vorteil der Spione vereinfacht. Da nur noch in wenigen Fällen personeller Einsatz vor Ort nötig ist, reduziert sich das finanzielle Engagement bei einer gleichzeitigen Minimierung des Risikos. Der

---

1 Vgl. *Hofmann* 2013, S. 210.

2 Vgl. acatech & BDI 2017, S. 7.

neue virtuelle Weg ist über Landesgrenzen hinweg möglich und sehr risikoarm: Informationen werden „still“ mitgelesen, abgefangen und/oder verändert – weitgehend unerkannt auf dem Weg zwischen Sender und Empfänger, wobei sowohl automatisch als auch manuell initiierte Informationsflüsse betroffen sein können.

Nicht nur global agierende Konzerne, sondern vor allem kleine und mittlere Unternehmen (KMU) sind betroffen und leiden unter den Folgen von illegalem Wissensabfluss. Laut einer Bitkom-Studie aus dem Jahr 2015 gehören IT-Angriffe schon „zum Alltag vieler Unternehmen“.[3] Danach werden nahezu die Hälfte aller befragten Unternehmen mindestens einmal pro Monat angegriffen, fast jedes zehnte (9 %) sogar täglich.[4] Eine weitere Studie bestätigt, dass bereits zwei Drittel der deutschen Unternehmen Firmengeheimnisse durch Cyberspionage verloren haben, 15 Prozent der Unternehmen waren sogar schon häufiger betroffen.[5] Gerade dem Mittelstand entstehen durch Spionageangriffe die größten Schäden, allen voran dem Maschinenbau.[6] Als stärkste Bedrohung durch Spionage wird mit 68 Prozent die Verletzung von Geschäfts- und Betriebsgeheimnissen bewertet, gefolgt von der Verletzung von Urheber- und sonstigen Schutzrechten.[7]

Obwohl sich die meisten Unternehmen dieser Gefahren bewusst sind,[8] werden trotzdem E-Mails unverschlüsselt verschickt, USB-Sticks ungeprüft in den Laptop gesteckt und unsichere Apps auf Geschäftsgeräten installiert. Hier muss hinterfragt werden, wie dieses Verhalten zu erklären ist. Durch die rasante Entwicklung der Informations- und Kommunikationstechnologie (IKT) ist ein schneller Transfer auch sehr komplexer, technologischer Informationen möglich, der die traditionellen Know-how-Vorsprünge von KMU rascher schwinden lässt als bisher und so zu einem wachsenden Innovations- und Technologiedruck führt.[9] Ein Datenleck kann das ganze Unternehmen ruinieren, ebenso ein Wettbewerber, der das gleiche Produkt oder die gleiche Leistung schneller und günstiger auf den Markt bringt.

2. Was wird angegriffen?

Zunächst ist zu klären, was das vorrangige Ziel eines Angriffs ist. Im Volksmund ist es die Information, die an sich nicht gegenständlich ist und auch keinen eindeutigen

---

3 Bitkom 2015, S. 12.

4 Vgl. Bitkom 2015, S. 12.

5 Vgl. IfD Allensbach 2011, S. 2.

6 Vgl. Corporate Trust 2015, S. 14, 16.

7 Vgl. DIN 2013, S. 48.

8 Vgl. *Roßnagel* 2007, S. 98–99; Agentur Karg und Petersen 2010, S. 5.

9 Vgl. *Pleitner* 1998, S. 66–69; *Koller, Raithel & Wagner* 1998, S. 175–203.

Wert hat. Weder positive Abgrenzungsversuche in einzelnen Fachdisziplinen wie den Wirtschaftswissenschaften, den Sozialwissenschaften und der Informatik als „dritte universelle Grundgröße“ noch Abgrenzungen im negativen Sinne als „nicht greifbar, nicht zeitlich beschränkt“, vermögen den Begriff der „Information“ umfassend zu definieren. Unumstritten ist jedoch, dass Information einen ökonomischen Wert haben kann, den es zu nutzen und zu schützen gilt.[10] Informationen und deren Verwertung in Form von Wissen sind heute der bedeutendste Erfolgsfaktor von nationalen Ökonomien und Unternehmen.[11] Der Wert der Information ist entsprechend der Qualität und der strategischen Bedeutung für das innehabende Unternehmen anzusetzen.[12] Informationen – und mit deren Hilfe spezifisches Wissen – zu erlangen, ist das Ziel der Konkurrenzausspähung und Wirtschaftsspionage.

Zu unterscheiden ist weiterhin zwischen Daten im informationstechnischen Sinn einerseits, beispielsweise aus einer Produktionsanlage, und Informationen und Wissen/Know-how andererseits. Einem Angreifer ist mit Daten im informationstechnischen Sinn nicht gedient – z.B. 1,2; 2,9; 0,1; 0,1; 1,4; t; ... – es bedarf einer weiteren verknüpfenden Information (wie z. B. der Zuordnung zu einer Variablenliste oder zumindest zu einem Anlagentyp), um die Daten nutzen zu können und Wissen zu generieren. Im Kontext von industriellen Wertschöpfungsprozessen wird analog zu Wissen auch der Begriff Know-how verwendet.[13] Betrachtet man Wissen als eine Ressource des Unternehmens, so ergibt sich der besondere Schutzbedarf daraus, dass Wissen beliebig teilbar ist und auch bei Weitergabe/Teilung nicht an Qualität und Wert verliert. Dies unterscheidet es von allen anderen materiellen Ressourcen, die dem Konkurrenzprinzip der Nutzung unterliegen.[14] Damit umfasst Wissen alle betrieblichen Informationen, die sowohl technischer als auch kaufmännischer Natur sein können[15] wie z.B. Konstruktionszeichnungen, Kundenlisten, Bezugsquellen und Herstellungsverfahren.[16] Mit ihnen kann der Nutzer ein technisches oder wirtschaftliches Ergebnis (bzw. eine Lösung) erzielen, welches ihm ohne diese Kenntnisse nicht oder nur schwer möglich gewesen wäre.[17]

---

10 Vgl. *Blum* 2003, S. 64, 66; *Wodtke & Richters* 2004, S. 15; *Röder* 2011, S. 24.

11 Vgl. *Lux & Peske* 2002, S. 14.

12 Vgl. *Hummelt* 1997, S. 6.

13 Vgl. z.B. *Kochmann* 2009, S. 19.

14 Vgl. *Lux & Peske* 2002, S. 1.

15 Eine Beschränkung des Begriffs auf technisches Wissen hat sich im Forschungssprachgebrauch nicht durchgesetzt. Siehe dazu *Kochmann* 2009, S. 24–26 m.w.N.

16 Vgl. *Harte-Bavendamm* 2013, § 17 UWG, Rn. 7; DIN 2013, S. 61.

17 Diese Ausrichtung auf eine Problemlösung fordert auch der BGH in zahlreichen Urteilen: siehe BGHZ 167, 374 (379) = GRUR 2006, 927 (928) – Kunststoffbügel; BGH NStZ 2007, 93 (94); BGH GRUR 2003, 356 (358) – Präzisionsmessgeräte; BGH GRUR 2002, 958 (960) – Technische Lieferbedingungen; BGH GRUR 2002, 91 (92 ff.) – Spritzgießwerkzeuge; BGHZ 107, 117 (122) = GRUR 1009, 221 (222) – Forschungskosten;

3. Risiken für KMU

Vorab lässt sich festhalten: Angriffe auf Informationen können auf unterschiedlichen Wegen erfolgen. Es wird zwischen personengebundenen und technikgebundenen Methoden der Informationsbeschaffung unterschieden.[18] Zu den personengebundenen zählen die Gesprächsabschöpfung, Social Engineering oder die Einschleusung eines Spions. Sie sind besonders gefährlich für ein Unternehmen, da alle Mitarbeiter Ziel eines solchen Angriffs werden können und sich oft nicht bewusst sind, dass sie an illegalem Wissensabfluss beteiligt sind. Auf Wissen, welches nicht auf Papier oder in Systemen gespeichert wurde, sondern quasi in den Mitarbeitern verankert ist, kann auf diese Weise zugegriffen werden.[19] Bei technikgebundenen Methoden wird die Recherche durch elektronische Auswertung betrieben. Dies kann sowohl über frei verfügbare Daten im Internet geschehen als auch über klassische Hackerangriffe oder das Abhören von Telefonaten.[20] Wenn auch medial nicht so präsent wie Social Engineering oder Hackerangriffe, zählen auch der physische Einbruch und der Diebstahl von Informationsträgern zu den Möglichkeiten des illegalen Informationsabflusses. Besonders die Kombination aus unterschiedlichen Angriffsmethoden ist höchst gefährlich für jedwedes Unternehmen.

Um insbesondere die Risiken für und den Umgang mit ihnen bei KMU zu untersuchen, wurde ein mehrstufiges Forschungsdesign gewählt: In einem ersten Schritt konnten die Ergebnisse einer großen, etablierten und repräsentativen Erhebung im Verarbeitenden Gewerbe dazu genutzt werden, die aktuelle Wahrnehmung der Unternehmen von „Spionage" und die Nutzung von Präventionsmaßnahmen zu erfassen. Dabei handelt es sich um regelmäßige Erhebungen zum Thema „Modernisierung der Produktion", die das Fraunhofer-Institut für System- und Innovationsforschung ISI seit 1993 durchführt und durch die alle Branchen des Verarbeitenden Gewerbes abgedeckt werden.[21] Untersuchungsgegenstand sind die Produktionsstrategien, der Einsatz innovativer Organisations- und Technikkonzepte in der Produktion, Fragen des Personaleinsatzes sowie Fragen zur Wahl des Produktionsstandortes. Die vorliegenden Aussagen stützen sich auf Daten der Erhebungsrunde 2015, für die 15.720 Betriebe des Verarbeitenden Gewerbes in Deutschland angeschrieben wurden. Bis August 2015 schickten 1.282 Firmen einen verwertbar ausgefüllten Fragebogen zurück (Rücklaufquote 8 %). Betriebe mit weniger als 100 Beschäftigten stellten 66 Prozent, mittelgroße Betriebe 31 Prozent und große Betriebe (mit mehr als 1.000 Beschäftigten) 3 Prozent der antwortenden Firmen.

BGH GRUR 1985, 129 (130) – Elektrodenfabrik; BGH GRUR 1984, 753 – Heizkessel-Nachbau.

18 Vgl. *Warnecke* 2010, S. 259 f.

19 Vgl. *Warnecke* 2010, S. 267 f.

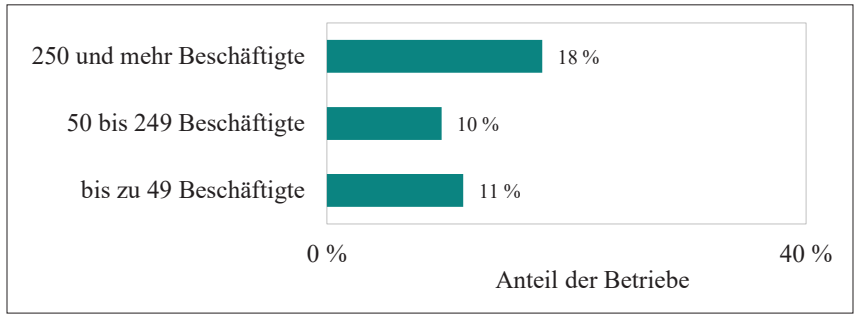
20 Vgl. *Warnecke* 2010, S. 259 f.

21 Fraunhofer, Erhebung „Modernisierung der Produktion 2015".

In einem zweiten Schritt wurden Experten aus der Industrie, von industrienahen Dienstleistern und Verbänden sowie von Strafverfolgungsbehörden mithilfe teilstandardisierter Interviews befragt, um die Beweggründe für und gegen Präventionsmaßnahmen und deren Ausgestaltung zu erfahren und die Gefahreneinschätzung zu eruieren. Dieser qualitative Ansatz sollte es ermöglichen, die untersuchten Gegebenheiten „von innen heraus" zu verstehen und nicht nur anhand von Zahlen zu analysieren.

Die Frage nach konkreten Spionagefällen bzw. Verdachtsfällen im Unternehmen in den letzten fünf Jahren wurde von 11,5 Prozent der Unternehmen im Verarbeitenden Gewerbe bejaht (vgl. *Abbildung 1*). Besonders betroffen scheinen zunächst die größeren Unternehmen mit mehr als 250 Beschäftigten zu sein. Zu beachten ist, dass sich die Angaben auf bekannte Vorfälle und Verdachtsfälle beziehen. Aus der Befragung ergab sich, dass in kleineren Betrieben Frühwarnsysteme zur Identifikation von ungewolltem Informationsabfluss selten eingesetzt werden, somit Vorfälle und Verdachtsfälle oftmals unbemerkt bleiben und Auffälligkeiten aufgrund fehlender Weiterverfolgung(smöglichkeiten) nicht als Verdachtsfälle eingestuft werden. Weiterhin führt der Sprachgebrauch von Spionage bzw. Ausspähung bei vielen KMU zur spontanen Verneinung. Befragt nach einem ungewollten Informationsabfluss an Dritte, wird die Frage durch einige Unternehmen jedoch plötzlich bejaht. Vor dem Hintergrund des Wordings bzw. der unterschiedlichen Assoziationen sind auch die stark schwankenden Zahlen zur Betroffenheit der deutschen Wirtschaft durch Wirtschaftsspionage und Konkurrenzausspähung in diversen Studien der letzten Jahre zu erklären, bei denen die Zahl der ausspionierten Unternehmen zwischen acht und über fünfzig Prozent schwankt.

Abbildung 1 Vorfälle und Verdachtsfälle bei Unternehmen



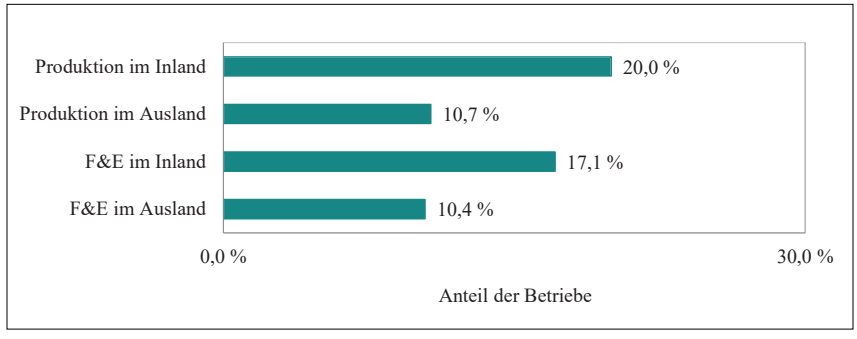
Quelle: Fraunhofer ISI, Erhebung „Modernisierung der Produktion 2015".

Erwartungsgemäß sind Unternehmen mit mittlerer (2,5–7 % F&E-Aufwendungen) und hoher Forschungs- und Entwicklungs- (F&E) Intensität (> 7 % F&E-Aufwendungen) mit 18,1 Prozent bzw. 19,4 Prozent der Unternehmen stärker betroffen. Das lässt sich vor allem dadurch begründen, dass diese Unternehmen durch ihre

Forschungsaktivitäten ins Visier von Wirtschaftsspionen gelangen und zudem für Wettbewerber interessant sind.

Ein weiterer Sachverhalt, der die Unternehmen ins Ziel der Angreifer rückt, ist der Auslandsbezug: Unternehmen mit einer Produktionsstätte im Ausland sind mit 17,1 Prozent deutlich stärker betroffen, als solche ohne (10,4 %). Ebenso meldet jedes fünfte Unternehmen, das eine Forschungs- und Entwicklungsabteilung im Ausland unterhält, bereits mindestens einen Vorfall oder Verdachtsfall. Bei den Unternehmen mit einer F&E-Abteilung im Inland sind es nur 10,7 Prozent (vgl. *Abbildung 2).*

Abbildung 2 Vorfälle und Verdachtsfälle bei Unternehmen mit Auslandsbezug

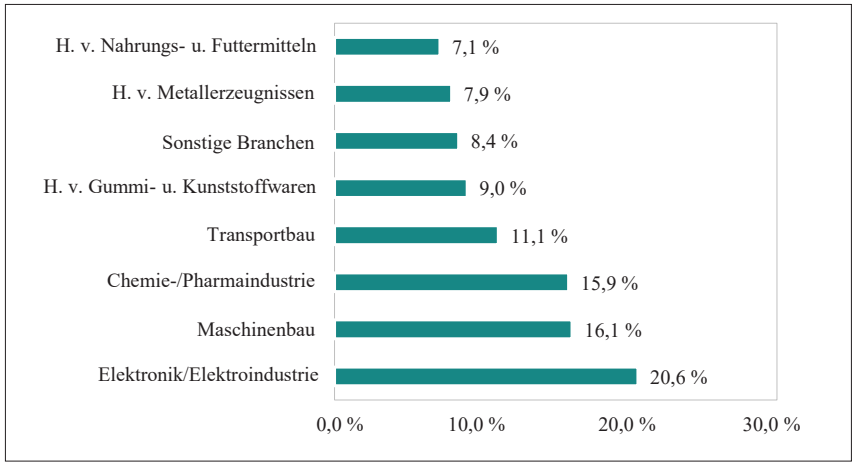


Quelle: Fraunhofer ISI, Erhebung „Modernisierung der Produktion 2015".

Erwartungsgemäß ist die heterogene Verteilung der Vorfälle und Verdachtsfälle über die verschiedenen Branchen (vgl. *Abbildung 3).* Besonders betroffen sind die Elektronik- bzw. Elektroindustrie mit fast 21 Prozent, gefolgt vom Maschinenbau (16 %) und der Chemie-/Pharmaindustrie (ebenfalls 16 %). Begründen lässt sich diese Verteilung durch die langen Forschungs- bzw. Vorlaufzeiten bis zur Produktreife sowie die große Bedeutung von Produkt- und Prozessinnovationen in den betroffenen Branchen.

Generell lässt sich sagen, dass ein Unternehmen nicht allein aufgrund seiner vermeintlich unbedeutenden Größe bereits geschützt ist. Innerhalb der KMU sind weitere Gruppen identifizierbar, die aus verschiedenen Gründen eines besonderen Schutzes bedürfen. Start-Ups sind durch ihre offene Kommunikation auch vertraulicher Inhalte besonders gefährdet. Oft stammen die Mitarbeiter aus dem universitären Umfeld und sind offene Kommunikationsprozesse zum Informationsaustausch gewohnt. In der freien Wirtschaft herrschen jedoch strengere Anforderungen an Geheimhaltung und Vertraulichkeit, die oft unterschätzt werden. Daneben verkennen auch Familienunternehmen oft die eigene Anfälligkeit für Spionageangriffe. Da hier Vertrauen sehr groß geschrieben wird, kommt es vor, dass bei jahrelanger guter Zusammenarbeit mit Lieferanten und anderen Parteien, Sicherheitsauflagen gelockert

Abbildung 3 Verteilung der Vorfälle und Verdachtsfälle nach Branchen



Quelle: Fraunhofer ISI, Erhebung „Modernisierung der Produktion 2015".

werden (wie z.B. das Versenden von Zeichnungen „auf Zuruf" per unverschlüsselter E-Mail) und das Unternehmen dadurch angreifbarer wird.

Neben anonymen Tätern kommen auch „gute Bekannte" oder eigene Mitarbeiter (Innentäter) in Betracht. Nicht bei allen Befragten und nicht in jeder Branche sind Unternehmen durch alle drei Gruppen von Tätern bedroht. Die bewusste oder zufällige Mittäterschaft eigener Mitarbeiter wird von den befragten Unternehmen immer wieder als in der Praxis vernachlässigt, aber enorm gefährlich herausgestellt. Gerade bei frustrierten oder verärgerten Angestellten ist es möglich, dass sie bewusst Manipulationen zulassen und wissentlich zu Komplizen werden. Der Schaden, den die Mitwirkung eines Mitarbeiters verursacht, ist somit als besonders hoch einzuschätzen. Haben innerhalb des Unternehmens alle Mitarbeiter uneingeschränkten Zugriff auf Informationen und Daten, können Betriebsgeheimnisse auch durch Praktikanten und neue Mitarbeiter leicht ausgespäht werden.[22]

3.1 Schwachstelle IT-Sicherheit

Der folgende Abschnitt soll dazu dienen, eine Übersicht über mögliche Angriffsmechanismen auf die Kommunikationswege bzw. auf die IT-Infrastruktur zu geben. Dazu werden Schwachstellen des Systems, d.h. „die verwundbaren Stellen eines Systems, über welche die Sicherheitsmaßnahmen des Systems umgangen bzw. überlistet werden können" gezielt ausgenutzt.[23]

---

22 Vgl. *Sonnen* 2016, S. 63.

23 BSI 2003, S. 56.

IT-Sicherheit ist als Rechtsbegriff legaldefiniert im Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik in § 2 Abs. 2:

> Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
>
> 1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
> 2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

Daraus ergeben sich die drei wesentlichen Schutzrichtungen der Verfügbarkeit, der Unversehrtheit und der Vertraulichkeit von Informationen. Die Schutzrichtung Verfügbarkeit beschreibt den Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung.[24] Daneben tritt die zweite Schutzrichtung des Begriffes, die Unversehrtheit von Informationen. Diese beschreibt den Schutz vor jeglicher Form der ungewollten Informationsveränderung. Die Vertraulichkeit der Informationen beschreibt schließlich den auch strafrechtlich relevanten Teil der Schutzrichtung, nämlich die Wahrnehmung von Informationen durch Unbefugte.[25]

Die meisten Unternehmen verfügen heute über einen Internetzugang und damit eine Anbindung an offene Umgebungen. Spätestens in dem Moment, in dem sie auch Daten über offene Netze kommunizieren wollen, müssen sie sich auch mit den Risiken für die technische Sicherheit beschäftigen. Grob lassen sich die Angriffsarten nach dem Schadensbild in 3 Kategorien unterteilen, wie in *Abbildung 4* dargestellt.

Bei den Angriffen der *Kategorie A* ist es Ziel des Angreifers, das gegnerische Kommunikationssystem zum Erliegen zu bringen. Ist ein produzierendes Unternehmen betroffen, wirkt sich der Angriff nicht auf den Produktionsbetrieb aus, lediglich online eingebundene Lieferanten und Dienstleister können temporär ihre Leistungen nicht erbringen. In diese Kategorie fallen z.B. *Denial-of-Service-Angriffe* (DoS), bei denen der Angreifer so viele offene Verbindungen erzeugt, bis der Server lahmgelegt wird und damit seinen Service auch für alle anderen Benutzer beendet.[26] Derartige Angriffe erfreuten sich zeitweise großer Beliebtheit, um Unternehmen zu erpressen, die Online-Services oder gut besuchte Internet-Shops betrieben, da diesen dadurch ein direkter Umsatzausfall und Imageverlust drohte.[27] Da heute die meisten Server mit dieser Art von Angriffen umgehen können, spielen sie nur noch selten eine Rolle.

---

24 Vgl. *Heckmann* 2006, S. 281.

25 Strafrechtlich relevant nach den § 202a StGB und § 17 Abs. 2 UWG.

26 Vgl. BSI 2003, S. 57.

27 Zum Beispiel der Angriff auf Online-Wettbüros während der Fußball Europameisterschaft (siehe *Brauch* 2004).

Abbildung 4 Ziele und Folgen von Angriffen

Kategorie des Angriffs	Ziel des Angriffs	Folgen	Bedeutung für den Produktionsbetrieb
A	▪ Störung des Kommunikationssystems ▪ Erpressen von Handlungen durch Demonstration von Macht ▪ Erzwingen eines Server-Neustarts = Zeitverlust ▪ Verursachen von temporärer Nicht-Erreichbarkeit des Servers/ des Unternehmens	▪ temporäre Nicht-Erreichbarkeit des Servers / des Unternehmens ▪ Verlust von nicht-zustellbaren Datenpaketen ▪ eingebundene Lieferanten und Dienstleister können temporär nicht arbeiten ▪ keine Internet-Kommunikation mit der Außenwelt möglich => Einschränkung der Handlungsfähigkeit des Unternehmens	▪ überschaubar ▪ Schaden entsteht nur sehr kurzfristig ▪ wirksame Präventionsmöglichkeiten vorhanden ▪ hohes Schadenspotenzial lediglich bei Umsätzen über Internet-Shops und großen Stückzahlen
B	▪ Manipulation / Störung der IT-Infrastruktur ▪ Manipulation / Störung des Produktionsbetriebs ▪ Einschleusen von Datenpaketen	▪ Übernahme fehlerhafter/ manipulierter Daten in das System ▪ Fehlsteuerung v. automatisierten Prozessen ▪ u.U. Anlagenstillstände, mech. Schäden u. Ausschussproduktion	▪ mittel bis hoch ▪ nach Umgehen der Sicherheitseinrichtungen bestehen kaum noch Möglichkeiten, die Manipulationen zu bemerken ▪ jedoch keine aktive Weitergabe/ Kommunikation von Informationen nach außen => nur Schädigung, keine Informationsgewinnung
C	▪ Informationsgewinnung durch Übernahme von Kontrolle über Kommunikationsvorgänge ▪ Ausnutzen der erlangten Vertrauensstellung eines Kommunikationspartners ▪ Manipulation / Störung der IT-Infrastruktur ▪ Manipulation / Störung des Produktionsbetriebs	▪ der Angreifer erhält dieselben Privilegien wie der berechtigte Benutzer ▪ Kommunikation wird bewusst umgelenkt => Informationen verlassen unkontrolliert das Unternehmen (Datenverlust) ▪ beide Richtungen der Kommunikation werden fremdgesteuert Fehlsteuerung v. Automatisierten bzw. IT-gestützten Prozessen ▪ u.U. Anlagenstillstände, mech. Schäden u. Ausschussproduktion	▪ sehr hoch ▪ Informationen werden gezielt & unbemerkt abgefragt, manipuliert oder gelöscht ▪ Know-how-Verlust ▪ Gefahr der Fehlsteuerung des Unternehmens ▪ Gefahr der Fehlsteuerung von datengestützten Prozessen, Anlagenstillstand, mech. Anlagenschäden…

Quelle: Bollhöfer 2017, S. 82.

Bei Angriffen der *Kategorie B* schleust der Angreifer einzelne Datenpakete in das Zielsystem ein, in der Hoffnung, dass diese dort wie die echten Pakete weiterbehandelt werden. Die Absicht ist somit eine Manipulation oder Störung der IT-Infrastruktur, ggf. auch bereits eine Manipulation oder Störung des Produktionsbetriebs. Diese Art von Angriff wird auch als *Spoofing*[28] bezeichnet. Spoofing kann in verschiedenen Varianten und Kombinationen eingesetzt werden (IP-Spoofing, DNS-Spoofing, Mail-Spoofing, URL-Spoofing …), ist jedoch als alleinige Maßnahme nicht zur Informationsgewinnung geeignet, da die Antwortpakete des angegriffenen Systems i.d.R. zurück an die vermeintliche Absenderadresse und nicht an den Angreifer gesendet werden.

Der *Kategorie C* zuzuordnende Angriffe haben die Übernahme der Kontrolle über Kommunikationsvorgänge zum Ziel. Der Angreifer dringt so tief in das System des Unternehmens ein, dass er sowohl die eingehende wie auch die ausgehende Kommunikation steuern und manipulieren kann (*Man-in-the-Middle-Angriffe*). Dazu erlangt der Angreifer z.B. die Kontrolle über einen Router des Opfers, sodass die Internetkommunikation beliebig und unerkannt umgelenkt werden kann. Darauf folgend erhält der Angreifer dieselben Privilegien wie der rechtmäßig authentifizierte Benutzer. Diese Art der Angriffe ist damit die gefährlichste Art, um aus automatisiert übertragenen Daten Wissen zu generieren.

Verschärft wird die Problematik durch die Kommunikation über schwach abgesicherte Netze und den Einsatz von mobilen Geräten wie Smartphones oder Tablets auch im Business-to-Business-Bereich. Durch diese Geräte wird zwar ein schnelles Agieren vor Ort ermöglicht, gleichzeitig steigen aber die Anforderungen an die Informationssicherheit.[29] Zusätzlich zu den oben beschriebenen Angriffen sind in den letzten Jahren vermehrt Attacken über Schwachstellen in Webbrowsern[30] bzw. über die Software auf mobilen Endgeräten[31] zu verzeichnen. Nochmals gesteigert werden die Anforderungen an die Informationssicherheit, wenn sich die oben genannten Geräte auch parallel in privater Nutzung befinden.[32] Mobile Geräte zählen zu den technologisch am höchsten entwickelten und verfügen über eine Vielzahl technischer Eigenschaften auf aktuellstem Niveau. Exponenzielle Steigerungen beim Software-Angebot für mobile Geräte (Apps) erfordern jedoch eine ständige Anpassung und Erweiterung der Security-Funktionen und -Maßnahmen.[33] Wenn Experten Unternehmen empfehlen, stündlich Updates der Virenprogramme und System-Updates

---

28 Zu Spoofing-Angriffen siehe auch die ausführliche Darstellung von *Ruetten & Stutzke* 2005.

29 Vgl. *Wiehler* 2004, S. 32, 136; *Eckert* 2003, S. 104.

30 Vgl. *Borges, Schwenk, Stuckenberg & Wegener* 2011, S. 84.

31 Vgl. *Wiehler* 2004, S. 136.

32 Vgl. *Eckert* 2003, S. 106; *Hohensee* 2013, S. 99.

33 Vgl. *Duscha, Klees & Weisser* 2011, S. 66.

vorzunehmen,[34] so betrifft das selbstverständlich alle Geräte, die über offene Netze kommunizieren, somit ebenso mobile Geräte wie auch Maschinen und Anlagen.

An dieser Stelle zeigt sich nun eine bisher wenig diskutierte Problematik: Mobile Endgeräte und Browser-Anwendungen sind die Mittel der Wahl für die fortschreitende Digitalisierung. Sie kommunizieren mit Maschinen und Anlagen, die die oben genannten Sicherheitsanforderungen schlichtweg nicht zeitnah erfüllen können. Das liegt vor allem daran, dass mit einem Software-Update auch oftmals ein Neustart des Systems erforderlich wird und dies bei einer Anlage oder einer ganzen Produktionslinie ein Stoppen der Produktion, d.h. eine ungeplante Stillstandszeit bedeutet, die in modernen Produktionsbetrieben jedoch nicht akzeptabel ist. Somit bleibt einzig die Durchführung der Updates innerhalb geplanter Stillstandszeiten. Diese wiederum hängen von den Wartungsintervallen der Anlagen ab und differieren zwischen wenigen Wochen und mehreren Monaten.[35] Festzustellen bleibt ein großer Bedarf an Lösungen, um die Angriffsfläche in diesem Bereich zu verringern.

3.2 Schwachstelle Organisation

Die besten Lösungsansätze auf technischer Ebene sind wirkungslos, wenn der technische Zugangsschutz auf organisatorischer Ebene umgangen wird. In vielen Unternehmen prägen Sicherheitsmängel im organisatorischen Bereich den Alltag; oftmals werden Sicherheitsaspekte zugunsten einer besseren Handhabbarkeit von Prozessen vernachlässigt.[36] Unternehmen akzeptieren die Gefahren, „solange ihre Verwirklichung in einem wirtschaftlich erträglichen Ausmaß und das Risiko kalkulierbar bleibt".[37] Doch wird auf diese Weise zugelassen, dass Anzahl und Bedeutung der Schäden durch immer ausgereiftere Angriffsstrategien stetig steigen und die damit einhergehende sicherheitsbedingte Zurückhaltung sich als Hemmschwelle für die weitere Digitalisierung erweist.

Die Empfehlung der Experten geht daher dahin, Sicherheit als eine Frage der Organisation ganzheitlich zu betrachten.[38] Zu einem kontinuierlich fortzuschreibenden Datenschutz- und Sicherheitsmanagement gehören neben der Einhaltung der oben genannten Schutzrichtungen der IT-Sicherheit auch die Einhaltung der rechtlichen Erfordernisse des Wirtschaftsverwaltungsrechts, der Datenschutzgesetze und der bilateralen vertraglichen Verpflichtungen. In letzter Konsequenz ist damit jeglicher unternehmerischer Planungs- und Steuerungsprozess betroffen, der eine IT-gestützte Kommunikationsschnittstelle nutzt.

---

34 Vgl. *Schleupner* 2012, S. 15 m.w.N.

35 Vgl. *Schleupner* 2012, S. 15.

36 Vgl. *Duscha, Klees & Weisser* 2011, S. 29.

37 *Knopp, Wilke, Hornung & Laue* 2008, S. 724.

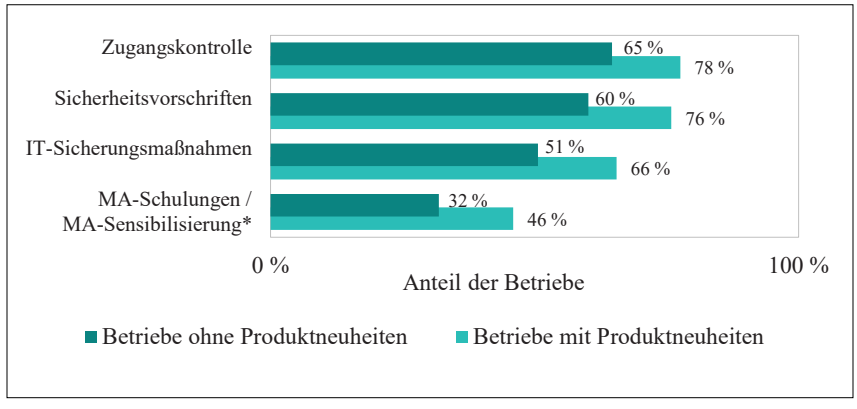
38 Vgl. *Faber* 2009; *Blume* 2009, S. 123; *Heckmann* 2006, S. 282.

4. Schutzmaßnahmen und ihre Verbreitung

Im Folgenden werden vier große Kategorien von Schutzmaßnahmen betrachtet, die Gegenstand der oben genannten repräsentativen Befragung *Modernisierung der Produktion 2015* waren: der Schutz vor physischem Zugang zu Produktionsstätten, die Existenz von Sicherheitsvorschriften zum Schutz gegen den unerlaubten Abfluss von Informationen (z.B. Regelungen zum Umgang mit sensiblen Daten gegenüber Dritten), die Existenz von speziellen IT-Sicherheitsmaßnahmen (wie z.B. Verschlüsselung von Dokumenten, Nutzungsverbot von Cloud-Diensten und von fremden portablen Datenträgern) und die Schulung bzw. Sensibilisierung von Mitarbeitern zu den Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung.

Insgesamt lässt sich ein verstärktes Bewusstsein für die Gefahrenlage und daraus resultierend ein größerer Umfang an realisierten Schutzmaßnahmen bei Unternehmen feststellen, die in den letzten Jahren Produktneuheiten auf den Markt gebracht haben (vgl. *Abbildung 5).*

Abbildung 5 Realisierte Schutzmaßnahmen zur Abwehr von Spionage bzw. Ausspähung



Quelle: Fraunhofer ISI, Erhebung „Modernisierung der Produktion 2015".

* MA: Mitarbeiter.

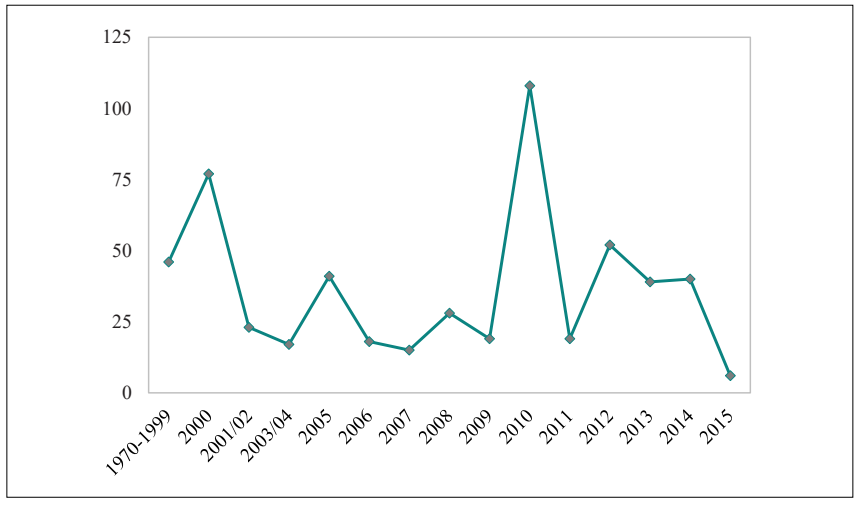
Mit z.T. weit unter 50 Prozent erschreckend niedrig ist der Anteil der KMU, die ihre Mitarbeiter überhaupt für die Gefahren sensibilisieren. Dieser Umstand wurde daher in den zeitlich später erfolgten Experteninterviews mit Unternehmensvertretern thematisiert: Ohne an dieser Stelle die Ergebnisse umfassend darzustellen, kann jedoch festgestellt werden, dass einige Unternehmen die Schulung/Sensibilisierung ihrer Mitarbeiter nicht für nötig erachten, da sie das bei den Mitarbeitern vorhandene Wissen als nicht relevant für Wirtschaftsspionage bzw. Konkurrenzausspähung erachten. Beispielsweise wurde angeführt, dass nur sehr wenige Mitarbeiter

aus dem engsten Führungskreis überhaupt wissen, welche Produkte in Planung sind bzw. über welche technischen Details diese verfügen (sollen). Ein anderes Beispiel ist, dass sich die Kundenkommunikation und die Kundendatenbank ausschließlich auf dem PC der vertrauenswürdigen Assistentin befinde und diese nicht explizit auf die Sensitivität hingewiesen werden müsse. Von Informationsabfluss durch eigene Mitarbeiter betroffene Unternehmen reagieren jedoch nach einem Vorfall sofort und führen Präventionsmaßnahmen ein – die bis zum Zeitpunkt der eigenen Betroffenheit mit den oben genannten Argumenten nicht für nötig gehalten wurden. Dies ist unverständlich, gerade angesichts der Tatsache, dass die Mitarbeiterschulung bzw. -sensibilisierung mit geringem Aufwand und ohne Investitionen angegangen werden kann. Erfolgreiche Beispiele hierfür sind Info-Plakate an zentralen Stellen und Bildschirmschoner bzw. Startscreens am PC.

Weitere Handlungsnotwendigkeiten werden deutlich, wenn man sich die Umfrageergebnisse zur Existenz von IT-Sicherheitsmaßnahmen ansieht: Hier treffen 34 Prozent der Unternehmen mit Produktneuheiten und sogar fast jedes zweite Unternehmen ohne Produktneuheiten überhaupt keine Schutzmaßnahmen gegen ungewollten Informationsabfluss. Angesichts der besonderen Bedrohung, die Cyberangriffe darstellen – sei es durch das Ausnutzen von Sicherheitslücken im IKT-Bereich, den direkten Angriff auf Maschinen und Anlagen mit Netzwerkeinbindung, die Schadsoftware-Infiltration per Internetnutzung *(Drive-by-Exploits)* oder gezielte Angriffe auf Sicherheits-Hardware (Router) und Firewalls –, ist dies unverständlich. Auch hier wurde im Rahmen der anschließenden Experteninterviews nachgefragt und nach Gründen gesucht: Den fehlenden IT-Schutz räumten die meisten Experten durchaus ein, wenn auch mit unterschiedlichen Begründungen. Überwiegend bestand durchaus große Bereitschaft, sich des Themas anzunehmen, doch scheitern diesbezügliche Bemühungen an Zeit und Ressourcen. Auch ist das Thema IT-Sicherheit inzwischen derart komplex, dass die Unternehmen sich bei der Auswahl der geeigneten Maßnahmen häufig überfordert fühlen. Sie haben keinen Überblick über wirkungsvolle und aktuelle Technologien. Hinzu kommt die Schnelllebigkeit mancher Lösung: Kaum ist ein wirksamer Schutz verfügbar, wird er schon wieder umgangen. Daher kapitulieren einige Unternehmen regelrecht vor dem Thema. Eher als Einzelfall zu betrachten ist in dem Kontext die Aussage eines KMU-Geschäftsführers, die in seinem Unternehmen verfügbaren Daten seien für Dritte nicht von Bedeutung, daher müsse er sie nicht weiter schützen.

Interessant ist auch ein Blick in die Historie: Die Unternehmen, die angaben, IT-Sicherheitsmaßnahmen implementiert zu haben, wurden nach dem Jahr der Ersteinführung befragt (vgl. *Abbildung 6*). Angesichts der schwer nachzuvollziehenden genauen Jahresdaten, ist eine Konzentration bei den „runden" Werten als normal anzusehen. Ein erster Peak liegt im Jahr 2000, was mit den zur Jahrtausendwende angekündigten Programmierfehlern und der Reaktion darauf gut zu erklären ist. Die gesteigerte Aktivität im Jahr 2005 ist nicht durch äußere Einflüsse, jedoch durch die oben genannten Rundungen bei der Schätzung der Jahreszahl erklärbar. Auffällig ist das Jahr 2010 als Beginn des aktuellen Jahrzehnts. Auch dieser Peak kann nicht

Abbildung 6 Jahr der Ersteinführung von IT-Sicherheitsmaßnahmen



Quelle: Fraunhofer ISI, Erhebung „Modernisierung der Produktion 2015".

direkt durch äußere Anlässe erklärt werden, jedoch über das Antwortverhalten bei Schätzungen und Erinnerungen. Die letzten drei Jahre sind noch sehr präsent; was davor geschah, aber sicher erst in diesem Jahrzehnt, wird auf das Jahr 2010 reduziert. Sichtbar wird dies z.B. an dem auffällig niedrigen Wert für 2011. Bedeutend ist vor allem, dass viele der befragten Unternehmen erst in den letzten Jahren überhaupt IT-Sicherheitsmaßnahmen getroffen haben – wohingegen die Nutzung von Hardware mit Internetzugang bereits seit den neunziger Jahren auch in Unternehmen zum Standard gehört. Hier besteht offensichtlich ein immenser Nachholbedarf.

Die abgefragte dritte Kategorie von Maßnahmen betrifft die Zugangskontrolle. Diese umfasst zum einen Maßnahmen zum Schutz vor physischem Zugang zu den Betriebs- und Produktionsstätten bzw. bestimmten Bereichen (z.B. Serverraum, Büros der Geschäftsleitung) durch Unbefugte (Zutrittskontrolle) und zum anderen Maßnahmen, die die Nutzung von Maschinen, Anlagen und vor allem Datenverarbeitungseinrichtungen durch Unbefugte verhindern sollen (Zugangskontrolle i.S.d. Nr. 2 der Aufzählung in der Anlage zu § 9 Satz 1 BDSG). Letzteres erfolgt klassisch über eine Kombination von Benutzername und Passwort. Gerade bei Maschinen und Anlagen ist oft festzustellen, dass die Standard-Zugangsdaten des Herstellers nicht geändert werden und dem Angreifer somit sein Vorhaben erleichtert wird, da die Zugangsdaten bekannt sind. Ist die Maschine sogar an das Internet angebunden, steigert sich das Risiko nochmals. Die Internetsuchmaschine Shodan[39] sucht gezielt nach ungeschützten Geräten, kategorisiert sie nach Typ und Standort und fragt sys-

39 Vgl. www.shodan.io [10.10.2017].

tematisch Schwächen ab. Die Maschinen nennen dabei sogar freiwillig Typ- und Seriennummern, oft sogar die Standard-Zugangsdaten im Klartext wie z.B. „Basic realm=Default: admin/1234“. Im Rahmen der Sicherheitskonferenz DEFCON hat der US-Sicherheitsexperte *Dan Tentler* Geräte vorgestellt, die er über diese Suchmaschine gefunden hat. Einige imposante Beispiele waren eine Autowaschanlage, die er live an- und abschalten konnte, sowie die Ampelsteuerung einer mittelgroßen US-Stadt und das Kontrollpanel eines französischen Wasserkraftwerks. Diese Beispiele verdeutlichen, dass bereits kleine Nachlässigkeiten bei der Inbetriebnahme von Gerätschaften große Sicherheitslücken hervorrufen können.

Ein ähnlich großes Potenzial für wirksame Präventionsmaßnahmen besteht im Bereich der Sicherheitsvorschriften für Mitarbeiter, die lediglich bei 60 Prozent der Betriebe ohne Produktneuheiten und immerhin bei 76 Prozent der Betriebe mit Produktneuheiten etabliert sind. Auch hier ist eine Umsetzung einfach und kostengünstig.

Zusammenfassend lässt sich feststellen, dass selbst innovative Unternehmen das Thema Gefahrenabwehr nicht umfassend adressiert haben und damit ein großer Nachholbedarf im Bereich des Schutzes von Unternehmensdaten vor allem bei KMU besteht.

5. Fazit

Für private oder öffentliche Unternehmen sowie Organisationen ist es von essenzieller Bedeutung, die zum Wettbewerbsvorteil beitragenden Informationen und vertraulichen Unterlagen in den eigenen Geschäftsräumen zu verwahren und Dritten nicht zugänglich zu machen. Besonders wenn Innovationskraft die Basis für den Geschäftserfolg darstellt, ist es wichtig, Frühwarnsignale drohender Angriffe zu erkennen und ernst zu nehmen. Immer stärker vernetzte Abläufe und automatisierte Prozesse – besonders im Rahmen von Industrie 4.0 – verlangen die Implementierung eines umfassenden Sicherheitssystems.[40]

Unternehmen sollten in Fragen der Sicherheit nicht allein auf die eigenen Ressourcen vertrauen. Es gibt umfangreiche Informationsangebote, die helfen, wirksame Maßnahmen zu identifizieren. Erster Ansprechpartner in allen Angelegenheiten des Schutzes vor ungewolltem Informationsabfluss sind die Polizeibehörden sowie die Landesämter für Verfassungsschutz. Auch das BSI sowie die Branchenverbände haben Angebote, um die Unternehmen im Bereich der Prävention zu unterstützen und zu informieren.

---

40 Vgl. *Hofer & Weiß* 2016, S. 31 ff.

Literatur

acatech/BDI, siehe acatech – Deutsche Akademie der Technikwissenschaften e. V. & Bundesverband der Deutschen Industrie e.V.

acatech – Deutsche Akademie der Technikwissenschaften e. V. & Bundesverband der Deutschen Industrie e.V. (2017): Innovationsindikator 2017. Schwerpunkt digitale Transformation; www.innovationsindikator.de/fileadmin/2017/PDF/Innovationsindikator_2017.pdf [25.07.2017]; zit.: acatech/BDI 2017.

Agentur Karg und Petersen, siehe Karg und Petersen – Agentur für Kommunikation GmbH.

Bitkom, siehe Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Blum, U. (2003): § 3: Volkswirtschaftliche Grundlagen, in: G. Gounalakis (Hrsg.), Rechtshandbuch Electronic Business. München, S. 44–68.

Blume, A. (2009): Awareness – Grundvoraussetzung für effektiven Know-how-Schutz in und außerhalb Chinas, in: J. Freimuth, R. Krieg, M. Luo, C. Müller & M. Schädler (Hrsg.), Geistiges Eigentum in China – Neuere Entwicklungen und praktische Ansätze für den Schutz und Austausch von Wissen. Wiesbaden, S. 121–130.

Bollhöfer, E. (2017): Schutz von Unternehmensdaten bei der Erbringung von E-Services. Wiesbaden.

Borges, G., Schwenk, J., Stuckenberg, C.-F. & Wegener, C. (2011): Identitätsdiebstahl und Identitätsmissbrauch im Internet. Heidelberg.

Brauch, P. (2004): DDoS-Erpressung gegen Online-Wettbüros. Heise online; www.heise.de/newsticker/meldung/DDoS-Erpressung-gegen-Online-Wettbueros-102957.html [12.02.2016].

BSI, siehe Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (2003): Studie: Kommunikations- und Informationstechnik 2010 + 3. Neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit; www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Trend2010/Trend2010_3.pdf?__blob=publicationFile&v=2 [10.10.2017], zit.: BSI 2003.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter; www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf [10.10.2017], zit.: Bitkom 2015.

Corporate Trust (2015): Studie: Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co?; http://s496374728.online.de/wp-content/uploads/2016/06/CT-Studie-2014_DE.pdf [03.11.2016].

Deutsches Institut für Normung (Normenausschuss Maschinenbau) und VDMA (2013): Status quo des Know-how-Schutzes im Maschinen- und Anlagenbau – INS-Studie; https://industrialsecurity.vdma.org/documents/16227999/31931764/INS+2013+Know-how+Schutz.pdf/4d9b7c20-c7c9-caff-0e64-df32711b9f88 [03.11.2016]; zit.: DIN 2013.

DIN, siehe Deutsches Institut für Normung.

Duscha, A., Klees, M. & Weisser, R. (2011): Studie Netz- und Informationssicherheit in Unternehmen 2011 – Ergebnisse einer Befragung von kleinen und mittelständischen Unternehmen in Deutschland. E-Commerce-Center Handel; www.mittelstand-digital.de/MD/

Redaktion/DE/PDF/studie-it-sicherheit-2011-pdf,property=pdf,bereich=md,sprache=de,rwb=true.pdf [15.09.2017].

Eckert, C. (2003): Mobil, aber sicher!, in: F. Mattern (Hrsg.), Total vernetzt. Szenarien einer informatisierten Welt. Berlin, S. 85–121.

Faber, E. v. (2009): Datensicherheit: Beyond the Hype; www.all-about-security.de/security-artikel/management-und-strategie/single/datensicherheit-beyond-the-hype/ [08.11.2016].

Fraunhofer-Institut für System- und Innovationsforschung ISI (2015): Erhebung „Modernisierung der Produktion"; www.isi.fraunhofer.de/de/publikationen/mitteilungen-modernisierung-produktion.html [10.10.2017].

Harte-Bavendamm, H. (2013): § 17 UWG, in: H. Harte-Bavendamm & F. Henning-Bodewig (Hrsg.), Gesetz gegen den unlauteren Wettbewerb (UWG). 3. Aufl. München.

Heckmann, D. (2006): Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen. Maßstäbe für ein IT-Sicherheitsrecht. MultiMedia und Recht (MMR) 5, S. 280–285.

Hofer, A. & Weiß, M. (2016), Wirtschafts- und Industriespionage. Informationsgewinnung – Management – Kompetenz. Wiesbaden.

Hofmann, K. (2013): Schutz der informationellen Selbstbestimmung von Unternehmen in „intelligenten" Netzwerken. Zeitschrift zum Innovations- und Technikrecht 1/4, S. 210–216.

Hohensee, M. (2013): Allgemeine Verunsicherung. Der Trend zu mobilen Geräten macht Technologiekonzerne anfällig für Hackerangriffe. Während die Politik über Gegenmaßnahmen streitet, boomt die Sicherheitsbranche. Wirtschaftswoche 10, S. 99.

Hummelt, R. (1997): Wirtschaftsspionage auf dem Datenhighway. Strategische Risiken und Spionageabwehr. München.

Institut für Demoskopie Allensbach (2011): Sicherheitsreport 2011. Eine repräsentative Studie zum Thema Sicherheit in Deutschland im Auftrag von T-Systems; www.ifd-allensbach.de/uploads/tx_studies/7660_Sicherheitsreport2011_01.pdf [27.07.2017]; zit.: IfD 2011.

Karg und Petersen – Agentur für Kommunikation GmbH (2010): Piraterie-Bekämpfung als Wettbewerbsfaktor. Wie stellen sich Unternehmen in Deutschland, Österreich und der Schweiz gegen Produkt- und Markenpiraterie auf?; www.textilwirtschaft.de/news/media/1/Ergebnisberi-zur-Stu-Pirate-Bekmpf-als-Wettbewerbs-1244.pdf [15.09.2017], zit.: Agentur Karg und Petersen 2010.

Knopp, M., Wilke, D., Hornung, G. & Laue, P. (2008): Grunddienste für die Rechtssicherheit elektronischer Kommunikation. MultiMedia und Recht (MMR) 11, S. 723–728.

Kochmann, K. (2009): Schutz des „Know-how" gegen ausspähende Produktanalysen („Reverse Engineering"). Berlin.

Koller, H., Raithel, U. & Wagner, E. (1998): Internationalisierungsstrategien mittlerer Industrieunternehmen am Standort Deutschland – Ergebnisse einer empirischen Untersuchung. Zeitschrift für Betriebswirtschaft (ZfB) 2/1998, S. 175–203.

Lux, C.& Peske, T. (2002): Competitive Intelligence und Wirtschaftsspionage – Analyse, Praxis, Strategie. Wiesbaden.

Pleitner, H.J. (1998): KMU vor dem Hintergrund der Internationalisierung. IO Management 3, S. 66–69.

Röder, N. (2011): Industriespionage – Risikofaktor Mensch. Masterarbeit. Hochschule Hannover, Fakultät IV – Abteilung Betriebswirtschaft; https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/298/ file/2011_07_21_SerWisS_Masterarbeit_Industriespionage_Risikofaktor_Mensch.pdf [10.10.2017].

Roßnagel, A. (2007): Datenschutz in einem informatisierten Alltag. Gutachten im Auftrag der Friedrich-Ebert-Stiftung; http://library.fes.de/pdf-files/stabsabteilung/04548.pdf [15.09.2017].

Ruetten, G. & Stutzke, O. (2005): Angriff von innen. Heise online; www.heise.de/security/artikel/Angriff-von-innen-270632.html [07.11.2016].

Schleupner, L. (2012): Perfekt sichere Kommunikation in der Automatisierungstechnik. Dissertation. Fernuniversität Hagen. Fakultät für Mathematik und Informationstechnik; https://ub-deposit.fernuni-hagen.de/servlets/MCRFileNodeServlet/mir_derivate_00000142/Diss_Schleupner_Kommunikation_2012.pdf [07.01.2013].

Sonnen, B. (2016): Wirtschaftsspionage und Konkurrenzausspähung – Untersuchung staatlicher Präventionsangebote für kleine und mittlere Unternehmen (KMU) in Deutschland. Unveröffentlichte Bachelor-Thesis. Hochschule Karlsruhe.

Warnecke, G. (2010): Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage, in: C. Fussan (Hrsg.), Managementmaßnahmen gegen Produktpiraterie und Industriespionage. Wiesbaden, S. 249–331.

Wiehler, G. (2004): Mobility, Security und Web Services. Neue Technologien und Serviceorientierte Architekturen für zukunftsweisende IT-Lösungen. Erlangen.

Wodtke, C. & Richters, S. (2004): Schutz von Betriebs- und Geschäftsgeheimnissen. Leitfaden für die Praxis. Berlin.

Staatliche Präventionsangebote zum Schutz vor Wirtschaftsspionage und Konkurrenzausspähung

Eine Analyse der Best Practices aus einigen europäischen Ländern zur Optimierung des Schutzes von KMU in Deutschland

Binia Sonnen & Esther Bollhöfer

1. Einleitung

Im Zentrum bisheriger Forschung zum Thema Wirtschaftsspionage und Konkurrenzausspähung[1] stehen die unterschiedlichen Angriffsarten und das Ausmaß der verursachten Schäden. Dieser Beitrag hingegen fokussiert die Erarbeitung von zusätzlichen Präventionsangeboten, die von staatlichen Stellen in Deutschland für kleine und mittlere Unternehmen[2] (KMU) bereitgestellt werden können, um deren Sicherheit zu erhöhen. Die Experteninterviews, die im Rahmen des Projektes WiSKoS geführt wurden, haben gezeigt, dass sich diese aufgrund fehlender Ressourcen oder fehlenden Gefährdungsbewusstseins nicht in demselben Umfang absichern wie große Konzerne.

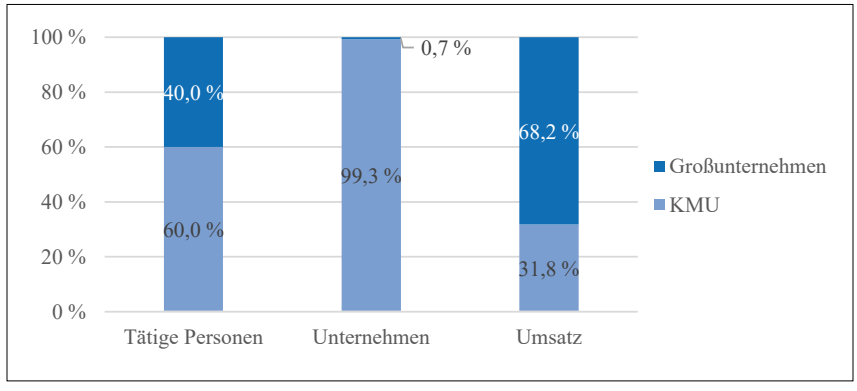
Da KMU für die deutsche Wirtschaftsleistung eine entscheidende Rolle spielen, ist die Gewährleistung ihrer Informationssicherheit besonders wichtig, um den Schutz der deutschen Wirtschaft vor Spionage und Ausspähung zu erhöhen. Wie aus *Abbildung 1* hervorgeht, waren im Jahr 2013 etwa 99,3 Prozent der 2,2 Mio. gemeldeten

---

1 Zur Definition vgl. *Abschnitt 2* der *Einleitung* im vorliegenden Band.

2 Klassifikation der EU: Unternehmen mit weniger als 250 Mitarbeitern und einem Jahresumsatz von unter EUR 50 Mio. oder einer Jahresbilanz von unter EUR 43 Mio. werden als mittlere Unternehmen angesehen. Die Richtwerte für kleine Unternehmen liegen bei 50 Mitarbeitern und einem Jahresumsatz/einer Jahresbilanz unter EUR 10 Mio. Unternehmen mit weniger als 10 Mitarbeitern und einem Jahresumsatz von unter EUR 2 Mio. zählen zu der Gruppe der Kleinstunternehmen (vgl. Europäische Union 2003, Die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Amtsblatt der Europäischen Union Nr. L 124; Art. 2; http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3An26026 [15.09.2017]).

Abbildung 1 KMU und Großunternehmen in Deutschland im Vergleich



Quelle: Eigene Darstellung auf Basis von Destatis 2013.

Unternehmen[3] der Gruppe der KMU zuzuordnen. Die 60 Prozent der Beschäftigten, die in KMU tätig waren, erwirtschafteten etwa ein Drittel des Gesamtumsatzes in Deutschland (ca. 32 %).

Im Zentrum dieses Beitrags stehen staatliche Präventionsangebote zum Schutz vor Wirtschaftsspionage und Konkurrenzausspähung, die speziell auf KMU ausgerichtet sind. Es wird analysiert, inwieweit bestehende Maßnahmen verbessert werden können oder ob es neuer Maßnahmen bedarf. Sogenannte Best Practices aus anderen Ländern, namentlich aus Bulgarien, Dänemark, Großbritannien, Österreich und der Schweiz, sollen als Anhaltspunkte dienen, um in Deutschland neue, aber bewährte Maßnahmen zu implementieren. Es sollen folgende Fragen beantwortet werden:

- Welche staatlichen Präventionsmaßnahmen werden in anderen Ländern angeboten?
- Wo findet eine erfolgreiche Kooperation zwischen staatlichen Stellen und Unternehmen statt und wie ist diese gestaltet?
- Welche Maßnahmen helfen effektiv, Unternehmen vor Angriffen auf ihr Know-how zu schützen?

Wirtschaftsspionage und Konkurrenzausspähung stellen globale Phänomene dar, die nicht an Landesgrenzen enden. Die weltweite Verknüpfung der Angriffe erfordert eine lösungsorientierte Herangehensweise, die über nationale Ansätze hinausgeht. Dieser Forderung soll durch die Ermittlung von Best Practices anderer Länder

---

3 Diese Unternehmen gehören nach der Klassifikation der Wirtschaftszweige, Ausgabe 2008, den Wirtschaftsabschnitten B bis N (außer K) und S95 an (vgl. Destatis 2008, S. 76–140).

Rechnung getragen werden. Zur Analyse der etwaig bestehenden Erfolgskonzepte sind Experteninterviews geführt worden. Aus den hieraus ermittelten Best Practices werden konkrete Maßnahmen abgeleitet, bewertet und in diesem Beitrag vorgestellt. Mit Bezug auf die zeitliche Umsetzbarkeit erfolgt eine Einteilung in kurz-, mittel- und langfristige Angebote, die abschließend im Hinblick auf ihre Übertragbarkeit auf Deutschland untersucht werden.

2. Stand der Forschung

Die Begriffe Wirtschaftsspionage und Konkurrenzausspähung werden von vielen wirtschaftlichen und gesellschaftlichen Akteuren verwendet und üblicherweise durch die hinter den Angriffen stehenden Handelnden unterschieden. Der Definition der *Wirtschaftsspionage* folgend, die bereits im Rahmen der Einleitung zu diesem Band gegeben wurde, umfasst diese staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung bzw. Aufklärung von Wirtschaftsunternehmen und Betrieben.[4] Wirtschaftsspionage ist langfristig angelegt und zielt auf Geheimnisse aus den Bereichen Politik, Verwaltung, Militär und Forschung ab, aber auch die Wirtschaft ist immer häufiger betroffen.[5] Davon abzugrenzen ist die ebenfalls einleitend definierte *Konkurrenzausspähung*. Sie ist eher kurzfristig angelegt und dient der Ausspähung von Produktinformationen und Prozessabläufen. Geschädigter ist in diesem Falle ein Einzelner bzw. ein einzelnes Unternehmen und nicht die gesamte Volkswirtschaft.[6] *Kilchling* und *Carl* stellen allerdings die Relevanz dieser Unterteilung besonders für KMU infrage.[7] Sie verweisen auf die aus Sicht der Betroffenen deutlich schwerer wiegenden möglichen materiellen und immateriellen Schäden. Oft ist die Urheberschaft der Angriffe für KMU nicht auszumachen und somit auch die strafrechtliche Zuständigkeit,[8] die aus dieser Unterteilung resultiert, den Unternehmen nicht klar.

Existierende Studien fokussieren weniger die spezifische Situation der KMU und die Prävention als die aktuelle Bedrohungslage und Betroffenheit von Unternehmen

---

4 Vgl. *Graf & Otte* 2011; *Carl, Kilchling, Knickmeier & Wallwaey* 2017, S. 2.

5 Vgl. *Kasper* 2014, S. 8.

6 Vgl. *Graf & Otte* 2011.

7 Vgl. *Kilchling & Carl* 2016, S. 186–187.

8 Wirtschaftsspionage fällt in den Bereich der Staatsschutzkriminalität. Es handelt sich um ein Offizialdelikt, das von Amts wegen verfolgt wird. Das Legalitätsprinzip verpflichtet die LKAs, das BKA und die Polizei dazu, Ermittlungen einzuleiten, sobald der Verdacht einer Straftat besteht. Konkurrenzausspähung hingegen ist ein relatives Antragsdelikt, das von den Betroffenen selbst angezeigt werden muss und ansonsten nur verfolgt werden kann, wenn die Staatsanwaltschaft das Bestehen eines besonderen öffentlichen Interesses an der Strafverfolgung bejaht.

allgemein. Corporate Trust[9] hat zum Beispiel in einer Studie zur Industriespionage bezüglich der Betroffenheit ermittelt, dass etwa die Hälfte der befragten Unternehmen (in Deutschland: n = 412) zwischen 2012 und 2014 einen Angriff oder versuchten Angriff zu verzeichnen hatten. Prävention betreffende Studien der vergangenen Jahre wurden von Prüfungsgesellschaften und Unternehmensberatungen wie KPMG, Ernst & Young und der PricewaterhouseCoopers AG (PwC) durchgeführt. Die weitgehende Fokussierung auf IT-Themen legt jedoch nahe, dass hiermit eigene (Beratungs-)Ziele verfolgt werden und kein Beitrag zum strukturellen Verständnis geleistet werden soll. Es ist also erforderlich, die Phänomene der Wirtschaftsspionage und Konkurrenzausspähung im Rahmen unabhängiger Forschung zu betrachten und neue belastbare Daten zu erheben. Das Feld der Informationssicherheit hat sich in den letzten Jahren insgesamt als sehr aktiv erwiesen. Es beschäftigen sich nicht nur Forschungsinstitute und Dienstleister, sondern auch zahlreiche Verbände, Unternehmen, Behörden und die Politik aktuell mit dieser Thematik. So wurde beispielsweise im April 2016 mit der Initiative Wirtschaftsschutz (www.wirtschaftsschutz.info) ein Kooperationsprojekt zwischen den Sicherheitsbehörden des Bundes und Partnern aus der Wirtschaft gestartet, um unter dem Leitmotiv „Prävention durch Dialog und Information“ Unternehmen, Forschungseinrichtungen und öffentlichen Stellen eine zentrale Anlaufstelle bei Fragen zum Wirtschaftsschutz zu bieten.

In Deutschland sind besonders KMU gefährdet, von illegalem Wissensabfluss betroffen zu werden. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) kommt in seiner Studie zum Thema „Wirtschaftsschutz im digitalen Zeitalter“ aus dem Jahr 2015[10] zu dem Ergebnis, dass zwischen 2013 und 2015 51 Prozent der deutschen Unternehmen Opfer von digitaler Ausspähung wurden. Kleine Unternehmen waren zu 47 Prozent betroffen, mittelständische Unternehmen zu 61 Prozent und Großunternehmen zu 54 Prozent. Es wird deutlich, dass besonders kleine und mittlere Unternehmen unter digitaler Ausspähung zu leiden hatten, sogar in höherem Maß als große Unternehmen. Zu ähnlichen Ergebnissen gelangen auch Corporate Trust sowie *Birkner*.[11] Daher ist zu fragen: „Wie sehen gute/erfolgreiche Präventionsangebote in anderen europäischen Ländern aus und (wie) lassen sich diese Erfolgskonzepte auf KMU in Deutschland übertragen?“

3. Methodik und Vorgehen

Um das Wissen über die Phänomene der Wirtschaftsspionage und Konkurrenzausspähung zu erweitern, war es möglich, sowohl quantitative als auch qualitative Studien durchzuführen. Da die beiden Deliktsbereiche bislang kaum wissenschaftlich

---

9 Vgl. Corporate Trust 2014, S. 8.

10 Vgl. Bitkom 2015, S. 5.

11 Vgl. Corporate Trust 2014; vgl. *Birkner* 2014.

untersucht worden sind, wurde eine offene, explorative Herangehensweise bevorzugt. Auf welche Weise staatlich unterstützte Prävention gegen Wirtschaftsspionage und Konkurrenzausspähung für KMU in Deutschland verbessert werden kann, lässt sich alleinig anhand von quantitativen Auswertungen – wie Mittelwerten, Varianzen und Häufigkeiten – nicht beschreiben. Daher verlangt die Untersuchung der Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung und besonders der Präventions- und Erkennungsstrategien in Deutschland und Europa eine qualitative Datenerhebung. Als Erhebungsmethode wurde das Experteninterview ausgewählt, da es einen Blick auf die Metaebene der betrachteten Phänomene ermöglicht und maßgeblich dazu beitragen kann zu erfahren, „aus welcher Perspektive und mithilfe welcher Begrifflichkeiten in der Gesellschaft über bestimmte Probleme nachgedacht wird."[12] Die Gespräche mit Experten ermöglichen es, ein umfassendes Bild aus verschiedenen Blickwinkeln von Wirtschaftsspionage und Konkurrenzausspähung zu zeichnen. Zur Unterstützung der Interviews findet ein semi-strukturierter Gesprächsleitfaden Anwendung. Dieser erlaubt einerseits das Eingehen des Interviewers auf die jeweilige Interviewgruppe und deren länderspezifische Besonderheiten, andererseits wird sichergestellt, dass die Ergebnisse vergleichbar sind. Die sich an die Datenerhebung anschließende inhaltsanalytische Auswertung der anonymisierten Gesprächsprotokolle erfolgt softwareunterstützt[13] anhand eines eigens entwickelten Codierleitfadens. Die Einhaltung der Gütekriterien für wissenschaftliche Erkenntnismethoden ist durch das Vier-Augen-Prinzip und die kommunikative Validierung gewährleistet.

Die Experteninterviews wurden in den fünf oben genannten europäischen Vergleichsländern durchgeführt und bieten die Datengrundlage zur Identifizierung wirkungsvoller staatlicher Präventionsangebote. Die Länderauswahl erfolgte anhand des normativen und soziokulturellen Rahmens, des Innovationsgrades der Länder und, sofern vorhanden, statistischer Daten zur Strafverfolgung von Wirtschaftsspionage und Konkurrenzausspähung. Da die Anzeigebereitschaft in Deutschland sehr gering ist, besteht die Hoffnung, Erfolgskonzepte zu ermitteln, die die Kooperation deutscher Unternehmen mit Behörden verbessern können. Die einzelnen Experten der analysierten Länder Bulgarien, Dänemark, Großbritannien, Österreich und der Schweiz stammen aus Behörden, Wissenschaftsorganisationen und der Industrie. In der Untersuchung von Wirtschaftsspionage und Konkurrenzausspähung können sie einen Überblick über die nationalen Strukturen und bereits implementierten Präventionsstrategien geben und gleichzeitig eine erste Bewertung der einzelnen Maßnahmen vornehmen, da sie in unmittelbarem Kontakt zur Zielgruppe der KMU stehen oder dieser sogar selbst angehören. Im ersten Schritt ist es das Ziel herauszufinden, welche staatlichen Präventionsmaßnahmen angeboten, ob diese genutzt und wie sie

---

12 *Bogner, Littig & Menz* 2014.

13 Genutzt wurde die MaxQDA Version 11 der VERBI GmbH.

von ihren Nutzern, also Unternehmen, bewertet werden. Erst wenn dies bekannt ist, kann überprüft werden, ob sie sich auch für Deutschland ganz oder in Teilen eignen.

4. Analyse der im europäischen Ausland ermittelten Best Practices

Die folgenden Abschnitte stellen die Ergebnisse der Experteninterviews dar. Zuerst wird ein Überblick über die Auswahl der einzelnen Länder gegeben, dann die Wahrnehmung der Phänomene Wirtschaftsspionage und Konkurrenzausspähung sowie der allgemeinen staatlichen Aktivitäten dargestellt. Anschließend folgt die Darstellung der einzelnen Best Practices.

4.1 Länderauswahl und Wahrnehmung der Phänomene

Nach umfassenden Analysen der 28 EU-Mitgliedstaaten und der Schweiz wurden Bulgarien, Dänemark, Großbritannien, Österreich und die Schweiz für die nähere Betrachtung und die qualitative Datenerhebung ausgewählt. Die Gespräche mit den jeweiligen Länderexperten haben die Aktualität des Themas bestätigt und gezeigt, dass es bislang keine ideale und allgemeingültige Lösung für das Problem des illegalen Wissensabflusses gibt. Jedes Land hat jedoch eigene Herangehensweisen bezüglich staatlicher Präventionsmaßnahmen entwickelt und stellt dabei auf unterschiedliche Aspekte im Umgang mit Wirtschaftsspionage und Konkurrenzausspähung ab. Teilweise liegt der Schwerpunkt auf der Bereitstellung von Informationen, teils auf Präventionsmaßnahmen und teils in der Strafverfolgung, also auf repressiven Maßnahmen. Für die einzelnen Länder lässt sich die Wahrnehmung der Phänomene und der angebotenen staatlichen Maßnahmen wie folgt zusammenfassen:

Bulgarien steht noch am Anfang der Bereitstellung staatlicher Angebote, allerdings ist die Bedrohungswahrnehmung auch weitaus geringer als in den anderen betrachteten Ländern. Unternehmen sind deutlich weniger innovativ tätig. Produktpiraterie stellt ein größeres Problem dar als illegaler Wissensabfluss, der in diesem Beitrag thematisiert wird. Dennoch ist die Anzahl der vor Gericht verhandelten Fälle besonders hoch, sodass das Land für eine genauere Betrachtung ausgewählt wurde.

Dänemark weist einen sehr hohen unternehmerischen Innovationsgrad, überdurchschnittliches gesellschaftliches Vertrauen und eine sehr offene Grundhaltung der Bevölkerung gegenüber der Staat auf. Es ist daher interessant zu untersuchen, ob die Kombination aus hoher Innovationskraft mit einem offenen, vertrauensvollen Umgangsstil zu einer höheren Anzahl an Angriffen auf Unternehmensgeheimnisse führt oder ob die Zahlen deshalb gering sind, da die Unternehmen außerordentlich gut geschützt sind. Der Staat und die Behördenstruktur sind positiv konnotiert und wirken auf die Befragten im Hinblick auf den Umgang mit der Problematik unterstützend. Ein zu großer Fokus auf repressive Maßnahmen wird abgelehnt, Program-

me zur Förderung des Problembewusstseins und zur Umsetzung von Präventionsmaßnahmen werden jedoch herausgestellt. Eine große Anzahl von Projekten wird in einem Multi-Stakeholder-Ansatz durchgeführt; hierbei sind alle unterschiedlichen Interessensgruppen vertreten.

Großbritannien ist aufgrund seines sich unterscheidenden Rechtssystems für die genauere Betrachtung ausgewählt worden. Hier herrscht das Common Law, im Gegensatz zum Civil Law, das im kontinentaleuropäischen Raum stärker verbreitet ist. In Großbritannien befassen sich viele verschiedene staatliche Stellen mit dem Themengebiet der Informationssicherheit und Teilaspekten von Spionage und Ausspähung. Die Befragten nehmen dies allerdings als undurchsichtige Strukturen mit nicht klar erkennbaren Zuständigkeiten wahr. Die zahlreichen staatlichen Angebote werden aufgrund fehlender Kommunikation kaum genutzt, obwohl sie als gut bewertet werden. Das große staatliche Angebot rückt Kammern und Verbände in den Hintergrund; sie spielen kaum eine Rolle in der Prävention.

Österreich ist ähnlich aufgestellt wie Deutschland. Die am BIP gemessene F&E-Quote ist in Österreich sehr hoch, ebenso die Anzahl an Patentanmeldungen. Beides sind Zeichen für eine wissensintensive Unternehmenslandschaft und haben das Land für die nähere Betrachtung qualifiziert. Es erstaunt, dass die staatlichen Angebote in Österreich vorrangig von KMU genutzt werden. Die Experteninterviews mit KMU in Deutschland haben gezeigt, dass die Zusammenarbeit mit Behörden als sehr bürokratisch und ressourcenintensiv wahrgenommen und daher oft vermieden wird. Wenn jedoch in Österreich eine funktionierende Kooperation zwischen Behörden und KMU existiert, ist das Anlass, diese genauer zu betrachten.

Die *Schweiz* ist im Gegensatz zu den anderen ausgewählten Ländern kein Mitgliedsstaat der Europäischen Union. Es ist interessant herauszuarbeiten, ob in der Schweiz Prävention vor Wirtschaftsspionage und Konkurrenzausspähung anders umgesetzt wird und wenn ja, wie. Das Land zählt zu den innovativsten und wettbewerbsfähigsten Ländern der Welt und ist dadurch besonders attraktiv für Ausforschungsaktivitäten und Datendiebstahl. In der Schweiz wird der Staat, der zuweilen direkt in die Wirtschaft eingreift, als überdurchschnittlich stark empfunden. Der Nachrichtendienst des Bundes (NDB) beispielsweise betreibt eine aktive Informations- und Präventionsstrategie und steht in engem Kontakt zu Unternehmen. Das Vertrauen in staatliche Stellen ist höher als in den anderen untersuchten Ländern.

In den befragten Ländern machen KMU – ähnlich wie in Deutschland – einen bedeutenden Teil der Unternehmenslandschaft aus und stellen viele Arbeitsplätze bereit, sind aber nicht in besonderem Maße geschützt. Kritische Infrastrukturen hingegen unterliegen in allen Ländern speziellen Regelungen zum Schutz geheimer Unternehmensdaten und erfahren gezielt staatliche Unterstützung bei der Umsetzung von Präventionsmaßnahmen. Einige wenige staatliche Angebote für KMU, die z. T. auch bereits erfolgreich implementiert wurden, konnten jedoch identifiziert werden. Im

Folgenden werden die durch die Experteninterviews identifizierten Best Practices zu Präventionsangeboten aufgezeigt und analysiert.

4.2 Identifizierte Best Practices

Die im Folgenden aufgeführten Maßnahmen und Programme sind einige Beispiele, die aus den Experteninterviews hervorgegangen sind. Sie erheben daher keinen Anspruch auf Vollständigkeit und sollen eher Impulse zur Diskussion der Weiterentwicklungsmöglichkeiten in Deutschland bieten.

4.2.1 Public-Private-Partnership-Programme

In Bulgarien wird der Fokus in Projekten zur Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung auf Public-Private-Partnership-Programme (PPP) gelegt. Diese Multi-Stakeholder-Ansätze werden favorisiert, da so gewährleistet werden kann, dass die Bedürfnisse von allen betroffenen Gruppen Berücksichtigung finden. Bei der Entwicklung von weitreichenden Projekten ist die Zusammenarbeit mit allen Beteiligten als wichtig angesehen, um unterschiedliche Sichtweisen kennenzulernen und das Projekt an den Bedürfnissen möglichst jedes Einzelnen auszurichten. Nach Angaben der Experten werden immer mehr Projekte in einer Kooperation zwischen staatlichen Stellen und privaten Unternehmen durchgeführt. Innerhalb der Unternehmen erziele die Implementierung von Präventionsmaßnahmen im Top-down-Ansatz zwar oft eine erhöhte Informationssicherheit, allerdings ohne dabei auf die einzelnen Mitarbeiter einzugehen und diese umfassend über die Hintergründe zu informieren und aufzuklären. Dabei könne das umfassende Einbeziehen aller Beteiligten den Erfolg des Know-how-Schutzes erhöhen. Auch in der Zusammenarbeit mit den Behörden besteht bei bulgarischen Unternehmen teils das Gefühl, dass Regelungen und Gesetze im Top-down-Ansatz entwickelt werden, die für sie nicht nachvollziehbar sind. In diesen Fällen liegt keine ausgeglichene Kooperation zwischen den Parteien vor. Um diesem Informationsmissverhältnis entgegenzuwirken, stufen die Befragten PPP als erfolgreich zur Erhöhung der Informationssicherheit ein, da sie bei mehreren kleineren Projekten bereits gut funktioniert haben.

4.2.2 Umfassende Definition kritischer Infrastrukturen

Ein weiteres Beispiel, das mithilfe der bulgarischen Experten identifiziert werden konnte, ist die Definition der Unternehmen, die zu den kritischen Infrastrukturen zählen. In Bulgarien gehören ihnen mehr Branchen an als in den meisten anderen europäischen Ländern. Insgesamt zählen nach Angaben der Befragten 16–19 Branchen zu den kritischen Infrastrukturen. Es sind somit mehr Unternehmen berechtigt, eigens ausgearbeitete Programme zur Informationssicherheit und für den gesamten Schutz des Unternehmens zu nutzen. Des Weiteren sind sie auf Grund der Zugehörigkeit zu den kritischen Infrastrukturen dazu verpflichtet, ihre Daten zu schützen,

Vorfälle aufzuzeichnen und Angriffe an das nationale CERT (Computer Emergency Response Team) zu melden.

4.2.3 ICT-Engineers – Verfügbarkeit hochqualifizierter Fachkräfte

In Dänemark gibt es ein Modell, um die Expertise einzelner Fachkräfte zentral aufzubauen und anschließend dezentral anzubieten. Sogenannte ICT-Engineers sind sehr gut ausgebildete Experten auf dem Gebiet der Informations- und Kommunikationstechnologien. Sie sind dem National Cyber Crime Center (NC3) der dänischen Polizei unterstellt und für unterschiedliche Regionen zuständig. Innerhalb dieser können die lokalen Polizeidienststellen bei Bedarf die Unterstützung durch einen ICT-Engineer beantragen:

> In case of a criminal incident (hacking, ransom), actors are forced to contact the police. The first contact must be the local police and nobody else. The local police might ask for consultancy by the Danish police's National Cyber Crime Center. They have officers (ICT engineers) in every region of the country and support the local police with their expertise.

Dieser temporäre Einsatz mobiler Fachkräfte spart besonders in kleinen Behörden Ressourcen ein, da Experten dort nicht permanent angestellt sind, sondern nur bei Bedarf unterstützen. Um langfristig mit den sich fortwährend weiterentwickelnden Angriffsformen und Bedrohungen umgehen zu können, ist die Verfügbarkeit hochqualifizierter Experten essentiell. Innovative KMU sind in Dänemark immer wieder in ländlichen Gebieten angesiedelt, die außerhalb des direkten Einflussgebietes nationaler Behörden liegen. Zwar haben Polizeibehörden einen Auftrag zur Präventionsarbeit, jedoch fehlt gerade in lokalen Dienststellen die Erfahrung und das Fachwissen zu Spionage und Ausspähung. Die Ansiedelung gut ausgebildeter Experten ist auch auf dem Land und in kleineren Polizeidienststellen bedeutend, um flächendeckende staatliche Präventionsarbeit leisten zu können.

4.2.4 Risikoanalysen durch staatliche Stellen und Gutscheinprogramme

Ebenfalls in Dänemark nehmen laut Auskunft der Experten bereits viele Unternehmen die Gefahr des illegalen Wissensabflusses durch Wirtschaftsspionage und Konkurrenzausspähung wahr. Oft stehen aber keine ausreichenden Ressourcen zur Verfügung, um eine Analyse des Informationssicherheitssystems vorzunehmen. In Dänemark haben Unternehmen die Chance, Risikoanalysen durch staatlichen Stellen durchführen zu lassen. Eine solche Bewertung schließt das implementierte Informationssicherheitskonzept mit ein und spiegelt dem einzelnen Unternehmen wider, wie gut es gegen Wirtschaftsspionage und Konkurrenzausspähung abgesichert ist. Da ein solches Angebot für den Staat sehr kostspielig ist, steht dieses Erfolgskonzept in Dänemark jedoch lediglich den Top 20 der börsennotierten Unternehmen zur Verfügung.

In Großbritannien konnte eine ähnliche Praxis identifiziert werden. Die Experten sprachen hier von einer ressourcenschonenden Alternative zu personalintensiven Risiko-Assessments vor Ort. Eine äquivalente Analyse des Sicherheitssystems durch ein online verfügbares Tool ist hier bereits nutzbar – die sogenannten *Cyber Essentials*.[14] Es wird von den Experten als sehr effektiv eingeschätzt, werde allerdings bislang kaum von KMU genutzt. Unternehmen können eigenständig einen Test durchführen, um zu erfahren, wie gut ihre Cybersicherheit ausgebaut ist. Über eine Plakette ist dann öffentlich ersichtlich, ob ein Unternehmen durch die Cyber Essentials zertifiziert ist und somit staatlich ausgeschriebene Standards erfüllt. Auf lokaler Ebene unterstützen Polizeidienststellen KMU bei der Auswahl und Einführung angemessener Präventionsmaßnahmen. Zusätzlich gibt es die Möglichkeit über ein Gutscheinprogramm finanzielle Unterstützung zu erhalten, um die für die Informationssicherheit notwendigen Maßnahmen zu implementieren und sich anschließend bei staatlich zertifizierten Stellen einem Risiko-Assessment zu unterziehen. Auf diese Weise werden besonders KMU dazu angeregt, der Informationssicherheit einen höheren Wert beizumessen.

4.2.5 Zielgruppenspezifische Ansprache der Unternehmen/ leichter Zugang zu Angeboten

Neben den eben vorgestellten Cyber Essentials gibt es in Großbritannien zahlreiche weitere Angebote von unterschiedlichen Behörden, wie dem GCHQ (Government Communications Headquarters), dem CPNI (Centre for the Protection of National Infrastructure) oder dem CERT;[15] sie werden jedoch nach Einschätzung der Experten ebenfalls kaum genutzt:

> The government does a great job and invests a lot of money. But it would be an exponentially huge change if the government would improve communicating.

In mehreren Gesprächen wurde deutlich, dass hier primär ein Kommunikationsdefizit vorliegt, da die Angebote zwar sehr gut für KMU geeignet sind, dies der Zielgruppe nur noch nicht bewusst ist. Zwar handelt es sich hierbei nicht um ein klassisches Beispiel für Best Practices, doch verdeutlicht es die Wichtigkeit des leichten Zugangs zu Informationen und Präventionsangeboten. Es reicht nach Angaben eines Experten nicht aus, Angebote über Flyer und einen Internetauftritt zu bewerben, selbst wenn staatliche Angebote als besonders glaubwürdig bewertet werden:

---

14 Siehe www.cyberessentials.org [15.09.2017].

15 Beispielsweise „20 Critical Controls“ des CPNI, das Gutschein System für die Cyber Essentials Zertifizierung oder das Onlineforum „Cybersecurity Information Sharing Partnership“ des GCHQ.

> The government offerings are rated quite high. It's got a HMG[16] stamp on, so in general it's trusted, e.g. GCHQ. But they have the problem that sometimes they are too broad, for some problems it's not specific enough. The second problem is how they are getting the message out there.

Staatliche Angebote müssen den Experten zufolge besser auf die Bedürfnisse der unterschiedlichen Unternehmen ausgerichtet sein und diese direkt adressieren.

4.2.6 Online-Plattform zum Informationsaustausch

Um Know-how von einzelnen Wissensträgern an einen großen Nutzerkreis weiterzugeben, wird in Großbritannien eine Online-Plattform genutzt. Die identifizierte Best Practice, die hier Anwendung findet, ist die Plattform Cybersecurity Information Sharing Partnership (CiSP)[17], die ähnlich wie der Social-Media-Kanal Facebook funktioniert. Sie ist 2013 als Partnerschaftsprojekt zwischen der Regierung und der Industrie eröffnet worden. In unterschiedlichen Gruppen und Foren tauschen sich registrierte Nutzer themenspezifisch aus, Meldungen über aktuelle Bedrohungen werden nach Art eines Newstickers veröffentlicht und Checklisten sowie Informationsmaterial zum Download angeboten. Die von den Experten angesprochene Informationsvielfalt des Portals ergibt sich zum einen durch den aktiven Austausch der Mitglieder in Fachforen und zum anderen durch die Möglichkeit der Diskussion über aktuelle Angriffe in Echtzeit. Eine Registrierung zu dieser Plattform ist nur per Einladung durch einen anderen Nutzer möglich. Es können individuelle und Unternehmens-Konten eröffnet werden. Nutzungsanfragen von Einzelpersonen müssen jedoch erst durch einen Kollegen des gleichen Unternehmens validiert werden. So ist sichergestellt, dass nur real existierenden Mitarbeitern Zugriff auf die Inhalte gewährt wird.

4.2.7 Informelle Gesprächsrunden

Eine Best Practice, die länderübergreifend von mehreren Experten als sehr wichtige und ergiebige Informationsquelle eingestuft wurde, sind informelle Gesprächsrunden. Der Austausch in etablierten Netzwerken mit befreundeten Unternehmern, Bekannten, Kollegen, aber auch Mitarbeitern staatlicher Stellen findet oft branchenübergreifend und in vertraulichem Rahmen statt. In einem der österreichischen Interviews merkt der Befragte an:

> Es ist wichtig, dass der informelle Rahmen gewahrt wird. Sie [die Gesprächsrunden] sollten klein und vertraulich bleiben, nicht zu groß werden und nicht in der Öffentlichkeit stehen. Es besteht sonst die Gefahr, dass das Netzwerk selbst zum Angriffspunkt wird.

---

16 HMG – Her Majesty's Government (Britische Regierung).

17 Siehe www.ncsc.gov.uk/cisp.

Der Aufbau eines solchen Netzwerkes kann sehr langwierig sein, da besonders die Bildung von Vertrauen viel Zeit benötigt, wie der britische Länderexperte erläuterte. Der CIO (Chief Information Officer) eines Energieunternehmens aus Großbritannien hat die Erfahrung gemacht, dass mehr Informationen zu aktuellen Bedrohungen und dem Umgang mit ebendiesen innerhalb des Netzwerkes geteilt werden, je mehr Erfahrungen das eigene Unternehmen in die Diskussion einbringt. Er sagt:

> The key there is how it's done and how confidential the reporting process is. If you tell me that you promise if I tell you what's going on, you're going further and then I would probably tell you more – but in the second that it does leak out then I'm never going to talk to you again.

Die Wichtigkeit des Vertrauens bezüglich der Geheimhaltung entsprechender Informationen wird hier besonders deutlich. Besteht ein Vertrauensverhältnis, werden Informationen erwartungsgemäß offen mit den Beteiligten geteilt. Wird das Vertrauen jedoch missbraucht, kann das Unternehmen die Kooperation sofort beenden. Durch den informellen Charakter und die sehr kurzen Kommunikationswege werden offenbar selbst tagesaktuelle Ereignisse weitergegeben. So wurde laut Expertenbericht beispielsweise die Problematik des CEO-Frauds in einigen österreichischen Netzwerken bereits eineinhalb Jahre vor der offiziellen Warnung der Kammern und Behörden diskutiert.

4.2.8 Melde- und Analysestelle Informationssicherheit

Die Melde- und Analysestelle Informationssicherheit (MELANI) in der Schweiz ist speziell für KMU ausgelegt und veröffentlicht etwa halbjährlich umfassende Reports zu den wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in den Informations- und Kommunikationstechnologien (IKT). Zusätzlich stehen Checklisten und Anleitungen zum Download bereit, um die Absicherung der Unternehmenssysteme in verschiedenen Themenbereichen zu unterstützen. MELANI stellt keine konkreten Programme, sondern generelle Vorgehensweisen zum Informationsschutz vor. Die Themen Social Engineering, Schadsoftware in E-Mails und auf Internetseiten, Phishing, Internet-Attacken, gefälschte Supportanrufe, Spam und Verschlüsselungstrojaner werden steckbriefartig, gut verständlich und mit Beispielen erläutert. Die Plattform MELANI dient nicht nur Informations- und Präventionszwecken, es besteht auch die Möglichkeit, Angriffe anonym über ein Onlineformular zu melden. Die Auswertung der eingegangenen Meldungen soll darüber hinaus helfen, das Informationsangebot auf die Bedürfnisse der Nutzer auszurichten.[18] Bei Angabe einer E-Mailadresse können Vorfälle je nach freien Ressourcen technischen Analysen unterzogen werden. Zur strafrechtlichen Abklärung

---

18 Vgl. MELANI 2012, 2. Abs.

verweist MELANI an die zuständigen Behörden und empfiehlt eine Meldung an die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität. Dem Großteil der Unternehmen aus der Schweiz ist MELANI bekannt und die Plattform wird aktiv genutzt.

4.2.9 Höhere Serviceorientierung

Die befragten Unternehmen aller Länder geben an, zumindest in IT-Fragen nicht auf staatliche Angebote angewiesen zu sein, da zahlreiche Dienstleister Sicherheitschecks, Penetrationstests, Präventionsmaßnahmen und Frühwarnungen in unterschiedlichen Preissegmenten anbieten. Sie könnten bei fehlendem eigenen Know-how präventiv auf diese zurückgreifen, liefern jedoch keine Erklärung, warum sie es nicht bereits tun. Aus Sicht der Unternehmen fehlt den staatlichen Stellen die Serviceorientierung, um auf Augenhöhe mit den Unternehmen kooperieren zu können. Dies schließt auch die Erreichbarkeit von zuständigen Behörden und Abteilungen ein. Das Internet kennt keine Öffnungszeiten und gerade Cyberangriffe können jederzeit erfolgen. Eine direkte Mailadresse ist einer „info@-Mailadresse“ vorzuziehen. Ebenso werden allgemeine Telefonnummern, die nur an Werktagen von 8 bis 15 Uhr erreichbar sind, als nicht ausreichend eingestuft. Eine 24-Stunden-Notfallnummer ist gewünscht. Die befragten Experten betonen immer wieder, dass es bei einem Angriff besonders wichtig ist, zeitnah zu handeln:

> Zeitnahe Warnungen und Unterstützung auf operativer Ebene würden uns weiterhelfen. Eine schlagkräftige Einheit mit dem nötigen Know-how, die im Angriffsfall schnell agiert – eine Wunschvorstellung.

Da besonders KMU oft nicht sofort wissen, welche Schritte einzuleiten sind, benötigen sie professionelle Unterstützung und gerade im Schadensfall einfach zugängliche Informationen.

4.2.10 Single Point of Contact

Besonders in den Gesprächen mit den britischen Experten wurde darauf hingewiesen, dass die Vielzahl der behördlichen Ansprechpartner besonders bei kleineren Unternehmen zu Unklarheiten darüber führt, wo in welcher Situation die Zuständigkeiten liegen. Ein einzelner Kontaktpunkt (Single Point of Contact) sei sehr erwünscht. Dieser kann je nach Anliegen an die entsprechenden Stellen weiterverweisen. In der Schweiz beispielsweise ist der NDB Hauptansprechpartner der Unternehmen. Er besitzt Entscheidungskompetenzen, Unternehmen nur bezüglich geeigneter Präventionsmaßnahmen zu beraten oder sie nach Absprache an Strafverfolgungsbehörden weiterzuvermitteln. Nach diesem Vorbild könnten staatliche Anlaufstellen einen neutralen und kompetenten Partner für KMU im Aufbau von Präventionsmaßnahmen wie auch bei der Handhabung von Vorfällen darstellen.

4.2.11 Erhöhung der Resilienz

Da besonders KMU oft wenig geschützt, aber immer häufiger Ziel von Angriffen sind, ist es laut dem Leiter der F&E-Abteilung eines österreichischen Industrieunternehmens umso wichtiger, das generelle Niveau an Informationssicherheit für diese Unternehmen zu erhöhen. Ziel muss es sein, den Aufwand eines Datendiebstahls so zu erhöhen, dass er den Nutzen der gewonnenen Informationen übersteige:

> Wenn viele Unternehmen Vorfälle melden und es eine flächendeckende Prävention gibt, dann ist die Messlatte für Kriminelle sehr hoch gelegt. Man muss es schaffen, dass der Aufwand des Datendiebstahls aufgrund der hohen Sicherheitsstandards nicht mehr lukrativ ist.

Wichtig ist folglich weniger die konkrete Ausgestaltung von Präventionsmaßnahmen und -angeboten als die reine Existenz von Schutzkonzepten. Eine erhöhte Resilienz und die Implementierung umfassender Informationssicherheitssysteme erschwert es den Tätern, auf unternehmensinternes Wissen zuzugreifen. Auch in Bulgarien wird ein ähnlicher Ansatz verfolgt. Mit der geplanten neuen Nationalen Strategie zur Cybersicherheit soll nicht nur das Bewusstsein für mögliche Angriffe auf Unternehmensinformationen geschärft werden, sondern auch Privatpersonen sollen für den Schutz ihrer Daten sensibilisiert werden.

In den Gesprächen mit den Experten der verschiedenen Länder hat sich gezeigt, dass sich Unternehmen und Behörden gleichermaßen mit den Phänomenen der Spionage und Ausspähung auseinandersetzen und momentan an ähnlichen Punkten arbeiten. Wirtschaftsspionage und Konkurrenzausspähung sind zwei sehr komplexe und sich ständig weiterentwickelnde Phänomene, die nicht durch einzelne konkrete Schutzmaßnahmen und Gesetze zu verhindern sind. Es wurde offenkundig, dass staatliche Angebote in der Lage sind, Unternehmen bei der Eindämmung von Angriffen zu unterstützen. Oft erfolgen sie aber zu spät und nicht mit der notwendigen Geschwindigkeit und Intensität, um den immer neuen Modi Operandi erfolgreich entgegenzuwirken. Es ist also ein System zu etablieren, das sich aus unterschiedlichen Angeboten und Maßnahmen zusammensetzt und kontinuierlich aktualisiert wird.

5. Diskussion der Ergebnisse und Vorschläge für eine erfolgreiche Umsetzung in Deutschland

Dieser Abschnitt befasst sich mit der Umsetzbarkeit der ermittelten Best Practices in Deutschland. Es werden deren Grenzen aufgezeigt und mögliche Schwierigkeiten bei der Implementierung dargelegt. Nach einigen allgemeinen Anmerkungen wird konkret auf die unterschiedlichen Maßnahmen eingegangen. Da der Aufwand der Umsetzung und die Bereitstellung hierfür benötigter Ressourcen als limitierende Faktoren die Implementierung stark beeinflussen, sind die Best Practices nach ihrer

zeitlichen Umsetzbarkeit angeordnet. Sie werden dementsprechend in kurzfristige (< 1 Jahr), mittelfristige (1–5 Jahre) und langfristige Maßnahmen (> 5 Jahre) unterteilt.

5.1 Allgemeine Anmerkungen

Die mithilfe der Experteninterviews identifizierten Best Practices sind nur partiell in Deutschland anwendbar. Ein generelles Hindernis stellen die unterschiedlichen Behördenstrukturen und die damit verbundenen Kompetenzen dar. Innerhalb staatlicher Stellen liegen Restriktionen vor, die bei der Entwicklung und Umsetzung neuer Präventionsangebote zu beachten sind. Zum einen gibt es bereits mehrere Behörden, die auf diesem Gebiet unterschiedliche, teils sich überschneidende Kompetenzen besitzen, zum anderen sind Stellen innerhalb der Behörden festgelegt und auch die sie besetzenden Personen sind kurzfristig nicht variabel und beliebig einsetzbar. Die Gründung einer komplett neuen Behörde ist denkbar, doch kurzfristig nicht zu realisieren; die Zuweisung genauer Kompetenzen in Absprache mit bestehenden Behörden spielt hier eine große Rolle. Auch die Bereitstellung von finanziellen Mitteln und Ressourcen stellt einen limitierenden Faktor bei der Umsetzung neuer Angebote dar.

Die ermittelten Best Practices können jedoch in abgeänderter Form einen großen Beitrag zur Sensibilisierung von KMU und einer gesteigerten Informationssicherheit leisten. Kurzfristig umsetzbar sind Awareness-Kampagnen zur Erhöhung der Resilienz, informelle Gesprächsrunden und die Herausgabe aktueller Reports und Warnmeldungen. Mittelfristig können Risikoanalysen durch staatliche Stellen, Gutscheinprogramme, ein Single Point of Contact, SOS-Notfallnummern, eine Online-Plattform und Public-Private-Partnership-Programme angeboten werden. Eine längere Planungs- und Realisierungsphase benötigen allerdings die Ausbildung weiterer Experten und die Definition neuer Cluster mit besonderem staatlichen Schutz, ähnlich den kritischen Infrastrukturen. Auch eine Veränderung des normativen Rahmens wäre nur langfristig zu vollziehen. Dennoch gibt es Restriktionen, die auch auf sehr lange Sicht nicht aufgehoben werden können, wie beispielsweise die föderalistisch aufgeteilte Sicherheitspolitik und die Organisation der Polizei.

5.2 Umsetzung kurzfristiger Maßnahmen

Die Implementierung von kurzfristig wirksamen Maßnahmen und Angeboten ist angesichts der Aktualität und Intensität der Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung bedeutend. Auch mit nur begrenzt zur Verfügung stehenden Ressourcen ist es möglich, den Zugang zu existierenden Angeboten zu erleichtern und auf eine zielgenaue Ansprache der unterschiedlichen Akteure zu achten, um so die Informationssicherheit zu erhöhen.

5.2.1 Erhöhung der Resilienz

Der Bundesverband der Deutschen Industrie e.V. (BDI) bemängelt in seinem Positionspapier, dass in Deutschland besonders bei KMU das Problem- und Gefährdungsbewusstsein sowie das Wissen um geeignete Präventionsmaßnahmen oft nicht oder nur in Ansätzen vorhanden sind.[19] Dies ist allerdings kein deutsches Phänomen, wie die Gespräche mit den internationalen Experten gezeigt haben. Auch in anderen Ländern ist eine fehlende Resilienz festzustellen. Deren Erhöhung ist allerdings sehr zeitintensiv und kann kurzfristig nur schwer erreicht werden. Dennoch ist es unerlässlich, auch in Deutschland bereits jetzt bestehende Informationsveranstaltungen und -kanäle auszubauen, um kontinuierlich das Niveau an Informationssicherheit zu erhöhen. Gleichzeitig wird der Aufwand des Datendiebstahls erschwert, bis er schließlich den Nutzen für die Angreifer übersteigt. Die Initiative Wirtschaftsschutz startete beispielsweise im Jahr 2016 die „Roadshow Wirtschaftsschutz“ in Potsdam – eine Awareness-Kampagne für die Zielgruppen KMU und innovative Startup-Unternehmen. Die Ausweitung dieses Programms auf weitere Zielorte ist ein möglicher Ansatz, um die Resilienz zu erhöhen. Ebenso kann die Zugänglichkeit von Informationen über die Roadshow ausgebaut werden. Bislang ist es bei der Recherche im Internet sehr mühsam, an genauere Informationen zu dieser Initiative zu gelangen. Ein eigener Internetauftritt mit Auskünften über deren nächste Stationen, Ziele und Inhalte könnte hier Abhilfe schaffen. Auch die Bereitstellung von detaillierteren Informationen zu den Regionalveranstaltungen für die breite Öffentlichkeit anstatt nur im Nutzerbereich, für den eine Registrierung notwendig ist, würde die Bekanntheit der Initiative erhöhen.

5.2.2 Multiplikatoren

Die zielgerichtete Ansprache von KMU muss nicht zwingend direkt durch staatliche Stellen erfolgen. Durch die Arbeit mit Multiplikatoren können Behörden ressourcenschonend arbeiten und dennoch flächendeckend über Präventionsangebote aufklären. In der heutigen Zeit spielen beispielsweise Verbände eine wichtige Rolle bei der Bündelung von Interessen und der Selbststeuerung der Gesellschaft. Sie kennen die Bedürfnisse ihrer Mitgliedsunternehmen sowie die Anforderungen, die in Bezug auf Informationssicherheit in der jeweiligen Branche gestellt werden, genau. In Deutschland wäre es möglich, dass Behörden generelle Standards vorschlagen und Informationen bereitstellen, die Verbände und Branchen dann für die Mitgliedsunternehmen anpassen und großflächig, aber zielgerichtet weitergeben. Auf diese Weise wäre gewährleistet, dass KMU gezielt über Gefahren aufgeklärt werden, staatliche Stellen aber nicht in direkten Kontakt mit jedem einzelnen Unternehmen treten müssten. Der Verband Deutscher Maschinen- und Anlagenbau e.V. zum Bei-

---

19 Vgl. BDI 2012, S. 6.

spiel ist mit rund 3.100 vorwiegend mittelständischen Mitgliedern der größte Industrieverband in Europa und stellt somit ein ideales Sprachrohr für staatliche Stellen dar. Durch die Festlegung der Informationssicherheit als eines seiner Kernthemen und damit verbundenen Veröffentlichungen mit leicht zugänglichen und gezielt ausgerichteten Informationen kann er helfen, den Schutz der Unternehmen zu erhöhen. In der Schweiz hat die Pharmabranche einen großen Einfluss auf ihre Mitglieder und, unter anderem im Bereich der Absicherung von Know-how, einige spezifische Branchenregularien verabschiedet. Einer der Gesprächspartner merkt an:

> Der Branchenverbund ist sehr stark, sodass eine Zusammenarbeit mit Staatsorganen nicht fokussiert wird. Der Austausch über Vorfälle ist nur dann von Interesse, wenn ein beidseitiger Nutzen entsteht.

Auf diese Weise finden branchenspezifische Bedürfnisse Berücksichtigung, staatliche Angebote werden jedoch in den Hintergrund gedrängt. Eine funktionierende Kooperation staatlicher Stellen mit Fachverbänden könnte dem entgegenwirken.

5.2.3 Zielgruppenspezifische Ansprache der Unternehmen/ leichter Zugang zu Angeboten

In den untersuchten Ländern wie auch in Deutschland haben in den letzten Jahren zahlreiche staatliche Institutionen Präventionsangebote bereitgestellt. In Deutschland ist die Arbeit der CERT-Stelle ebenso hervorzuheben wie die des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der Allianz für Cybersicherheit und der Initiative Wirtschaftsschutz. Die Gespräche mit KMU in Deutschland haben allerdings bestätigt, dass viele Unternehmen dieser Gruppe nur geringe Ressourcen aufwenden können oder wollen, um das eigene Know-how zu schützen. Sie begründen dies zum Teil damit, dass Dritte keine Verwendung für ihre Daten hätten und nehmen praktizierte Informationssicherheit nicht als Wettbewerbsvorteil wahr. Es ist folglich umso wichtiger, dass staatliche Stellen diesen Unternehmen das Gefahrenpotenzial aufzeigen und über Risiken informieren. Staatliche Angebote sollten von den Behörden aktiv an Unternehmen und KMU im Speziellen herangetragen werden. An dieser Stelle spielt der genutzte Kanal der Ansprache eine wesentliche Rolle, um Zugang zu den Unternehmen zu erhalten. Mit einer zielgerichteten Kontaktaufnahme über Verbände sind traditionell ausgerichtete KMU zu erreichen; die Nutzung von neuen Medien und Onlinekanälen hilft hingegen, junge und innovative Startups zu sensibilisieren. Je nach Kenntnisstand zu Wirtschaftsspionage und Konkurrenzausspähung sollten die Angebote eher allgemeine Informationen erhalten oder sehr detailliert auf spezielle Fragestellungen eingehen. Es besteht die Möglichkeit, Warnungen und Reports in zwei unterschiedlichen „Tiefenstufen“ zu veröffentlichen: eine allgemeiner gehaltene Meldung für Mitarbeiter und Geschäftsführer von KMU, die auf dem Gebiet der Informationssicherheit nicht umfassend ausgebildet sind, sowie eine detailliertere Version für Experten der Fachabteilungen.

5.2.4 Herausgabe aktueller Warnmeldungen

Das deutsche CERT gibt bereits jetzt täglich mehrere Warnmeldungen zu Schwachstellen und Sicherheitslücken in Software bekannt. Zur Optimierung aktueller Warnmeldungen könnten zusätzliche Reports mit Informationen zu häufig betroffenen Branchen, physischen Angriffen oder neuen Vorgehensweisen der Täter angeboten werden. In der Summe werden diese Warnungen jedoch von KMU kaum wahrgenommen, da diese die Masse an ungefilterten Warnungen nicht verarbeiten können. Positiv zu werten ist der Warn- und Informationsdienst des CERT dahingehend, dass er auf die eigenen Bedürfnisse personalisierbare Meldungen per E-Mail verschickt. Die Kurzinformationen zu den gefundenen Schwachstellen sind ferner öffentlich auf der Homepage des CERT zugänglich und klären über Sicherheitslücken in Software und deren Auswirkungen auf.[20] Diese Kurzmeldungen sind für Unternehmen wie Bürger gleichermaßen zugänglich. Eine Ausweitung der Zielgruppe für die Bereitstellung von ausführlichen Informationen und Gegenmaßnahmen von Bundesbehörden auf alle Unternehmen in Deutschland würde die Reichweite dieser Informationen zusätzlich erhöhen.

5.2.5 Melde- und Analysestelle für aktuelle Vorfälle

Anders als z.B. in der Schweiz[21], gibt es bislang in Deutschland keine zentrale Anlaufstelle, bei der angegriffene Unternehmen einen Vorfall melden können und eine fallorientierte Rückmeldung erhalten. Realisiert wurde eine solche Funktion jedoch von der Initiative Wirtschaftsschutz, die allerdings (noch) keinem der befragten Experten aus der Industrie bekannt war. Auf der Homepage der Allianz für Cybersicherheit des BSI gibt es ein Meldeformular, doch ist dort keine Rückmeldung an die betroffenen Unternehmen vorgesehen.[22] Die Angliederung einer Meldestelle an eine deutsche Behörde erweist sich aufgrund der unterschiedlichen Zuständigkeiten je nach Art des Angriffs als schwierig. Es ist aber denkbar, dass eine solche Meldestelle ähnlich wie MELANI in der Schweiz an die zuständigen Behörden weiterverweist. Die Integrierung einer Meldestelle für Angriffe in ein allgemeines Informationsportal vereinfacht für KMU den Umgang mit Spionage und Ausspähung, da sich die Anzahl der zu nutzenden Kontaktpunkte reduziert. Es ist dabei besonders auf die Erreichbarkeit des Personals zu achten, die nicht auf die Bürozeiten beschränkt, sondern rund um die Uhr gewährleistet sein sollte. Die Auswertung von gemeldeten Fällen und eine sich daran anschließende mögliche Clusterbildung von Gefahrenpotenzialen könnte im gleichen Portal an die Unternehmen zurückgespiegelt werden. Ein weiteres vorherrschendes Problem liegt zum einen in der fehlenden Anzeigebe-

---

20 Vgl. www.cert-bund.de/overview/AdvisoryShort [15.09.2017].

21 Siehe *Abschnitt 4.2.8.*

22 Vgl. www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/Online_Meldung/onlinemeldung.html [15.09.2017].

reitschaft der Unternehmen, zum anderen bei den fehlenden Ressourcen innerhalb der Behörden. Nur wenn Unternehmen die Bedrohung realisieren, Angriffe erkennen und bei Behörden melden, können Analysen der Bedrohung durchgeführt, konkrete und gezielte Maßnahmen ergriffen und neue Angebote bereitgestellt werden.

5.2.6 Informelle Gesprächsrunden

International haben sich informelle Gesprächsrunden als sehr nützliche und vertrauenswürdige Informationsquellen zu tagesaktuellen Geschehnissen etabliert. Die Gespräche mit deutschen KMU haben gezeigt, dass solche informellen Netzwerke hierzulande nicht in gleichem Maße aufgebaut sind. Zwar findet häufig ein Austausch unter befreundeten Unternehmen statt, allerdings nicht branchenübergreifend oder in einem geregelten Umfeld. Der Aufbau solcher informellen Netzwerke ist für staatliche Stellen nur mit sehr viel Vorlauf und persönlichem Engagement umsetzbar, da das benötigte Vertrauen nicht erzwungen werden kann, sondern kontinuierlich wachsen muss. Dennoch besteht die Möglichkeit, auf Informationsveranstaltungen Unternehmern verschiedener Branchen und Firmen die Möglichkeit des Netzwerkens zu geben und hierzu anzuregen. Außerdem können sich einzelne Mitarbeiter von Behörden ganz bewusst in bestehende Netzwerke einbringen und Informationen über aktuelle Bedrohungen und Präventionsmaßnahmen weitergeben. Da Unternehmer häufig in mehreren Netzwerken aktiv sind, könnten sich Warnungen und Bekanntgaben auf diesem Wege multiplikativ weiterverbreiten.

5.3 Umsetzung mittelfristiger Maßnahmen

In einem mittelfristigen Zeithorizont von einem bis fünf Jahren sind ressourcenintensivere Präventionsangebote von staatlichen Stellen umsetzbar. Um die hierfür benötigten finanziellen Mittel freizugeben, sind die Haushaltspläne von Bund und Ländern anzupassen. Taktische Ansätze können überarbeitet werden und umfassen unter anderem Risikoanalysen, die Nutzung von IT-gestützten Systemen, aber auch die generelle Herangehensweise an die operative Umsetzung einzelner Angebote im Rahmen von PPP-Programmen und Multi-Stakeholder-Ansätzen.

5.3.1 Risikoanalysen durch staatliche Stellen

Staatliche Risiko-Assessments nach dänischem Vorbild sind aufgrund des enormen finanziellen Aufwandes und der Anzahl der benötigen Fachkräfte für die Durchführung mit deutschen KMU kaum möglich. Der Ausbau eines IT-gestützten Assessments, wie es bereits in Großbritannien im Rahmen der Cyber Essentials genutzt wird, ist eher umsetzbar. Im Rahmen einer Selbstbewertung könnten KMU so selbst überprüfen, wie gut ihr Informationssicherheitsmanagementsystem (ISMS) aufgebaut ist. Vorstellbar ist eine Eingabemaske oder ein Fragebogen, der ähnlich dem Bewertungsbogen eines normalen Audits verschiedene Aspekte der Informations-

sicherheit erfragt. Anhand vorher festgelegter Parameter würde nach abgeschlossener Eingabe der Informationen zum Schutzkonzept des Unternehmens die Güte der getroffenen Präventionsmaßnahmen errechnet. Als definierte Standards gelten bei den Cyber Essentials die Richtlinien der ISO-27000-Reihe. Da diese auch in Deutschland eine große Akzeptanz erfahren, stellen sie auch hier eine gute Basis für die Bewertung der Informationssicherheitssysteme von KMU dar. Das automatisch generierte Feedback könnte je nach Ergebnis der Analyse individuell angepasste Informationsmaterialien zu den Bereichen bereitstellen, die noch nicht ausreichend geschützt sind. Auch das Ausstellen eines Zertifikats über die Qualität des ISMS wäre sinnvoll. Ebenso ist es denkbar, dass die Nutzer des Tools im Rahmen eines Benchmarkings einsehen, wie gut sie im Vergleich zu Wettbewerbern oder Unternehmen anderer Branchen geschützt sind. Obliege die Betreuung dieses online verfügbaren Analysetools einer Behörde, würde sie anhand der Auswertung der eingegebenen Daten einen besseren Überblick über das nationale Niveau der Informationssicherheit erlangen und könnte weitere Angebote daran ausrichten. Die Anpassung des Tools an neue Bedrohungslagen ist wichtig, um zu gewährleisten, dass KMU auch auf neue Modi Operandi eingehen können.

5.3.2 Gutscheinprogramme

In Deutschland stehen staatlichen Stellen weder unbegrenzte Ressourcen noch entsprechendes Know-how zur Verfügung, um jedes einzelne Unternehmen durch Präventionsmaßnahmen zu schützen. Mithilfe eines Gutscheinprogramms, ähnlich dem in Großbritannien umgesetzten, könnten Anreize für KMU geschaffen werden, sich stärker vor illegalem Informationsabfluss zu schützen. Denkbar ist ein Modell, bei dem staatliche Stellen Gutscheine für Präventionsmaßnahmen ausstellen, die KMU bei privaten Dienstleistern einsetzen können. Es ist ebenfalls denkbar, dass KMU die Kosten oder einen Teil davon für die Ausweitung des ISMS zurückerstattet bekommen. Mittels Audits könnte die Qualität der umgesetzten Maßnahmen anhand eines Kriterienkatalogs überprüft und die Höhe der erstattungsfähigen Kosten ermittelt werden. Auf diese Weise käme der Staat seiner Aufgabe nach, für den Schutz der Wirtschaft zu sorgen, ohne dabei die eigene Expertise ausbauen zu müssen und ohne direkt in das wirtschaftliche Geschehen einzugreifen. Die Unternehmen würden ihre geschäftliche Autonomie wahren, deren Wichtigkeit sowohl in den internationalen als auch den deutschen Gesprächen immer wieder betont wurde, und könnten auf Dienstleister oder eigenes Know-how zurückgreifen.

5.3.3 Online-Plattform

In Deutschland besteht bislang kein Internetportal, das umfassend über verschiedene Aspekte der Wirtschaftsspionage und Konkurrenzausspähung und die davon bedrohte Informationssicherheit aufklärt und eine Möglichkeit des Austausches bietet. Erste Ansätze dazu sind im Rahmen der von der Initiative Wirtschaftsschutz

eingerichteten Plattform sichtbar, jedoch werden derzeit weder jene selbst noch die Inhalte von den Industrieexperten als Mehrwert wahrgenommen. Informelle Gesprächsrunden hingegen helfen Unternehmen, aus einem kleinen vertrauten Kreis Informationen zu beziehen. Werden allerdings generellere Informationen zu neuen Trends oder Modi Operandi gesucht, gestaltet sich die Informationsgewinnung aufgrund der zahlreichen unterschiedlichen Quellen als äußerst aufwendig. Die Bündelung auf einer Online-Plattform, wie der bereits erwähnten CiSP in Großbritannien, würde KMU helfen, schnell an qualitativ hochwertige Informationen zu gelangen und sich mit anderen Nutzern darüber auszutauschen. Bei einer Implementierung in Deutschland bestünde die Möglichkeit, eine solche Plattform durch zusätzliche Funktionen zu erweitern. Neben themenspezifischen Diskussionsforen und einem Downloadbereich für aktuelle Reports wäre eine Chatfunktion oder eine ähnliche Option der Kontaktaufnahme mit anderen Nutzern oder den Behörden sinnvoll. Ebenso ist die Integration einer Meldestelle, an die sich angegriffene Unternehmen wenden können, erwägenswert. In Großbritannien obliegt die Pflege der Plattform dem CERT. In Deutschland könnte eine solche Plattform von unterschiedlichen staatlichen Ämtern betreut werden. Auch ist denkbar, dass eine Behörde zwar die Zuständigkeit übernimmt, das operative Management, das Know-how für Reports sowie aktuelle Meldungen allerdings aus der Privatwirtschaft zukauft und so bereits existierende Expertise nutzt, anstatt eigene Kompetenzen ressourcenintensiv auszubauen.

5.3.4 Public-Private-Partnership-Programme

Auch in Deutschland sind erste Projekte als PPP umgesetzt. Das präsenteste Beispiel im Kontext der Informationssicherheit ist die Initiative Wirtschaftsschutz, die die gemeinsamen Aktivitäten von Staat und Wirtschaft zur Abwehr von Wirtschaftsspionage in Form einer von vier Behörden gemeinsam betriebenen Plattform bündelt. Der ehemalige Präsident des Bundesamtes für Verfassungsschutz (BfV), Dr. *Hans-Georg Maaßen*, erklärte dazu, dass ein Zusammenwirken von Staat und Wirtschaft unverzichtbar sei, um das gemeinsame Ziel eines höheren Schutzniveaus für die deutsche Wirtschaft zu erreichen.[23] Weitere Projekte zur Erhöhung der Informationssicherheit sollten daher mit allen Stakeholdern abgestimmt sein, um effektiv wirkende Maßnahmen entwickeln und umsetzen zu können. Zu ähnlichen Erkenntnissen gelangt auch einer der befragten Experten aus Deutschland. Er betont besonders die Wichtigkeit, alle Beteiligten, also auch KMU, in den Austausch von Staat und Wirtschaft mit einzuschließen:

> Ein vertraulicher Austausch zwischen Staat und Wirtschaft ist wichtig. Besonders der Kontakt zu großen und gut vernetzten Unternehmen. Das Teilen von Wissen über

[23] BfV 2016, o.S.

das öffentliche Wissen hinaus sollte stärker fokussiert werden. Dabei dürfen KMU allerdings nicht vernachlässigt werden, sondern müssen ebenfalls einbezogen werden.

5.3.5 Single Point of Contact

Die Gespräche mit deutschen KMU haben bestätigt, dass Unternehmen oft nicht wissen, welche staatlichen Akteure sie in Bezug auf Präventionsmaßnahmen oder im Falle eines Angriffs ansprechen können. Ein Single Point of Contact könnte die Unzufriedenheit über den hohen bürokratischen und zeitlichen Aufwand in der Zusammenarbeit mit Behörden minimieren. Zusätzlich könnten die undurchsichtigen Zuständigkeiten strukturiert und vor allem aus Sicht von KMU der Einsatz von Ressourcen minimiert werden. Ergänzend hierzu ist eine SOS-Notfallnummer, vergleichbar der allgemeinen Behördennummer oder dem Notruf 110, vorstellbar. Konkrete behördliche Ansprechpartner sind unter anderem auf der Internetseite der Initiative Wirtschaftsschutz veröffentlicht, doch handelt es sich nicht um einen Ansprechpartner, sondern um mehr als 20 verschiedene Telefonnummern. Neben einer Telefonnummer ist auch eine Chatfunktion denkbar, um erste Anregungen zu erhalten, welche Gegenmaßnahmen nach einem Angriff einzuleiten sind. Anfragen über solch einen Chat könnten entweder durch Mitarbeiter staatlicher Stellen oder automatisch per Software beantwortet werden. Eine derartige Chatfunktion ließe sich auch kurzfristig in bereits bestehende Websites von Behörden integrieren. *Schaaf* merkt jedoch an, dass Unternehmen eher einen privaten Sicherheitsdienstleister einschalten würden, als den Vorfall bei Behörden zu melden.[24] Daher wäre vermutlich ein 'neutraler' Ansprechpartner vorzuziehen, bei dem die Geschädigten ersten Rat suchen und dann selbst entscheiden, ob sie sich für weitere Untersuchungen an Strafverfolgungsbehörden wenden möchten oder nicht. Die Vermittlung an die entsprechende zuständige Stelle wäre eine der möglichen Aufgaben des Single Point of Contact. Die Kompetenzen des NDB der Schweiz können hier als Vorbild dienen. Den Unternehmen in Deutschland dienen momentan unterschiedliche Behörden als Ansprechpartner in Bezug auf Wirtschaftsspionage und Konkurrenzausspähung. Zurzeit gibt es keinen Single Point of Contact, weder im Allgemeinen noch im Speziellen für KMU, wie es beispielsweise der BDI in seinem Positionspapier fordert.[25] Für Unternehmen ist die Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung sowie die Zuständigkeit für präventive und repressive Maßnahmen wenig relevant oder schlicht unbekannt.[26] Die Zuständigkeiten der LKA, des BKA, des BfV und des BSI sind zwar klar definiert, doch den Unternehmen in der Regel nicht bekannt.[27] Entscheidend für die Behörden ist hingegen das

---

24 Vgl. *Schaaf* 2009, S. 24–25.

25 Vgl. BDI 2012, S. 7.

26 Vgl. *Carl, Kilchling, Knickmeier & Wallwaey* 2017, S. 116.

27 Vgl. *Carl, Kilchling, Knickmeier & Wallwaey* 2017, S. 134.

Legalitätsprinzip, das die LKA, das BKA und die Polizei verpflichtet, Ermittlungen einzuleiten, sobald der Verdacht einer Straftat besteht. Da viele Unternehmen Reputationsverluste fürchten, treten sie nicht mit diesen Behörden in Kontakt, denn ein einzuleitendes Strafverfahren könnte zu einer Veröffentlichung führen.[28]

5.4 Umsetzung langfristiger Maßnahmen

Es ist anzunehmen, dass sich die Gefährdung von KMU in Deutschland durch Wirtschaftsspionage und Konkurrenzausspähung auch in den nächsten Jahren nicht verringert, sodass die Entwicklung von strategischen Maßnahmen zum Schutz dieser Unternehmen an Bedeutung gewinnt.

5.4.1 Verfügbarkeit hochqualifizierter Experten

In Dänemark dienen die lokalen Polizeidienststellen immer als erster Ansprechpartner bei einem Angriff auf das Know-how eines Unternehmens. Fehlt in der jeweiligen Dienststelle fachliche Expertise, kann diese sogenannte ICT-Engineers des National Cyber Crime Centers anfordern. Eine solche Zuordnung von Fachkräften zu den Polizeibehörden wäre auch in Deutschland möglich. Die Experten sind zwar über ganz Deutschland verteilt angesiedelt, könnten aber den Ländern zugeordnet und dann entsprechend in kommunale Dienststellen entsandt werden. Hierbei würde der Abstimmungsbedarf durch die föderalistischen Verwaltungskompetenzen auf dem Gebiet der Sicherheitspolitik umgangen. Die Ausbildung von Fachkräften benötigt allerdings neue Studiengänge und Weiterbildungsmöglichkeiten, die flexibel angelegt sind und sich in der gleichen Geschwindigkeit weiterentwickeln lassen, wie sich die Erscheinungsformen des illegalen Know-how-Abflusses ändern.

5.4.2 Übertragung von Maßnahmen aus dem Bereich der kritischen Infrastrukturen

Bereits existierende Präventionsangebote könnten teilweise ressourcenschonend und kurzfristig ausgebaut werden, um so ihre Effektivität in der Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung zu erhöhen. Um KMU bessere Angebote der Prävention unterbreiten zu können, müssen also nicht zwingend neue Maßnahmen eingeführt werden. Es gibt in Deutschland für Betreiber kritischer Infrastrukturen bereits besondere Angebote, die auch auf KMU ausgeweitet werden könnten. Eine flächendeckende Anwendung solcher Maßnahmen auf die große Gruppe der KMU erscheint jedoch aufgrund der immensen Finanzierungskosten nur schwer umsetzbar. Außerdem bedarf nicht jedes Unternehmen aus der Gruppe der KMU staatlicher Unterstützung bei der Implementierung von Präventionsmaßnahmen, da nicht alle innovativ tätig und somit direkt durch Spionage oder Ausspähung

---

28 Vgl. *Kasper* 2014, S. 80; *Schaaf* 2009, S. 23 f.

bedroht sind. Durch eine Ausweitung der Gruppe der kritischen Infrastrukturen nach bulgarischem Vorbild könnte die Zahl der geschützten Unternehmen angehoben werden. Alternativ besteht die Möglichkeit, neue Cluster einführen, anstatt die Liste der Betreiber kritischer Infrastrukturen auszuweiten. KMU werden auch als das „Rückgrat der Gesellschaft" bezeichnet, da sie viele Arbeitsplätze schaffen und für die Innovationskraft des Landes mitverantwortlich sind. Durch diese Eigenschaften qualifizieren sie sich als besonders schützenswert. Wie bereits erwähnt, stehen staatlichen Stellen jedoch keine unbegrenzten Ressourcen zur Verfügung, sodass nicht jedes einzelne Unternehmen durch staatliche Präventionsangebote geschützt werden kann. Es ist also notwendig, innerhalb der Gruppe der KMU zu entscheiden, welche Unternehmen von staatlichen Angeboten profitieren können. Eine Möglichkeit zur Definition eines neuen Clusters ist die Gruppe der sogenannten *Hidden Champions*.[29] Ergänzend hierzu könnten festgelegte Umsatz- oder Mitarbeiterzahlen Richtlinien zur Selektion von KMU sein, die ähnlich den Betreibern kritischer Infrastrukturen besondere staatliche Präventionsangebote bereitgestellt bekommen.

6. Fazit

International wie national hat sich gezeigt, dass kein ganzheitlicher Schutz vor Wirtschaftsspionage und Konkurrenzausspähung gewährleistet werden kann. Jedes staatliche Angebot setzt an einer anderen Stelle an und kann Angriffe nicht komplett ausschließen und bekämpfen. Dennoch leistet jedes einzelne Angebot einen Beitrag zur generellen Abwehr und Resilienz. Auch ist es nicht möglich, die im Ausland identifizierten Modelle unverändert auf Deutschland zu übertragen. Dennoch können sie dort, an lokale Verhältnisse angepasst, einen Beitrag zum Schutz von KMU vor Wirtschaftsspionage und Konkurrenzausspähung leisten. Wichtig ist, dass sowohl die einzelnen Behörden untereinander, aber auch mit Unternehmen und besonders KMU gemeinsam, neue Möglichkeiten entwickeln, um das Know-how und die sensiblen Daten der Wirtschaft zu schützen.

Literatur

BDI, siehe Bundesverband der Deutschen Industrie e.V.

BfV, siehe Bundesamt für Verfassungsschutz.

Birkner, D.G. (2014): Kriminelle Risiken im Mittelstand. Gefahren, Schäden und Prävention – eine Studie. Result Group GmbH Global Risk and Crisis Management & F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH (Hrsg.), Seeshaupt; www.result-group.com/downloads/ResultGroup_KriminelleRisikenMittelstand-201.pdf [15.09.2017].

---

29 Als Hidden Champion wird ein Unternehmen des Mittelstandes bezeichnet, das in seinem Nischenmarkt Europa- oder Weltmarktführer geworden ist. Ein solcher „heimlicher Gewinner" ist trotz seines Erfolgs oft medial und in der Öffentlichkeit kaum präsent. Ausführlich hierzu siehe z.B. *Simon* 2007.

BITKOM, siehe Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Bogner, A., Littig, B. & Menz, W. (2014): Interviews mit Experten: Eine praxisorientierte Einführung. Wiesbaden.

Bundesamt für Verfassungsschutz (2016): Roadshow Wirtschaftsschutz in Brandenburg. Pressemitteilung vom 05.09.2016. Köln; www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/presse/pm-20160905-roadshow-wirtschaftsschutz-in-brandenburg [15.09.2017]; zit: BfV 2016.

Bundesverband der Deutschen Industrie e.V. (2012): Wirtschaftsschutz in der deutschen Industrie stärken; Positionspapier. Berlin; https://bdi.eu/media/presse/publikationen/marketing/Positionspapier_online_2_.pdf [15.09.2017]; zit.: BDI 2012.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter: Studienbericht. Berlin; www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf [15.09.2017]; zit.: BITKOM 2015.

Carl, S., Kilchling, M., Knickmeier, S. & Wallwaey, E. (2017): Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa. Eine rechtsvergleichende Betrachtung. Bd. 49 der Reihe forschung aktuell/research in brief des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Freiburg i.Br.

Corporate Trust (2014): Studie Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co. München; www.corporate-trust.de/wp-content/uploads/ 2016/06/ CT-Studie-2014_DE.pdf 15.09.2017].

Destatis, siehe Statistisches Bundesamt.

Graf, G. & Otte, T. (2011): Wirtschaftsspionage: Strafverfolgung und Polizeiarbeit; Vortrag im Rahmen des 14. Europäischer Polizeikongresses. Berlin.

Kasper, K. (2014): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes, Ergebnisbericht einer Sekundäranalyse. Wiesbaden.

Kilchling, M. & Carl, S. (2016): Wirtschaftsspionage im globalen Markt: Sind die Ermittlungsstrukturen in Deutschland noch zeitgemäß?, in: P. Zoche, S. Kaufmann & H. Arnold (Hrsg.), Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung. Berlin, S. 183–196.

MELANI, siehe Melde- und Analysestelle Informationssicherung.

Melde- und Analysestelle Informationssicherung (2012): Meldeformular: Verwendung und Zweck; www.melani.admin.ch/melani/de/home/meldeformular/verwendung.html [15. 09.2017]; zit.: MELANI 2012.

Schaaf, C. (2009): Industriespionage. Der große Angriff auf den Mittelstand. Stuttgart.

Simon, H. (2007): Hidden Champions des 21. Jahrhunderts. Die Erfolgsstrategien unbekannter Weltmarktführer. Frankfurt a.M.

Statistisches Bundesamt (2013): Unternehmen, tätige Personen, Umsatz, Investitionen und Bruttowertschöpfung nach Unternehmensgröße und Wirtschaftsbereichen im Zeitverlauf; www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/_inhalt.html#sprg233752.

Statistisches Bundesamt (2008): Klassifikation der Wirtschaftszweige. Mit Erläuterungen; www.destatis.de/DE/Publikationen/Verzeichnis/KlassifikationWZ08_3100100089004.pdf?__blob=publicationFile [15.09.2017]; zit.: Destatis 2008.

Gemeinsam gegen Wirtschaftsspionage und Konkurrenzausspähung

Erfolgsfaktoren für die Kooperation zwischen Staat und Wirtschaft

Fabian Fischbach & Esther Bollhöfer

1. Einleitung

Das Weltwirtschaftsforum bewertet in seinem jährlich erscheinenden Risikobericht 2017 Datendiebstahl als das wahrscheinlichste technologische Risiko mit Platz 5 aller Risiken. Dies ist die höchste Platzierung für dieses Delikt seit dem zehnjährigen Bestehen des Rankings. Auch die Bundesregierung hat die Bedeutung von Datendiebstahl und Wirtschaftsspionage erkannt und verpflichtete sich im Koalitionsvertrag zur 18. Legislaturperiode zum Handeln: „Wir wollen unsere Unternehmen vor Wirtschafts- und Konkurrenzspionage aus aller Welt schützen und eine nationale Strategie für den Wirtschaftsschutz erarbeiten.“[1] Dieser Aufsatz soll dazu beitragen, indem er die Erfolgsfaktoren für Kooperationen zwischen Staat und Wirtschaft bei Wirtschaftsspionage und Konkurrenzausspähung analysiert und aufzeigt.

2. Kooperation in Deutschland

Wenn es um die Kooperation zwischen kleinen und mittelständischen Unternehmen (KMU) und Sicherheitsbehörden im Kontext von Wirtschafts- und Industriespionage in Deutschland geht, ist die Literaturgrundlage, wie eingangs erläutert,[2] sehr dünn. Untersuchungen und Publikationen, die sich speziell mit der Kooperation von KMU, öffentlichen und halb-öffentlichen Institutionen in diesem Themenfeld beschäftigen, sind den Autoren nicht bekannt. Jedoch werden entsprechende Fragestellungen immer wieder als Teilaspekte in verschiedenen Studien aufgegriffen,[3] sodass es wichtig erscheint, sich damit auseinanderzusetzen. Grundsätzlich kann festgestellt werden, dass Unternehmen, die sich dafür entscheiden, auf externe Unterstützung zurückzugreifen, private Dienstleister

---

1 Bundesregierung 2013, S. 145.

2 Vgl. Beitrag von *Wallwaey & Waldheim* im vorliegenden Band.

3 Vgl. *Kasper* 2014, S. 13–14.

den staatlichen Stellen vorziehen. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) zeigt in einer im Jahr 2016 durchgeführten repräsentativen Studie auf, dass sich von 349 befragten Industrieunternehmen, die in den letzten zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage geworden sind, nur jedes vierte dafür entschieden hat, den Kontakt mit staatlichen Stellen zu suchen.[4] Als Begründung dominiert die Angst vor Imageschäden (38 %), die Befürchtung von negativen Konsequenzen (36 %), sowie von Eingriffen in das Tagegeschäft im Zuge der Sicherung von Beweismitteln und dass der Aufwand für die Einschaltung staatlicher Stellen zu hoch sei (32 %). Eine im Jahr 2014 vom Beratungsunternehmen Corporate Trust durchgeführte Studie mit 412 Teilnehmern kam sogar zu dem Ergebnis, dass nur in 9,8 Prozent der Fälle staatliche Stellen beteiligt wurden.[5] *Kasper* zieht in seiner Sekundäranalyse, für die er 27 deutschsprachige empirische Studien zum Thema Wirtschaftsspionage und Konkurrenzausspähung auswertete, das Fazit:

> In keiner Studie gab mehr als ein Drittel der befragten Unternehmen an, sich im Verdachts- oder Schadensfall an die Sicherheitsbehörden zu wenden. In den meisten Studien war dieser Anteil sogar deutlich niedriger.[6]

Neben den bereits dargestellten Gründen für die geringe Meldebereitschaft identifiziert *Kasper* erstmals explizit das fehlende Wissen der Unternehmen über behördliche Ansprechpartner, deren Zuständigkeiten und Angebote als weiteren Faktor.

Die aktuelle Literatur erlaubt es zwar, ein grundsätzliches Bild zum Kooperationsverhalten von Unternehmen und Behörden in Deutschland zu zeichnen, verdeutlicht aber auch den existierenden Forschungsbedarf: Eine Vielzahl der bisherigen Studien genügt nur begrenzt wissenschaftlichen Standards, da deren Vorgehen und Methodik nicht nachvollziehbar und vollständig dargestellt sind.[7] Ein Teil der Studien bezieht sich auf unternehmerische Entscheidungen im Kontext von Wirtschaftskriminalität, was nicht nur Wirtschafts- und Industriespionage umfasst, sondern auch eine Vielzahl weiterer Delikte mit einschließt. Die Kooperationsbereitschaft variiert jedoch teilweise signifikant in Abhängigkeit von der Art des Delikts.[8] Wenn Daten zur Kooperation von privaten und staatlichen Akteuren erhoben werden, beziehen sich diese fast ausschließlich auf das Verhalten im Zusammenhang mit einem Vorfall. Da das Ziel einer effektiven Prävention sein sollte, Kooperationen früher und mit einer größeren Bandbreite anzubahnen, ist es wichtig, das Forschungsfeld neutral und ohne mögliche Interessenskonflikte anzugehen. Das ist bei privaten Unternehmen oder Netzwerken (wie z.B. Unternehmensberatun-

---

4 Vgl. *Kopke, Petri, Kob, Sopha, Holz, Seyerlein-Klug, Schulz, Geschonneck, Kröger & Münstermann* 2016, S. 33.

5 Vgl. Corporate Trust 2014, S. 34–35.

6 *Kasper* 2014, S. 77.

7 Vgl. *Kasper* 2014, S. 15–16.

8 Vgl. *Ziegleder* 2010, S. 156–157; *Hedayati & Bruhn* 2015, S. 19–20.

gen oder Herstellern von Computersicherheitssoftware) möglicherweise nicht immer der Fall. Des Weiteren mangelt es der aktuellen Forschung an qualitativen Aussagen zu Kooperation, da das Feld bislang durch quantitative Erhebungen dominiert wird. Um kooperieren zu können, benötigt es mindestens zwei Akteure. Bei der großen Mehrheit der Studien handelt es sich um reine Unternehmensbefragungen, die die Rolle und die Perspektive der Kooperationspartner, zum Beispiel der Strafverfolgungsbehörden oder Nachrichtendienste, nicht berücksichtigen.

Im Hinblick auf den beschriebenen Forschungsstand soll in diesem Beitrag mithilfe eines qualitativen Ansatzes folgende Fragestellung untersucht werden:

> Welche Faktoren hemmen, ermöglichen und fördern die Zusammenarbeit von Behörden, Unternehmen und Verbänden im Kampf gegen Wirtschafts- und Industriespionage?

Die Forschungsfrage soll in folgenden Schritten beantwortet werden: Aufbauend auf den bereits dargestellten Einblicken in die Literatur werden Erklärungsfaktoren zur Kooperation des öffentlichen und privaten Sektors erörtert, welche aus der (*Network-) Governance-* und *Public-Private-Partnership*-Forschung (PPP) gewonnen wurden. Anschließend wird die Methodik beschrieben. Im letzten Teil werden die Ergebnisse der Experteninterviews präsentiert.

3. Welche Faktoren beeinflussen Kooperationen?

Derzeit dominieren Erhebungen zu Kooperationen, die im direkten Zusammenhang mit Vorfällen stehen (s.o.). Hier wird jedoch ein umfassendes und frühzeitig ansetzendes Verständnis von Kooperation vertreten. Beispielhaft hierfür stehen etwa PPPs zur Kriminalitätsbekämpfung. Um diesem weit gefassten Verständnis von Kooperation Rechnung zu tragen, werden die bereits dargestellten Aspekte mit Erkenntnissen aus der (Network-)Governance-Literatur und der Forschung zu PPPs angereichert. Die Zusammenführung dieser Ansätze soll im Folgenden komprimiert dargestellt werden, da diese die deduktiven Auswertungskategorien begründen, welche zur Analyse des Datenmaterials verwendet wurden.

3.1 Vertrauen und wechselseitige Beziehungen

Vertrauen gilt als einer der Schlüsselfaktoren für erfolgreiche Kooperationen zwischen Staat und Wirtschaft.[9] Dieser Beitrag orientiert sich an der Definition von Vertrauen von *Rousseau et al.*:

---

9 Wie z.B. von *Dunn-Cavelty* und *Suter* dargelegt (*Dunn-Cavelty & Suter* 2009).

> Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another.[10]

Vertrauen zwischen Akteuren entwickelt sich durch reziproke und erfolgreiche Zusammenarbeit, die wiederum selbst abhängig ist von Vertrauen, was die initiale Entstehung besonders schwierig macht. Welche Faktoren darüber hinaus dies ermöglichen können, wird im Folgenden dargestellt. Auf beiden Seiten der Akteure sind Vorbehalte im Bezug auf Kooperationen dominierend, die auf mangelndes Vertrauen zurückzuführen sind. Diese wurden von *Givens* und *Busch* treffend zusammengefasst:

> Government may be concerned about disclosure of classified information– whether accidental or deliberate […]. Similarly, businesses may be concerned about their own proprietary information being disclosed in public. Trade secrets could leak to the media. Competitors could steal a firm‘s secrets. Confidential data could be introduced in court for civil or criminal matters. Government agencies could even seize upon discrepancies in company data, using them as a pretext to enforce certain business regulations.[11]

3.2 Anreize und Ressourcen

Mangelnde Anreize und Ressourcen sind ein Hemmnis für Kooperation. Die Abwägung von Unternehmen beruht auf der Wahrnehmung, dass der Aufwand und die potenziellen Nachteile – wie Imageschäden, Eingriffe in das operative Geschäft, Offenlegung von Schwachstellen und die Dokumentation der Vorfälle – im Vergleich zu den erwartenden Vorteilen – wie direkte und unbürokratische Unterstützung in der Prävention oder Schadenswiedergutmachung – überwiegen. Dies geht einher mit begrenzten Ressourcen, die für Kooperationen zur Verfügung stehen, was insbesondere für KMU ein relevanter Faktor ist.[12] Aus der Perspektive eines Unternehmens, das seine Entscheidungen auf der Basis von Wirtschaftlichkeitsberechnungen fällt, sind Sicherheit und Kooperation schwer zu bewerten.

3.3 Strukturelle Faktoren

Inwieweit strukturelle Faktoren die Kooperation und den Informationsaustausch in PPPs und Netzwerken beeinflussen, ist ein anhaltender Diskurs und hängt oftmals vom konkreten Kontext ab. Beim Austausch sensibler Informationen sind jedoch Foren mit geringer Mitgliederzahl zu bevorzugen.[13] Je größer ein Netzwerk ist, des-

---

10 *Rousseau, Sitkin, Burt & Camerer* 1998, S. 395.

11 *Givens & Busch* 2013, S. 128.

12 Vgl. *Levi & Williams* 2013, S. 18.

13 Vgl. *Turrini, Cristofoli, Drosini & Nasi* 2010, S. 541–542.

to weniger effektiv wird es von Mitgliedern wahrgenommen. Vertrauen lässt sich leichter in kleinen oder bereits etablierten Netzwerken aufbauen.[14] Zu den Erfolgsfaktoren gehören aber auch die Transparenz von Strukturen, angemessene Kommunikationswege und klar definierte Ansprechpartner.

3.4 Formalisierung und Institutionalisierung

Der Grad der Formalisierung von Kooperationen und damit einhergehenden Verfahrensweisen ist eng verknüpft mit den zuletzt genannten strukturellen Faktoren:

> Formalization refers to such mechanisms of network functioning as formalized rules, organizing of meetings, the written agenda, and decision-making procedures.[15]

Als vorteilhaft für eine erfolgreiche Zusammenarbeit gelten folgende Verfahrensweisen: Die Kooperationspartner sollten frühzeitig gemeinsame Ziele aushandeln und festlegen, um das Risiko von unerfüllbaren Erwartungen zu reduzieren.[16] Innerhalb dieses Prozesses sollten die Kompetenzen und Verantwortlichkeiten einzelner Akteure herausgearbeitet werden. Dies dient nicht nur der Reduktion interner Risiken der Zusammenarbeit, sondern auch der Verdeutlichung, welchen externen (regulatorischen) Rahmenbedingungen die einzelnen Kooperationsteilnehmer unterliegen. Aufgrund der Sensibilität der auszutauschenden Informationen und in Abhängigkeit von den verwendeten Kommunikationsmitteln empfiehlt es sich, spezifische Vorgehensweisen festzulegen, um Vertraulichkeit zu garantieren.[17] Von Bedeutung ist dabei, ein angemessenes Maß an Formalisierung zu finden. Bei Überregulierung besteht die Gefahr, Netzwerke und PPPs ihres Hauptvorteils gegenüber hierarchischen Organisationsstrukturen, nämlich der Flexibilität, zu berauben. Dem gegenüber kann ein höherer Grad an Formalisierung zur Stabilität beitragen, was sich positiv auf die Vertrauensbildung auswirkt.

Auf Basis der vorangegangenen Erörterung des Forschungsstands können die Kategorien *Vertrauen und wechselseitige Beziehungen*, *Anreize und Ressourcen*, *Strukturelle Faktoren und Zuständigkeiten* sowie *Formalisierung und Institutionalisierung* als Einflussfaktoren für Kooperation festgehalten werden. Diese begründen die deduktiven Auswertungskategorien, welche zur Analyse des Datenmaterials verwendet wurden. Deren Verwendung und das damit verbundene Vorgehen werden in den folgenden Abschnitten erläutert.

---

14 Vgl. *Dunn-Cavelty & Suter* 2009, S. 4; *Luiijf & Kernkamp* 2015, S. 19.

15 *Turrini et al.* 2010, S. 542.

16 Vgl. *Whelan* 2012.

17 Vgl. *Luiijf & Kernkamp* 2015, S. 25, 39.

4. Forschungsdesign

Die erwähnten deutschsprachigen quantitativen Studien sind nur begrenzt in der Lage zu erklären, was Kooperation hemmt. Dies ist jedoch methodisch bedingt: Quantitative Ansätze zielen darauf ab, spezifische Variablen zu identifizieren oder auszuschließen, die zu einem konkreten Outcome führen.[18] Ein tiefgreifendes Verständnis dafür, wie sich diese hemmenden Faktoren genau konstituieren und in welchen Gesamtprozessen sie eingebettet sind, können quantitative Ansätze jedoch nur sehr begrenzt ermöglichen. Auch solche Faktoren, die Kooperation ermöglichen könnten oder sogar fördern würden, wurden bisher nur begrenzt erforscht. Um jedoch ein tiefgreifendes Verständnis für diese Zusammenhänge zu bekommen, wurde hier ein qualitativer Ansatz gewählt.

Qualitative Forschung hat den Anspruch, solche Fälle zu untersuchen, die besondere Relevanz für die Beantwortung der jeweiligen Forschungsfrage haben. Die Auswahl der Interviewpartner erfolgte im vorliegenden Fall mithilfe eines selektiven Samplings. Hierzu wurden vor der Datenerhebung folgende Kriterien für die Auswahl festgelegt: Sowohl Akteure des öffentlichen wie auch des privatwirtschaftlichen Sektors können Ausgangspunkt für Kooperationen sein;[19] dementsprechend wurden Experten aus beiden Sektoren interviewt. Insgesamt wurden 25 Interviews geführt, die sich auf zwei Gruppen verteilen (vgl. *Abbildung 1*). Die Gruppe des öffentlichen Sektors umfasst fünf Interviews mit Experten aus den Nachrichtendiensten und Strafverfolgungsbehörden. Hierbei wurden sowohl Vertreter von Behörden der Länder als auch des Bundes interviewt, um den Eigenheiten der föderalen Sicherheitsarchitektur Deutschlands Rechnung zu tragen. Diese führt auch im Bereich Wirtschaftsschutz zu unterschiedlichem Engagement und divergierenden Vorgehensweisen. Zwanzig Interviews fanden mit Experten aus der Privatwirtschaft/Industrie statt. Hierfür wurde folgendes Kriterium formuliert: Die Unternehmen und industrienahen Dienstleister sind KMU gemäß der Definition der EU Kommission.[20] Zwei Interviews wurden mit Experten relevanter Industrieverbände und Interessens vertretungen geführt, da diese einerseits die Rahmenbedingungen für Kooperationen aktiv mitgestalten und andererseits auch in aggregierter Form das Know-how und die Interessen ihrer Mitgliedsunternehmen repräsentieren.

Die Interviews wurden mithilfe teilstrukturierter Leitfäden geführt. Im Kontext von Kooperation deckten die Fragen Aspekte von Relevanz, Viktimisierung, Prävention, Bekämpfung sowie Potenziale bzw. Erwartungen ab. Die Leitfäden dienten den

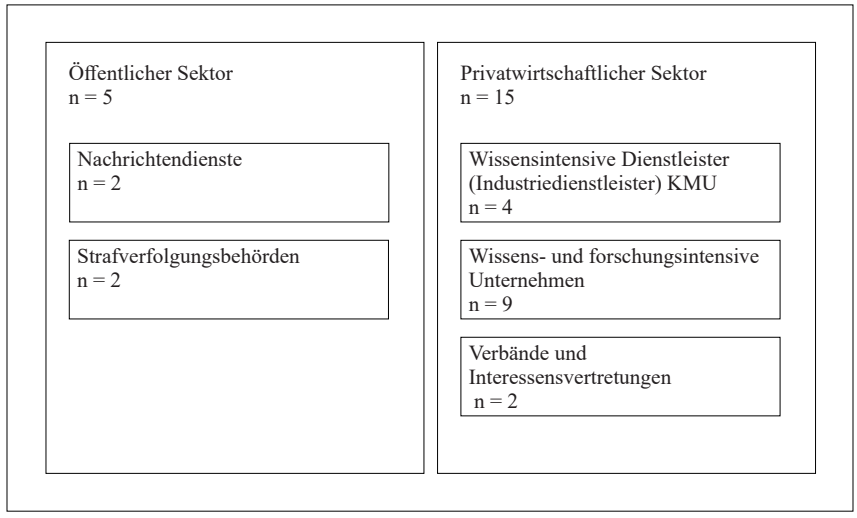
---

18 Vgl. *Przyborski & Wohlrab-Sahr* 2014, S. 122.

19 Gleiches gilt dementsprechend für die Adressaten von Kooperation.

20 Vgl. Klassifikation der EU 2003, Die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Amtsblatt der Europäischen Union NR. L 124 2005; Art 2; http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3An26026 [30.05.2017].

Abbildung 1 Sampling



Interviewern als Orientierung, um die relevanten Inhalte vollständig anzusprechen und Vergleichbarkeit zu sichern. Sie waren jedoch so flexibel gestaltet, dass auf die besondere Expertise des Interviewpartners eingegangen werden konnte. Die Interviews wurden persönlich oder telefonisch im Zeitraum von Mai bis November 2016 mit einer Dauer von 45 bis 210 Minuten durchgeführt. An jedem Interview waren zwei Wissenschaftler beteiligt, sowohl während des Interviews als auch bei der anschließenden Dokumentation/ Transkription. Zusätzlich wurde die Verschriftlichung den Interviewpartnern zur Kontrolle vorgelegt. Die Strukturierung und Auswertung der Interviews erfolgte mittels einer softwaregestützten[21] qualitativen Inhaltsanalyse angelehnt an *Mayring*.[22]

5. Ergebnisse der Experteninterviews

Im folgenden Abschnitt werden die Ergebnisse der Experteninterviews dargestellt. Hierfür erfolgte eine vergleichende Analyse des Status quo und der Erwartungshaltungen von Behörden, Unternehmen und Verbänden an Kooperationen. Die Gliederung dieses Abschnitts orientiert sich an den theoretisch begründeten Kategorien und wird ergänzt durch die induktiv gewonnenen Kategorien *Bewusstsein und Sensibilisierung* sowie *rechtliche und standardbasierte Faktoren*. *Bewusstsein und Sensibilisierung* bilden die erste Ergebniskategorie. Dies beruht darauf, dass die Grundlage für Aktionen gegen Wirtschaftsspionage darin besteht, selbige zu-

21 Verwendet wurde die Software MaxQDA 11 der Verbi GmbH.

22 Vgl. *Mayring* 2015.

nächst als Problem wahrzunehmen, zu identifizieren und zu beschreiben. Es folgen die deduktiven Kategorien *Vertrauen und wechselseitige Beziehungen*, *Anreize und Ressourcen*, *Strukturelle Faktoren und Zuständigkeiten* sowie *Formalisierung und Institutionalisierung*.

5.1 Bewusstsein und Sensibilisierung

Es konnte festgestellt werden, dass das Gefahrenbewusstsein für Wirtschafts- und Industriespionage zwischen den Unternehmen stark variiert, jedoch insgesamt eher gering ausgeprägt ist. Die Experten aus den Unternehmen bestätigten dies, als sie dazu aufgefordert wurden, eine Einschätzung des Gefahrenbewusstseins für ihre Branche und Geschäftspartner abzugeben. Als Beispiel ein Zitat eines KMU-Geschäftsführers aus dem Verarbeitenden Gewerbe:

> Ja, ich denke es wird prinzipiell komplett unterschätzt. Es ist zu beobachten, dass alle bei dem Hype um Industrie 4.0 mitmachen möchten, die Sicherheit dabei aber unbedacht bleibt. Apps wie z. B. die Fernwartung können ein offenes Tor zur Maschine sein, insbesondere, wenn dabei Ad-Ups, zum Beispiel mit Backdoor-Funktionen, zum Einsatz kommen. Es gibt teilweise enorm talentierte Entwickler im Maschinenbau, die beachtliche Dinge entwickeln und umsetzen, deren Kompetenzen jedoch nicht in der IT liegen. Die Sicherheitsverantwortung darf man hierbei jedoch nie vergessen und muss bei der Entwicklung und Betrieb berücksichtigt werden.

Ein Unterschätzen der Gefahren ist insofern problematisch, als das Bewusstsein für potenzielle Gefahren durch Wirtschafts- und Industriespionage die Basis für eigeninitiatives Handeln, einschließlich Kooperationen, bildet. Für das geringe Gefahrenbewusstsein bei Unternehmen konnten folgende Erklärungsansätze identifiziert werden: Teilweise betrachten die Unternehmen sich selbst schlichtweg nicht als potenzielle Ziele von Spionage, da sie ihre Vermögenswerte nicht als lohnenswerte Ziele einstufen und ihre eigene Bedeutung innerhalb ihrer Branche als gering bewerten. Diese Einschätzung ist grundsätzlich anzuzweifeln, da es sich bei den ausgewählten Unternehmen durchweg um solche mit innovativen Geschäftsmodellen handelt. Tendenziell konnte beobachtet werden, dass mit zunehmender Größe eines Unternehmens auch ein stärker ausgeprägtes Gefahrenbewusstsein vorhanden ist. Bei Kleinst- und Kleinunternehmen findet eine sehr starke Fokussierung auf das Tagesgeschäft statt. Für präventive Aktivitäten sind in der Regel wenig Ressourcen verfügbar, wie sich an der Aussage des folgenden Interviewpartners nach einem Vorfall verdeutlichen lässt:

> Es gibt zwar keine Beweise, aber signifikante Merkmale. Auch der eine oder andere Indizienbeweis ist über interne Aussagen von Mitarbeitern belegbar. Der Aufwand, diese Beweiskette zu schließen, ist allerdings sehr hoch. Würde ich diesen Weg gehen, hätte ich keine Zeit für das operative Geschäft und die Sicherung der Arbeitsplätze der anderen Mitarbeiter.

Bei allen Unternehmen, die bereits Opfer von Informationsdiebstahl waren, konnte ein deutlich stärker ausgeprägtes Gefahrenbewusstsein und eine höhere Sensibilisierung festgestellt werden. Bei Unternehmen, die unabhängig von einer Viktimisierung Präventionsmaßnahmen umgesetzt hatten, geschah dies nur bedingt auf Basis eines spionagespezifischen Gefahrenbewusstseins, sondern oft im Hinblick auf andere, aber verwandte Gefahren, wie etwa Cyberkriminalität. Diese Art der Wahrnehmung von Wirtschafts- und Industriespionage, welche sich aus einzelnen oder mehreren Modi Operandi ableitet, kam bei der Mehrzahl der Unternehmensexperten zum Ausdruck. Die vorgefundenen Präventionsmaßnahmen wurden jedoch nur selten auf Basis einer Kooperation mit Behörden initiiert oder umgesetzt. Die Kenntnisse von staatlichen Angeboten sind gering. Grundsätzlich kann festgestellt werden, dass die Wahrscheinlichkeit für unternehmerische Aktivitäten im Bereich der Informationssicherheit höher ist, wenn Wirtschafts- und Industriespionage als unmittelbare Gefahr mit einer hohen Eintrittswahrscheinlichkeit wahrgenommen werden. Des Weiteren ist ein relevanter Faktor, inwieweit solche Aktivitäten Teil des Geschäftsszenarios und der Wirtschaftlichkeitsberechnungen sind.

5.2 Vertrauen und wechselseitige Beziehungen

Die aus der Literatur bekannten vertrauensbasierten Vorbehalte gegenüber Kooperationen spiegeln sich auch in den Aussagen der Experten des privaten Sektors wider. Exemplarisch hierfür steht die Reaktion des Interviewpartners, der für einen wissensintensiven Industriedienstleister tätig ist:

> Zur Offenlegung von Unternehmensgeheimnissen: Ich kenne die internen Wege bei Behörden nicht und weiß auch nicht, was dem anderen mitgeteilt wird, wenn ich z. B. Anzeige erstatten würde gegen einen ehemaligen Mitarbeiter. Daher wäre ich da sehr vorsichtig, was ich überhaupt angebe.

Im Gegenzug zeigten die Interviews mit Behördenvertretern, dass diese ein sehr ausgeprägtes Bewusstsein für die von den Unternehmen angeführten Vorbehalte haben. Das Vertrauensdefizit auf Unternehmerseite scheint sich aus zwei Komponenten zusammenzusetzen: Unternehmen nehmen die Abläufe im öffentlichen Sektor als wenig transparent wahr und zweitens haben sie nur geringe Kenntnisse von den behördlichen Abläufen, namentlich dem Vorgehen bei Ermittlungen und dem Informationsaustausch zwischen Behörden und externen Akteuren. Das ist wenig verwunderlich, da es sich für Unternehmen nicht um alltäglichen Vorgänge handelt. Die Interviews zeigten zwar einerseits, dass zum Teil auf ein sehr ausgeprägtes Bewusstsein der Beamten aufgebaut werden kann, andererseits aber auch, dass ein „rücksichtsvolles“ Vorgehen deutlich mehr in den Mittelpunkt der Behördenkommunikation gerückt werden sollte. Dabei ist es besonders wichtig, Informationen zu Vorgehen und Abläufen leicht zugänglich und möglichst präzise und für „Laien“

verständlich zu kommunizieren. Beide Punkte sind besonders in Krisensituationen von hoher Bedeutung, um die Hemmschwelle für eine Zusammenarbeit zu senken:

> Während des Tagesgeschäfts ist praktisch keine Zeit, um sich mit der Thematik explizit zu beschäftigen, da immer das operative Geschäft im Vordergrund steht. Bei einem Vorfall müsste man sich dann entsprechend schnell informieren können.

In Einzelfällen gründen Vertrauensdefizite der Unternehmen auf negativen Erfahrungen bei der Zusammenarbeit mit Sicherheitsbehörden in der Vergangenheit. Diese bezogen sich jedoch auf Erfahrungen mit Strafverfolgungsbehörden und der Justiz in anderen Phänomenbereichen, die nun auf die Wirtschafts- und Industriespionage übertragen werden. Die Unternehmen machten deutlich, dass eine Zusammenarbeit transaktional sein muss, sind aber skeptisch, inwieweit die Behörden diesem Anspruch gerecht werden können:

> Ja, so etwas könnte ich mir auch vorstellen in Deutschland, nur müsste es in beide Richtungen gut funktionieren, d.h. ich müsste auch sehen können, wie jetzt der Status der von mir gemeldeten Bedrohung ist und was die Behörden unternehmen.

Aufgrund der wahrgenommenen Intransparenz behördlicher Vorgänge existiert ein großes Bedürfnis nach persönlichen Ansprechpartnern und zeitnahen Informationen zu Vorgängen, an denen Unternehmen beteiligt sind. Nur so können Unsicherheiten adressiert und kann Misstrauen reduziert werden. Der persönliche Kontakt war in der Vergangenheit ganz besonders im Kontext von akuten Vorfällen ein Schlüsselfaktor für erfolgreiche Kooperation. Rein transaktionale Kooperationsbeziehungen bergen aber auch Risiken, da staatliche und unternehmerische Ressourcen für Kooperationen begrenzt sind. Dabei können speziell kleine (und Kleinst-)Unternehmen schnell ins Hintertreffen gegenüber größeren Unternehmen geraten. Bei ersteren konnte nur wenig Interesse an einer vorfallsunabhängigen und direkten Kooperation festgestellt werden, da das Tagesgeschäft Priorität hat und entsprechend wenige Ressourcen für anderweitige Aktivitäten zur Verfügung stehen. Im Gegensatz dazu können größere Unternehmen größeren Aufwand in transaktionale Beziehungen investieren. Problematisch wird dies dann, wenn seitens der Unternehmen eine „gleichwertige" Gegenleistung, z.B. in Form von Beratung oder Informationen, erwartet wird– was in der Folge aufgrund begrenzter Ressourcen der Behörden zu Lasten des Engagements für kleinere Kooperationspartner ginge. Für Unternehmen, welche grundsätzlich an permanenter und/oder direkter Kooperation interessiert sind, ist für eine erfolgreiche Zusammenarbeit ausschlaggebend, dass die Beziehung direkte und greifbare Vorteile generiert, die zum Schutz des Unternehmens beitragen. Beispiele hierfür sind Best-Practice-Lösungen aus anderen Unternehmen oder anderen Kontexten, die mit wenig Aufwand anwendbar sind. Es konnte aufgezeigt werden, dass bei Kooperationsaktivitäten mit mehreren Teilnehmern die Wahrscheinlichkeit für einen erfolgreichen Informationsaustausch höher ist, wenn diese in kleinen Austauschforen mit

begrenzter Mitgliederzahl stattfanden, welche ein vertrauensvolles Interagieren ermöglichen. Austauschforen, die als Peer-to-Peer-Formate konzipiert sind, in denen der Staat sich auf die Rolle des Moderators und/oder Initiators beschränkt, scheinen für einen vertrauensvollen Austausch hinsichtlich ihrer Inhalte gewinnbringend zu sein.

Grundsätzlich kann festgestellt werden, dass ein Unternehmen, das eine etablierte Beziehung zu einem Behördenvertreter aufgebaut hat, bemüht ist, diese aufrechtzuerhalten und immer mit derselben Kontaktperson zu kommunizieren. Da der Aufbau solcher Beziehungen und vor allem des damit einhergehenden Vertrauens ein langfristiger Prozess ist, sollte dieser Aspekt auch bei der Personalplanung der Behörden berücksichtigt werden, um entsprechende Partner nicht zu verlieren.

5.3 Anreize und Ressourcen

Ein Mangel an Ressourcen im öffentlichen und privaten Sektor beeinträchtigt erfolgreiche Kooperation. Bei Unternehmen kann dies teilweise auf eine offensichtlich wenig attraktive Anreizstruktur für Investitionen in Informationssicherheit und damit einhergehende Kooperationen zurückgeführt werden. Des Weiteren können Faktoren festgestellt werden, welche spezifisch für den öffentlichen Sektor sind:

Behörden verfügen über zu geringe personelle Ressourcen, um früh ansetzende und nachhaltige Kooperationen umzusetzen, zumal es bei den Unternehmen ein großes Bedürfnis nach persönlichen Ansprechpartnern gibt und der Aufbau von Vertrauen und Netzwerken ein personalintensiver und langfristiger Prozess ist. In den Fällen, in denen eine direkte Zusammenarbeit im Bereich Wirtschaftsschutz stattgefunden hat, werden das Engagement und die Fachkenntnisse der Behörden stets als sehr positiv bewertet. Dies erscheint als ein möglicher Ansatz, um den allgemeinen Vorbehalt, Behörden seien insbesondere in Fällen der Cyberkriminalität kein hilfreicher Ansprechpartner, künftig auszuräumen. In Fällen, in denen Unternehmen aber erst gar nicht damit rechnen, dass ihnen bei entsprechenden Vorfällen angemessen und zeitnah geholfen werden kann, besteht ein deutlich geringerer Anreiz, mit den Behörden zusammenzuarbeiten.

Ein Mangel an Ressourcen konnte auch im privaten Sektor festgestellt werden:

> Es ist durchaus vorstellbar bei Prävention und Aufklärungsarbeit mit staatlichen Stellen zusammen zu arbeiten. Allerdings für unser Unternehmen nicht. Wir sind zu klein und es würde zu viele Ressourcen binden, die wir für das tägliche Geschäft benötigen.

Insbesondere kleine Unternehmen wenden nur wenige Ressourcen für Informationssicherheit auf. Dieses Defizit bezieht sich sowohl auf technische als auch auf nicht technische Maßnahmen. Wenn investiert wird, geschieht dies oftmals sehr punktuell und wenig strategisch. Beispielhaft hierfür ist die Fokussierung auf technische As-

pekte der IT-Sicherheit. Die Entscheidung der Unternehmen, ob es zu einer Kooperation mit Behörden kommt, ist in der Regel an einer Kosten-Nutzen-Abwägung orientiert. Anreize für eine Kooperation sind absehbare und substanzielle Vorteile, die dazu beitragen, (eventuelle) Schäden zu kompensieren und/oder signifikant zu reduzieren, unmittelbar den Schutz des Unternehmens erhöhen und sich mit geringem Aufwand umsetzen lassen.

Ein Teil der Sicherheitsbehörden ist äußerst bestrebt, Kooperationsbeziehungen als Win-Win-Situationen zu organisieren und es sind proaktive Ansätze erkennbar. Dazu werden den Unternehmen und Verbänden möglichst attraktive und passgenaue Kooperationsangebote unterbreitet. Für die Behörde bietet dies den Vorteil, das eigene Angebot stetig optimieren zu können. Ein solch proaktives Vorgehen deckt sich weitestgehend mit der Erwartungshaltung der Unternehmen und Verbände. Einer darüber hinausgehenden Erwartung der Unternehmen an die Erbringung von quasikommerziellen Dienstleistungen durch Behörden sollte jedoch mit Vorsicht begegnet werden.

5.4 Strukturelle Faktoren und Zuständigkeiten

Die derzeitigen administrativen Strukturen und die behördliche Kompetenzverteilung sind nicht immer von Vorteil für die Kooperation von Wirtschaft und Behörden. Die Wirtschaft nimmt die verteilten Verantwortlichkeiten als irritierend wahr. Es konnte eine starke Unsicherheit hinsichtlich der Zuständigkeiten und eventueller Folgen bei einer Kooperation festgestellt werden. Dies verdeutlicht beispielhaft die Aussage des folgenden Interviewpartners:

> Polizei kommt mir aber irgendwie komisch vor, da denke ich immer an Verkehrsunfälle und Einbrüche.

Die Behördenvertreter sind sich dieser Problematik grundsätzlich bewusst und haben auf der Arbeitsebene organisatorische Maßnahmen angestoßen und implementiert, um Hemmnisse für Kooperationen abzubauen.

Die Unsicherheit der Unternehmen lässt sich mit folgenden Fragen zusammenfassen: Welche Zuständigkeiten gibt es? Wer sind die Ansprechpartner? Was kann ich von diesen erwarten? Was sind die grundsätzlichen Konsequenzen einer Kooperation, und insbesondere was passiert mit von mir geteilten Informationen? Die Unternehmen erwarten einfach zugängliche Antworten auf diese Fragen. Zeitgleich mit der Datenerhebung wurden teilweise bereits Maßnahmen umgesetzt, die diese Fragen adressieren. Die Sichtbarkeit von Ansprechpartnern und der Angebote der Sicherheitsbehörden für Unternehmen zu erhöhen, ist auch wichtiger Bestandteil der *Initiative Wirtschaftsschutz*. Rückschlüsse, inwieweit diese Plattform das Informationsbedürfnis der Unternehmen deckt, können hier jedoch nicht gemacht werden, da sich das Portal www.wirtschaftschutz.info zum Zeitpunkt der Datenerhebung noch in der Anlaufphase befand und keinem der Unternehmen bekannt war.

Für die Mehrheit der interviewten KMU fungieren die lokalen Polizeidienststellen als erster behördlicher Ansprechpartner. Dies bedeutet im Umkehrschluss, dass die Beamten in der Fläche entsprechend geschult sein müssen, um geschulte Ansprechpartner zu vermitteln und Verdachtsfälle auch als Wirtschafts- und Industriespionage zu erkennen. Ob dieser Erstkontakt auf der untersten Ebene perspektivisch sinnvoll ist im Sinne eines Single-Point-of-Contact muss hinterfragt werden.

Ein weiterer wichtiger Aspekt für das Verständnis der unterschiedlichen Perspektiven ist die Diskrepanz zwischen der Wahrnehmung von Wirtschafts- und Industriespionage durch Unternehmen und die Organisation der staatlichen Strukturen, welche für deren Bekämpfung zuständig sind. Unternehmen unterscheiden zum einen nicht zwischen Wirtschafts- und Industriespionage, zum anderen nehmen sie diese nur als eine Bedrohung unter vielen wahr.[23] Teile der staatlichen Strukturen, insbesondere der Strafverfolgungsbehörden, sind jedoch auf Grundlage der Unterscheidung von Wirtschafts- und Industriespionage organisiert. Insgesamt entsprechen allerdings Organisationsstrukturen, die ganzheitlich den Bereich Wirtschaftsschutz bearbeiten, wie etwa bei einer Vielzahl der Verfassungsschutzämter, eher den Erwartungen der Unternehmen. Die Zusammenfassung und Bearbeitung vielfältiger Bedrohungen in Form einer einheitlichen Behörde wird von den Unternehmen erwartet und bietet auch die Möglichkeit, diese aus „einer Hand" zu betreuen. Zum Teil sind sich Behördenmitarbeiter dieser strukturellen Hemmnisse bewusst und haben bereits entsprechende Maßnahmen ergriffen. Hierzu gehören beispielsweise der Einsatz von Single-Points-of-Contact oder interne Kommunikationsrichtlinien zum Informationsaustausch. Verkürzt stellt es sich so dar, dass die Nachrichtendienste zwar aktiv Unternehmenskooperationen pflegen, jedoch hinsichtlich ihrer Kompetenzen verfassungsrechtlich auf die Prävention von Wirtschaftsspionage beschränkt sind. Im Gegensatz dazu sind die Strafverfolgungsbehörden zwar befugt, sich Fällen von Wirtschafts- und Industriespionage anzunehmen, besitzen jedoch nicht die optimale Ausstattung, um mit Unternehmen bereits im Präventionsbereich umfassend zu kooperieren. Angesichts der oft erst spät möglichen Unterscheidung, ob ein ausländischer Nachrichtendienst beteiligt ist, was zudem von einem Unternehmen kaum zu erkennen ist, ist hier der Gesetzgeber gefragt, eine einheitliche Erstzuständigkeit gegenüber den Unternehmen zu definieren.

Weitere strukturelle Hemmnisse ergeben sich aus der föderalen Sicherheitsarchitektur Deutschlands. Dies hat zu Folge, dass die Ressourcen und Angebote, welche die Sicherheitsbehörden in Kooperationen einbringen können, und deren Vorgehen im Einzelfall deutlich variieren. Dies verstärkt die bereits beschriebenen Unsicherheiten bei Unternehmen.

Wie bereits vielfach in der Literatur beschrieben, sind private Dienstleister oft der erste Ansprechpartner bei Vorfällen. Dies trifft mehrheitlich auch auf die inter-

---

23 Siehe auch *Abschnitt 5.1* im vorliegenden Kapitel.

viewten Experten zu. Häufig werden vor allem die für die IT des Unternehmens verantwortlichen Dienstleister als erste Ansprechpartner genannt. Hierbei handelt es sich eher um kleinere (und teilweise lokale) Anbieter mit denen oftmals bereits langfristige, vertrauensvolle Geschäftsbeziehungen bestehen. Solche IT-Dienstleister sollten auch von den Sicherheitsbehörden als potenzielle Kooperationspartner erwogen werden, da sie einen möglichen Zugang zur eigentlichen Zielgruppe der KMU darstellen.

5.5 Formalisierung und Institutionalisierung

Teilweise verfügen die interviewten Behörden über interne Strategien zu Vorgehensweisen und Zusammenarbeit mit Unternehmen. In welchem Umfang diese umgesetzt werden, lässt sich im Rahmen dieses Beitrags nicht überprüfen. Es kann jedoch festgestellt werden, dass diejenigen Behörden, die in ihren internen Strategien der Kooperation hohe Priorität beimessen, diese auch systematisch umsetzen, z.B. in Form von internen Richtlinien.

Aufseiten der KMU gibt es bei den befragten Unternehmen keine Richtlinien oder Grundsätze zur Kooperation mit Sicherheitsbehörden. Entscheidungen werden hier tendenziell eher fallbasiert getroffen. Mangels eines Anreizes haben kleinere Unternehmen, wie bereits beschrieben, derzeit wenig Interesse an einer dauerhaften Kooperation. Bei Unternehmen mittlerer Größe kann in Teilen Interesse an regelmäßiger Kooperation festgestellt werden, sofern diese keinen bürokratischen Aufwand mit sich bringt. Fast alle KMU stehen in regelmäßigem Austausch mit den Kammern, Fach- und Branchenverbänden, welche von den Behörden noch intensiver als mögliche Multiplikatoren genutzt werden könnten. Die bestehenden PPPs und formalisierten Kooperationen auf Ebene des Bundes und der Länder scheinen geringe unmittelbare Bedeutung für die interviewten KMU zu haben. Um die Bereitschaft zur Kooperation zu erhöhen, ist es daher wichtig, dass Strategien für eine direkte und zielgruppengerechte Ansprache der KMU entwickelt werden.

5.6 Rechtliche und standardbasierte Rahmenbedingungen

Sowohl der öffentliche als auch der private Sektor haben vergleichbare Vorstellungen davon, inwiefern ihre jeweiligen Kooperationsmöglichkeiten durch die derzeitigen rechtlichen Rahmenbedingungen beeinflusst werden. Es wird deutlich, dass Unternehmen sich durch die Zusammenarbeit mit Behörden Vorteile, wie konkrete Informationen zu Modi Operandi, erhoffen. Dieses Bedürfnis der Unternehmen wird auch von Behördenvertretern bestätigt. Die Behörden unterliegen jedoch starken rechtlichen und taktischen Einschränkungen hinsichtlich der Weitergabe von konkreten Informationen. Gerade diese stellen aber einen Anreiz für Unternehmen dar, mit Behörden zu kooperieren. Grundsätzlich stimmen die Experten beider Sektoren überein, dass die aktuellen rechtlichen und standardbasierten Rahmenbedingungen

wenig förderlich für Kooperationen sind. Interessant ist auch der Vorschlag der Vertreter der Sicherheitsbehörden, die höhere Sicherheitsstandards als Vorgabe für alle Unternehmensgrößen etablieren wollen, was auch die Berufung von Sicherheitsbeauftragten einschließt, die dann wiederum als direkte Ansprechpartner für die Behörden dienen könnten.

6. Fazit

Dieser Beitrag hat die Zusammenarbeit von Behörden und KMU mit einem qualitativen Ansatz untersucht. Auf Basis von 25 Interviews konnten sechs Themenfelder identifiziert werden, die Kooperationen im Bereich der Wirtschafts- und Industriespionage beeinflussen. Von besonderer Relevanz sind folgende Faktoren: Ein elementares Hemmnis ist das geringe Gefahrenbewusstsein für Wirtschafts- und Industriespionage bei KMU. Hieraus resultiert ein geringes Handlungsbedürfnis, Maßnahmen gegen Wirtschafts- und Industriespionage einzuleiten, was entsprechende Kooperationen einschließt. Hinzu kommt ein geringer Kenntnisstand zu Vorgängen und Angeboten der Behörden. Darauf beruht in Teilen auch das mangelnde Vertrauen in die Vorgehensweisen der Behörden, welche als intransparent wahrgenommen werden. Hilfreich sind in diesem Zusammenhang persönliche Ansprechpartner bei Behörden und eine proaktive Kommunikation. Weitere Faktoren sind mangelnde Anreize für Unternehmen, die sehr stark an absehbaren und substanziellen Vorteilen im Zuge von Kooperationen interessiert sind. Zusammenarbeit ist insbesondere dann erfolgreich, wenn diese als Win-Win-Situation wahrgenommen wird. Sowohl im öffentlichen als auch im privaten Sektor wird Kooperation durch mangelnde Ressourcen ausgebremst. Die derzeitigen administrativen Strukturen und Verantwortlichkeiten sind nicht vorteilhaft, da sie zur Verunsicherung bei Unternehmen beitragen und nur bedingt in der Lage sind, alle Kooperationsmöglichkeiten aus einer Hand anzubieten. Besagte Nachteile können teilweise durch Single-Points-of-Contact und interne Abstimmung ausgeglichen werden. Besonders kleine Unternehmen sind sehr stark auf das Tagesgeschäft fokussiert; dementsprechend müssen sich Kooperationsanstrengungen darin integrieren lassen.

Darüber hinaus hat die intensivere Erforschung von Kooperationen zwischen (halb-) staatlichen und privaten Akteuren eine signifikante Bedeutung im Zuge der anhaltenden Tendenz zur Schaffung von Sicherheit durch letztere, da diese Forschung dazu beitragen kann, einer Entkopplung von öffentlichem und privatem Sektor vorzubeugen.

Literatur

Boes, S. & Leukfeldt, E.R. (2017): Fighting Cybercrime: A Joint Effort, in: R.M. Clark & S. Hakim (eds.), Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level. Cham, pp. 185–203.

Bundesregierung (2013): Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD; www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile [28.05.2017].

Corporate Trust (2014): Studie Industriespionage 2014. Cybergeddon der deutschen Wirtschaft durch NSA & Co.?; www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2014_DE.pdf [30.05.2017].

Dunn-Cavelty, M. & Suter, M. (2009): Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection 2/4, pp. 179–187.

Givens, A.D. & Busch, N.E. (2013): Information Sharing and Public-Private Partnerships: The Impact on Homeland Security. The Homeland Security Review 7/2, pp. 123–150.

Hedayati, H. & Bruhn, H. (2015): Compliance-Systeme und ihre Auswirkung auf die Verfolgung und Verhütung von Straftaten der Wirtschaftskriminalität und Korruption; www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015ComplianceSystemeHauptstudie.html [30.05.2017].

Kasper, K. (2014): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Wiesbaden.

Kopke, C., Petri, A., Kob, T., Sopha, S.M., Holz, W., Seyerlein-Klug, A., Schulz, M., Geschonneck, A., Kröger, S. & Münstermann, M. (2016): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie; www.bitkom.org/noindex/Publikationen/2016/Studien/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-Industrie/161110-Studie-Wirtschaftsschutz.pdf [30.05.2017].

Levi, M. & Williams, M.L. (2013): Multi-agency partnerships in cybercrime reduction. Mapping the UK Information Assurance Network Cooperation Space. Information Management & Computer Security 21/5, pp. 420–443.

Luiijf, E. & Kernkamp, A. (2015): Sharing Cyber Security Information. Good Practice Stemming from the Dutch Public-Private-Participation Approach. https://repository.tudelft.nl/view/tno/uuid:1eeb81c7-4328-459f-944d-f55c52e31fb1/ [30.05.2017].

Mayring, P. (2015): Qualitative Inhaltsanalyse. Weinheim.

Przyborski, A. & Wohlrab-Sahr, M. (2014): Forschungsdesigns für die qualitative Sozialforschung, in: N. Baur & J. Blasius (Hrsg.), Handbuch Methoden der empirischen Sozialforschung. Wiesbaden, S. 117–134.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. & Camerer, C. (1998): Not So Different After All: A Cross-discipline View of Trust. Academy of Management Review 23/3, pp. 393–404.

Turrini, A., Cristofoli, D., Drosini, F. & Nasi, G. (2010): Networking literature about determinants of network effectiveness. Public Administration, 88/2, S. 528–550.

Whelan, C. (2012): Networks and National Security. Dynamics, Effectiveness and Organisation. Burlington.

Ziegleder, D. (2010): Wirtschaftskriminalität im Geschäftsleben. Eine empirische Untersuchung formeller und informeller Handlungsstrategien von Unternehmen am Beispiel Deutschlands. Baden-Baden.

Wissenschaftsspionage – Risiken für den deutschen Forschungsstandort?

Sabine Carl

1. Einleitung

Im Sommer 2015 berichtete das Nachrichtenmagazin „Der Spiegel", dass die Bundesanwaltschaft gegen einen russischen Wissenschaftler ermittle. Ihm wurde vorgeworfen, während eines früheren Aufenthaltes in Deutschland vertrauliche Forschungsergebnisse, die der Entwicklung ultraschneller Quantencomputer dienen, entwendet und dem russischen Auslandsgeheimdienst verraten zu haben.[1] Auch der chinesische Geheimdienst wird immer wieder hinter Angriffen auf deutsche Forschungseinrichtungen vermutet, um technologisch aufholen zu können, ohne selbst in die Forschung investieren zu müssen. Deutsche Forschungsergebnisse sind ein begehrtes Ziel wissenschaftlicher und wirtschaftlicher Konkurrenz aus dem In- und Ausland.[2] Dennoch spielt die Wissenschaftsspionage nicht nur in der Wahrnehmung potenziell betroffener Forschungseinrichtungen, sondern auch in der politischen und medialen Beobachtung eine eher untergeordnete Rolle.[3] Es stellt sich daher die Frage, ob sich universitäre und außeruniversitäre Forschungseinrichtungen der Möglichkeiten und Gefahren eines illegalen Datenabflusses bewusst sind und welche präventiven Strategien und Maßnahmen zur Entdeckung von Vorfällen sie etabliert haben.

---

1 Vgl. *Gude* 2015, S. 47.

2 Ebenso *Boos* 2012, S. 61, 67.

3 Vgl. beispielhaft die Anzahl der Google-Treffer allein für den Begriff Wirtschaftsspionage (203.000, 0,37 Sek.) mit den Treffern zum Begriff Wissenschaftsspionage (1.500, 0,31 Sek.) [03.04.2019]; dies entspricht einer knapp 135-mal höheren Trefferzahl für Wirtschaftsspionage. Mangels existierender (wissenschaftlicher) Publikationen kommt das vorliegende Kapitel ohne einen Abschnitt zum „Anschluss an den Forschungsstand" aus. Erwähnenswerte Ausnahme ist der Tagungsband der Freiberger Sicherheitskonferenz „Sicher forschen und entwickeln" aus dem Jahr 2012, und dort vor allem das Kapitel von *Boos* (siehe *Boos* 2012).

Im vorliegenden Kapitel werden nach der rechtlichen Einordnung der Phänomene der Wissenschaftsspionage und (Konkurrenz-)Ausspähung im Wissenschaftskontext die Bedrohungslage sowie mögliche Szenarien des illegalen Wissensabflusses vorgestellt, der Handlungsbedarf bestimmt und Lösungsansätze anhand von ausländischen Best-Practice-Beispielen diskutiert.

1.1 Ausgangslage

Spionage stellt für Wissenschaftsorganisationen anders gelagerte Herausforderungen als für Wirtschaftsunternehmen dar. Wissenschaftsorganisationen befinden sich in einem unauflösbaren und beständigen Zielkonflikt zwischen dem auf Austausch ausgerichteten Wissenschaftsbetrieb und dem Bedürfnis, selbst generierte Daten zu schützen. Sie sind aufgefordert, das in besonderem Maße an Hochschulen gestellte und aus der staatlichen Finanzierung herrührende Gebot der Offenheit, also die Forderung, Forschungsergebnisse der Allgemeinheit uneingeschränkt zur Verfügung zu stellen, mit dem Bedürfnis Daten zu schützen, die nicht[4] oder noch nicht zur Publikation vorgesehen sind oder in Kooperation mit der Industrie erarbeitet wurden und Geheimhaltungsregelungen unterliegen, in Einklang zu bringen. Im Vergleich zur Ausspähung von Unternehmen fehlen Erkenntnisse über die Höhe und die Art von Schäden.[5] Aus den im Rahmen des WiSKoS-Forschungsprojekts geführten Experteninterviews mit Vertretern von Wissenschaftsorganisationen ergibt sich, dass sich Wissenschaftsorganisationen vor allem von Vertrauensverlust bedroht sehen. Jener wirkt sich insofern negativ auf künftige Forschungsaktivitäten aus, als mit einem Entzug von industriellen oder auch staatlichen Fördermitteln und einer reduzierten Konkurrenzfähigkeit bei der Akquise von exzellenten Nachwuchsforschern zu rechnen ist. Schäden drohen aber auch insoweit, als die Investitionsausgaben der Bundesrepublik ihren volkswirtschaftlichen Nutzen im Fall der illegalen Abschöpfung neuer Erkenntnisse verfehlen.[6]

1.2 Terminologie und rechtliche Einordnung

Für den Begriff der Wissenschaftsspionage gibt es, wie auch im Fall der Wirtschaftsspionage und Konkurrenzausspähung, weder eine einheitliche Verwendung im Sprachgebrauch noch eine Legaldefinition.[7]

---

4 Hier kommt z.B. Forschung mit Dual-Use-Aspekten in Betracht.

5 Ebenso *Boos* 2012, S. 62.

6 Im Jahr 2010 wurden zwischen zwei und drei Prozent des BIP in F&E investiert, vgl. http://ec.europa.eu/eurostat/web/science-technology-innovation/overview [12.07.2017]; vgl. auch *Fleischer* 2016, S. 63.

7 Zur Diskussion und Abgrenzung von Wirtschaftsspionage und Konkurrenzausspähung siehe *Carl et al.* 2017, S. 2–3.

1.2.1 Definition von Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext

Die Verfassungsschutzbehörden, so z.B. das Bayerische Landesamt für Verfassungsschutz, verstehen Wissenschaftsspionage als die staatlich gelenkte Ausforschung von Hochschulen durch fremde Nachrichtendienste.[8] Werden die gegen Wissenschaftsorganisationen gerichteten Spionageaktivitäten durch Wirtschaftsunternehmen ausgeführt, wird, wie im Fall von Spionageaktivitäten zwischen Wirtschaftsunternehmen, von Konkurrenzausspähung gesprochen. Somit wird die für Unternehmen bestehende starre begriffliche Trennung von Wirtschaftsspionage und Konkurrenzausspähung auf den Wissenschaftsbereich übertragen. Aus der Perspektive betroffener Wissenschaftseinrichtungen ist im Fall eines schädigenden Vorfalls die Identifikation der Täter als staatliche Akteure, Unternehmen oder wissenschaftliche Konkurrenten genauso wenig relevant wie für geschädigte Wirtschaftsunternehmen.[9] Die Unterscheidung von Wissenschaftsspionage und Konkurrenzausspähung dient vor allem der Differenzierung von Behördenzuständigkeiten und anzuwendenden Normen und ist daher nur bedingt zweckmäßig.

Für die Anwendung der Definition von Wissenschaftsspionage als staatlich gelenkte Ausforschung von Wissenschaftsorganisationen durch fremde Nachrichtendienste finden sich einige Belege sowohl in der Presse als auch in Veröffentlichungen deutscher Behörden.[10] Für die Konkurrenzausspähung im Wissenschaftskontext stellt sich die Lage komplexer dar. Der Begriff der Konkurrenzausspähung, der als Ausforschung eines Wirtschaftsunternehmens durch konkurrierende Unternehmen definiert ist, kann nicht unangepasst in den Wissenschaftskontext übertragen werden, da nicht deutlich wäre, ob eine Ausforschung durch konkurrierende Unternehmen, konkurrierende Wissenschaftsorganisationen oder beides erfasst sein soll. Die Begrifflichkeit könnte jedoch auf „Konkurrenzausspähung im Wissenschaftskontext" erweitert werden, um so das Handeln aller potenziellen Akteure zu erfassen. Eine solche Erweiterung ist aber nur dann sinnvoll, wenn bei der Konkurrenzausspähung im Wissenschaftskontext überhaupt ein strafbares Handeln vorliegt.[11]

---

8 Vgl. hier und im Folgenden Bayerisches Landesamt für Verfassungsschutz (o.D.).

9 Vgl. *Kilchling & Carl* 2016, S. 188.

10 Von entsprechenden, aber letztendlich wohl nicht erfolgreichen Ermittlungen berichtet z.B. der Spiegel (*Gude* 2015, S. 47); Behördennachweise finden sich u.a. beim Bundesamt für Verfassungsschutz, so z.B. im Verfassungsschutzbericht 2016 (S. 259–295) und in der bfv-themenreihe „Spionage gegen Deutschland – Aktuelle Entwicklungen" 2008.

11 Für die ausführlichen Diskussionen der vorliegenden Rechtsproblematik danke ich ausdrücklich meiner Kollegin *Susanne Knickmeier* (MPICC) und Frau *Gisela Graf* (BKA).

1.2.2 Strafbarkeit von Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext

Wissenschaftsspionage ist, wie die Wirtschaftsspionage, ein Staatsschutzdelikt. Sofern ein Staatsgeheimnis im Sinne von § 93 StGB betroffen ist, ergibt sich die Strafbarkeit aus §§ 94 ff. StGB, ansonsten kann eine geheimdienstliche Agententätigkeit gem. § 99 StGB gegeben sein.

Im Bereich der Konkurrenzausspähung im Wissenschaftskontext sind zwei Szenarien voneinander zu unterscheiden. Zum einen kann die Wissenschaftsorganisation Forschung im Einklang mit den Zielen des Art. 5 Abs. 3 GG entsprechend allein um die Erweiterung des Wissens willen verfolgen oder sie agiert im Rahmen der Auftragsforschung wie ein wirtschaftlicher Geschäftsbetrieb. In letzterem Fall kann die ansonsten öffentlich-rechtliche Körperschaft in einem wirtschaftlich ausgerichteten Teilbereich einem Unternehmen gleichgestellt werden, sodass § 23 GeschGehG (bis April 2019: §§ 17 ff. UWG)[12] Anwendung findet. Im ersten Fall konnte eine Strafbarkeit nach der alten Rechtslage daran scheitern, dass das Opfer kein Unternehmen nach § 2 Abs. 1 Nr. 6 UWG war, sowie am Wortlaut des Merkmals „Geschäfts- und Betriebsgeheimnis". Dessen Schutzwürdigkeit setzte stets ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung voraus. Zudem fungierte lange Zeit der Begriff „Unternehmensgeheimnis" als Oberkategorie für „Geschäfts- und Betriebsgeheimnisse".[13] Durch die EU-Richtlinie 2016/943[14], die in Deutschland durch das im April 2019 in Kraft getretene Gesetz zum Schutz von Geschäftsgeheimnissen umgesetzt wurde, ist dieser Punkt nun geklärt.

Im Ergebnis bleibt festzuhalten, dass Konkurrenzausspähung im Wissenschaftskontext mittlerweile unabhängig davon strafbar ist, ob die geschädigte Wissenschaftsorganisation im konkreten Einzelfall im Rahmen einer Auftragsforschung tätig war. Als Täter kommen sowohl andere Wissenschaftsorganisationen als auch Unternehmen in Betracht. Die Fallzahlen dürften bei beiden Tätergruppen äußerst gering sein. Eine andere Ansicht vertritt *Oehler,* der – ohne darauf näher einzugehen – jeden zu wissenschaftlichen Zwecken handelnden Täter in jedem Falle für straflos hält.[15]

---

12 Seit Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) entfallen die Regelungen der §§ 17 ff. UWG. Sie wurden inhaltlich nahezu unverändert in § 23 GeschGehG übernommen.

13 Vgl. *Ulmer* 1965, Rn. 305 f.

14 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, Abl. L 157, S. 1.

15 Vgl. *Oehler* 1971, S. 4.

1.2.3 Weitere mögliche Tatbestände

Neben der Anwendbarkeit von § 23 GeschGehG (bis April 2019: §§ 17 ff. UWG) besteht in Einzelfällen ein strafrechtlicher Schutz auch nach anderen strafrechtlichen Normen. Hier kommen insbesondere das Ausspähen von Daten (§ 202a StGB), die Verletzung von Privatgeheimnissen (§ 203 StGB) oder die Verletzung von Dienstgeheimnissen und besonderen Geheimhaltungspflichten (§ 353b StGB) in Betracht. Scheitern könnte die Strafbarkeit bei § 202a StGB an einem fehlenden technischen Angriff und bei §§ 203 ff. StGB an einer fehlenden Offenbarung oder Verwertung eines Privat-, Betriebs- oder Geschäftsgeheimnisses. Werden außerhalb der Auftragsforschung generierte Erkenntnisse einer Wissenschaftsorganisation von eigenen Mitarbeitern, gleich ob zu wissenschaftlichen oder zu wirtschaftlichen Zwecken, abgeschöpft bzw. weiterverwendet, scheinen Strafbarkeitslücken zu bestehen, die § 353b StGB nur im Falle einer Verbeamtung oder besonderen Verpflichtung oder ggf. § 106 UrhG (unerlaubte Verwertung urheberrechtlich geschützter Werke) auffängt. Sollten alle Tatbestände nicht greifen, z.B. dann, wenn ein Habilitand im Rahmen eines von der Wissenschaftsorganisation betriebenen Forschungsprojekts generierte Daten für seine eigene Habilitation verwendet, kämen nur noch Verstöße gegen Datenschutzvorschriften oder arbeitsrechtliche Treuepflichten in Betracht.

1.2.4 Anwendungsbereich der Tatbestände im Wissenschaftskontext

Der Anwendungsbereich der Konkurrenzausspähung im Wissenschaftskontext ist äußerst begrenzt, da nur Fälle, in denen geschädigte Wissenschaftsorganisationen im Bereich der Auftragsforschung von nicht staatlichen Akteuren ausspioniert wurden, erfasst sind. Bei der Wissenschaftsspionage, also der Ausforschung durch staatliche, vor allem ausländische nachrichtendienstliche Akteure, besteht eine ungleich größere Praxisrelevanz, vor allem wenn die Wissenschaftsorganisation im Bereich von Dual-Use-Gütern forscht.

2. Methode der Untersuchung

Im Rahmen des WiSKoS-Projekts wurde u.a. der Umgang deutscher Wissenschaftsorganisationen mit Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext untersucht. Methodisch wurden die durch Experteninterviews erhobenen Daten anhand einer qualitativen Inhaltsanalyse ausgewertet. Die leitenden Fragen, die auch der Kategorienbildung dienten, bezogen sich auf die wahrgenommene Bedrohung durch Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext, festgestellte Angriffe auf Wissenschaftsorganisationen sowie die Täter und ihr Vorgehen, die Kooperationsbereitschaft und Kooperationen mit staatlichen Stellen sowie untereinander das Schutzniveau und Präventionsmaßnahmen.

Für die Datenerhebung wurde ein für Unternehmen erstellter Interview-Leitfaden an die besondere Situation von Wissenschaftsorganisationen angepasst. Mit einem solchen Leitfaden steht dem Interviewer ein Instrument zur Verfügung, durch das gewährleistet sein soll, dass ähnliche Fragen gestellt werden, durch das aber auch die Offenheit erhalten bleibt, flexibel auf unvorhergesehene Informationen zu reagieren. Insgesamt wurden elf Interviews mit Wissenschaftsorganisationen geführt – sechs mit deutschen Wissenschaftsorganisationen und jeweils ein Interview mit einer Wissenschaftsorganisation aus den in *Modul 1* des WiSKoS-Projekts ausgewählten Vergleichsländern (Bulgarien, Dänemark, Österreich, Schweiz und Vereinigtes Königreich).[16] Bei der Wahl der Gesprächspartner wurde sowohl auf eine ausgewogene Verteilung zwischen universitären und außeruniversitären Einrichtungen als auch auf eine hierarchie- und funktionsübergreifende Einbeziehung möglicher Adressaten innerhalb dieser Institutionen geachtet. Dementsprechend wurden Datenschutz-, Sicherheits-, oder IT-Beauftragte ebenso interviewt wie Direktoren von Forschungseinrichtungen und Lehrstuhlinhaber. Die Interviews mit Gesprächspartnern aus Deutschland, Österreich und der Schweiz wurden von der Autorin selbst geführt. Die Interviews mit entsprechenden Funktionsträger in Bulgarien, Dänemark und dem Vereinigten Königreich wurden von ausgewiesenen Länderexperten geführt und in den ersten beiden Fällen ins Englische übersetzt. Die Interviews wurden sodann transkribiert, durch den Verbundpartner Fraunhofer ISI kodiert und von der Autorin analysiert. Aufgrund der geringen Anzahl lassen die Interviews allerdings keine allgemeingültigen Aussagen zu, bieten aber einen Einblick in die Problematik.

3. Phänomenologische Ergebnisse

Im folgenden Abschnitt werden die Wahrnehmung der Bedrohungslage durch die Interviewpartner sowie die Täter und ihre Modi Operandi aus erlebten Angriffen dargestellt.

3.1 Wahrnehmung der Bedrohungslage

Im Hinblick auf die wahrgenommene Bedrohungslage berichteten die Interviewpartner von aktuell laufenden aber auch abgeschlossenen Cyberattacken[17] gegen die jeweiligen Wissenschaftsorganisationen sowie von Fällen physischer Kriminalität,[18] bei denen es zum Diebstahl von Datenträgern kam. Der Interviewpartner aus dem Vereinigten Königreich betonte, dass allein der Umstand, dass relativ wenige Berichte über Wissenschaftsspionage in der Presse zu finden seien, nicht aussagekräftig bzgl. der Relevanz des Phänomens sei, da es unter Wissenschaftsorganisationen aus

---

16 Siehe *Carl et al.* 2017, S. 122–129, oder die Einleitung zum vorliegenden Band.

17 Interview AUT, Seq. 21; Interview UK, Seq. 10; Interview DE 1, Seq. 38–40 und 40–42.

18 Interview DE 5, Seq. 10–15; Interview DE 3, Seq. 5–8; Interview UK, Seq. 10.

verständlichen Gründen ernsthafte Vorbehalte gegenüber dem Publikmachen eigener Betroffenheit gebe.[19] Während die Befragten aus Österreich und dem Vereinigte Königreich eindrücklich von einem Gefühl konstanter Bedrohung berichteten, verwiesen die Gesprächspartner aus Bulgarien und Dänemark zwar darauf, dass es zahlreiche Einzelfälle gegeben habe, jedoch verdichteten sich diese Erfahrungen bei ihnen nicht zu einem Gefühl konstanter Bedrohung.

Einig waren sich die Befragten aus dem In- und Ausland, dass wirklich „gut gemachte" Angriffe, besonders von ausländischen Geheimdiensten, über das Internet oder auf anderem Wege zunächst kaum bemerkbar seien. Vor allem die Gefahren, die mit überzeugend erstellten Phishing-Mails oder der manipulativen Beeinflussung beim Social Engineering verbunden seien, sollten aus ihrer Sicht nicht unterschätzt werden.[20]

In keinem Interview unterschieden die Interviewpartner zwischen Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext, was die Praxisferne dieser rechtlichen Unterscheidung für die Wissenschaftspraxis zeigt.[21]

Die Interviews zeigen eine große Bandbreite an berichteten Erfahrungen in den Bereichen personeller, organisatorischer und infrastruktureller Sicherheit. Im Folgenden werden die Bedrohung, die den Berichten der Interviewpartner entsprechend von Innen- und Außentätern ausgeht, sowie präventive Handlungsansätze dargestellt.

3.2 Täter

Potentieller Täter kann nicht nur der unbekannte Dritte (Außentäter) sein, sondern auch ein (ehemaliger) Mitarbeiter (Innentäter).

3.2.1 Risiko Innentäter

Ein Innentäter ist nach Aussage des Bundesamts für Verfassungsschutz

> der Faktor mit dem höchsten Risikopotenzial, [da er] in der Regel über volle physische und virtuelle Zugangsmöglichkeiten zu Räumlichkeiten, Netzwerken und Daten-

---

19 "[…] my overall experience is such that people are reluctant to talk about these kinds of things, for all the obvious reasons. And particularly, organisations where, you know, there's been some impact to them as an organisation, because if they're a large organisation, public, it […] undermines confidence, creates uncertainty. All those things that, you know, that go with something of this nature. There are, obviously, have been cases, where we've seen, in the public domain, you know, earlier this year […]. But in terms of the detail, it's not always out there, it's not always published" (Interview UK, Seq. 16).

20 Interview DE 1, Seq. 38–40 und 40–42, Interview UK, Seq. 10.

21 Dieselbe Feststellung für den Wirtschaftskontext findet sich im vorliegenden Band in *Kapitel 4* von *Sonnen & Bollhöfer* (Staatliche Präventionsangebote für KMU), dort *Abschnitt 5.3* (Umsetzung mittelfristiger Maßnahmen) sowie *Abschnitt 5.3.5 (*Single Point of Contact).

> banken im Unternehmen [verfügt und] mit den notwendigen sozialen Kontaktmöglichkeiten ausgestattet [ist].[22]

Es wundert daher nicht, dass 70 % der Täter im Wirtschaftssektor aus dem betroffenen Unternehmen selbst kommen sollen[23] – vergleichbare Zahlen für den Wissenschaftssektor existieren jedoch nicht. Die geführten Interviews zeigten, dass die deutschen und europäischen Wissenschaftsorganisationen die Bedrohung durch Innentäter sehr unterschiedlich einschätzen. Ein Interviewpartner hielt die Gefahr durch Innentäter für größer als durch Außentäter, auch weil seinem Eindruck nach mit der Gefährdung aus dem Inneren einer Organisation nachlässiger umgegangen werde.[24] Ein anderer Gesprächspartner ergänzte, dass man sich eingestehen müsse, dass vor allem eigene Mitarbeiter die Organisation schwer schädigen können.[25] Gegen Angriffe aus dem „maximal inneren Bereich", also z.B. durch hauseigene Administratoren, könne man sich kaum schützen.[26] Sobald ein Bewerber den Auswahlprozess überstanden habe, so die Interviewpartner (DE 4) weiter, könne sich die „Bedrohung durch einen Innentäter realisieren".[27] Entscheidender Zeitpunkt sei dabei die Erteilung von Zugriffsrechten auf Forschungsdaten.[28] Dem ist hinzuzufügen, dass selbst ehrliche Mitarbeiter zu einem Risiko für eine Wissenschaftsorganisation werden können, da stets Raum für menschliches Versagen oder Social Engineering besteht. Mit Blick auf Ersteres sprach der dänische Interviewpartner aus, was in vielen Gesprächen mitschwang:

---

22 Bundesamt für Verfassungsschutz 2015, S. 6; für den Wissenschaftskontext ebenso *Boos*, S. 63.

23 *Röder*, S. 3; siehe dazu auch *Bollhöfer & Jäger* 2018, S. 39, 40.

24 Interview CH, Seq. 34.

25 Interview AUT, Seq. 18.

26 Interview DE 4, Seq. 31–32.

27 Interview DE 4, Seq. 31–32. Zu bedenken ist jedoch, dass ein Bewerber schon mit der Bewerbungsmail Schadsoftware ins Unternehmen einbringen oder während des Auswahlgesprächs Zugang zu Forschungsergebnissen, z.B. über vor Ort zugängliche und ungeschützte Datenträger, erhalten kann.

28 Ein Interviewpartner sprach das dabei bestehende Spannungsverhältnis direkt an: „Aber es ist natürlich so, dass nicht jeder auf den Server zugreifen kann, aber dass Mitarbeiter dann das Zugriffsrecht bekommen. Im Prinzip muss man das dann an irgendeiner Stelle tun, wenn man mit Leuten zusammenarbeitet. Man kann es nicht machen ohne dass auch sie Zugriff haben auf die Rechner mit denen man arbeitet. […] Auf der anderen Seite ist es halt so, dass man vielleicht ein paar Wochen mehr warten kann, bevor man einem Neuen, der dazu kommt, den Zugriff auf den Rechner gestattet. Aber damit er irgendwann richtig arbeiten kann, muss man das natürlich tun. Also, ich denke, dass es eigentlich nicht schlecht gelaufen ist. Letzten Endes kann man so etwas nie zu hundert Prozent unterbinden. Aber wenn man es zu 99,999 % absichern wollte, dann würde es auch die Forschung und die Arbeit extrem behindern. Also das muss man ja auch gegenseitig abwägen" (Interview DE 3, Seq. 25, 26).

> Well-known vulnerabilities that have been addressed remain open because employees "don't use their brains.[29]

Soweit sie für eine potenzielle Bedrohung durch Innentäter grundsätzlich sensibilisiert waren, nahmen die einzelnen Wissenschaftsorganisationen die Risiken in den unterschiedlichen Phasen des Personaleinsatzes (von der Bewerbung bis zum Ausscheiden) unterschiedlich wahr und verfolgten dementsprechend eine individuelle Schwerpunktsetzung bei der Prävention. So hinterfragten einige Wissenschaftsorganisationen eingehende Bewerbungen kritisch, beobachteten die vertraglichen Beziehungen und etwaige Verhaltensänderungen des Stammpersonals und verfolgten teilweise nach Vertragsende die weitere Karriere ihrer ehemaligen Mitarbeiter, insbesondere bei einem Wechsel in die Industrie oder der Rückkehr ins Heimatland. Im Hinblick auf Bewerbungen betonte ein deutscher Interviewpartner, dass in seiner Institution zwar grundsätzlich Regeln zur Bearbeitung bestünden, die den Blick für einen sensiblen Umgang mit Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext schärften, jedoch besonders bei Bewerbern, die staatlicherseits mit einer ‚Legende' ausgestattet werden, fehleranfällig seien. Verdächtig würden solche Bewerber vor allem dann, wenn sie nicht die in ihrem Arbeitsbereich geforderten Leistungen erbrächten, obwohl dies aufgrund ihrer Zeugnisse zu erwarten gewesen wäre. Insgesamt sei es jedoch kaum realistisch, die Bedrohung durch Wissenschaftsspionage aufzufangen:

> Aber dem systematisch nachzugehen, wissen Sie das Problem ist, wenn jemand wirklich staatlicherseits geschickt wird, und der würde eine Legende aufgebaut bekommen, damit er da auch stromlinienförmig durch die Bewerbung geht, mit gefälschten Uni-Zeugnissen und Ähnliches, dann ist das so gut gemacht, dass wir mit den eigenen Mitteln der [Institution] keine Chance haben, das zu enttarnen. Aber da gibt es auch Listen, wenn ein Wissenschaftler, also das sind in der Regel die Doktoranden die sich bewerben, auffällt mit gefälschten Zeugnissen, was schon vorgekommen ist, dann tauschen sich die [unteren Organisationseinheiten] untereinander aus.[30]

Bezüglich der Verhaltensänderung von Mitarbeitern wurde häufig auf die Gefahren des Social Engineering eingegangen.[31] Ein Interviewpartner betonte, dass zwar die Existenz einer Vertrauensbasis wichtig und richtig sei, aber dass dennoch ein Bewusstsein für dieses Risiko bestehen müsse und die Wissenschaft in diesem Punkt noch sehr blauäugig sei.[32] Eine mögliche Maßnahme ist die Beobachtung von Karrieren in der Wissenschaft über das Vertragsende hinaus. Dies kann einerseits dem Umstand geschuldet sein, dass man auch künftig in ähnlichen Forschungsfeldern aktiv ist und weiterhin Berührungspunkte bestehen; andererseits kann so beobachtet

---

29 Interview DK, Seq. 13.

30 Interview DE 1, Seq. 101–102.

31 Interview DE, 5, Seq. 33.

32 Interview CH, Seq. 46–47.

werden, welches Wissen nach einem Wechsel in die Industrie mitgenommen wurde, was ‚Rückkehrer' in ihren Heimatländern forschen und ob Vorschriften zu Dual Use oder Proliferation umgangen wurden. Ein Interviewpartner wies darauf hin, dass besonders die Mitnahme von Know-how durch ausscheidende Mitarbeiter ein Problem sei. Man versuche durch Vertragsmanagement darauf zu reagieren.[33]

Einen eigenen Themenkomplex im Rahmen der Spionageproblematik im Wissenschaftskontext stellen Gastwissenschaftler dar. Im Wissenschaftssektor ist es nicht nur üblich, sondern gerade Ausdruck von Forschungsstärke und Attraktivität eines Standorts, wenn dieser viele Gastwissenschaftler anzieht. Nicht selten wird die Vergabe von Drittmitteln an internationale Zusammenarbeit geknüpft, werden Gastwissenschaftlerzahlen beobachtet und insbesondere Alexander von Humboldt-Stipendiaten getrennt gezählt sowie auf Institutswebseiten hervorgehoben.[34]

Zu entscheiden, ob Gastwissenschaftler, von denen eine potenzielle Spionagegefahr ausgehen könnte, eher der Gruppe der Innen- oder der Außentäter zuzuordnen sind, ist nicht einfach. Einerseits ist ihre Arbeit zeitlich begrenzt und dieser Personalbereich von einer hohen Fluktuation geprägt, andererseits erhalten sie häufig Zugangsberechtigungen für die physische und digitale Infrastruktur, sodass sie im internationalen Forschungsbetrieb vom Stammpersonal kaum zu unterscheiden sind. Die Interviewpartner berichteten häufig von einem identischen Risikoniveau von Stammpersonal und Gastwissenschaftlern, sodass Letztere im Folgenden auch der Gruppe der Innentäter zugeordnet werden. Dennoch nehmen sie insoweit eine Sonderrolle ein, als ihr Hintergrund und ihre Qualifikationen häufig nicht so gründlich und umfangreich geprüft werden bzw. werden können, wie dies bei der Stammbelegschaft der Fall ist.

Ein deutscher Interviewpartner fasste das Problem von Gastwissenschaftlern folgendermaßen zusammen und benannte in Teilen eigene Lösungsstrategien:

> Gastwissenschaftler, wie geflüchtete Forscher, stellen ein Problem dar. Vermeiden kann man dieses aber nicht, wegen des durch mangelnde internationale Projektanknüpfung eintretenden Verlusts. Gastwissenschaftler aus Embargoländern und z.B. Syrien und Afghanistan erhalten keine Aufbauskizzen von Gerätschaften. Bei chinesischen Wissenschaftlern wird manchmal beobachtet, dass diese nicht nur Forscher, sondern auch Kräfte zur Führung der Wissenschaftler mitbringen.[35]

Auffällig ist, dass nahezu alle Interviewpartner in diesem Zusammenhang von sich aus immer wieder dieselben Staaten ins Spiel brachten, und zwar China, Russland

---

33 Interview DE 6, Seq. 10–11.

34 Zur Veranschaulichung des hohen Stellenwerts von Gastwissenschaftlern in Deutschland soll die Institutswebpage der Ruhr-Universität Bochum ausreichen: www.ruhr-uni-bochum.de/universitaetsprogramme/index.html [04.04.2019].

35 Interview DE 6, Seq. 10–12.

und Iran.[36] Das Ausmaß von Spionageaktivitäten seitens Chinas beschrieb ein Interviewpartner folgendermaßen:

> […] es ist ein völlig normaler Prozess, dass bei uns viele Gäste sind. Die größte Gruppe in der [Institution] sind Chinesen, etwa 700–800 Chinesen müssten bei uns sein. Dass da Spione dabei sind, davon bin ich überzeugt, ich weiß aus Gesprächen mit Chinesen über die Spionagesituation. Es gibt keinen chinesischen Post-Doc, der nach Deutschland geht zum Forschen, der nicht einen Auftrag hat, was er ausspionieren soll. Da gehe ich von einer 100-%-Quote aus […] Und die werden wohl eingeladen von staatlichen Stellen zu Gesprächen und dann wird ihnen erzählt, was sie alles für den Staat tun können […].[37]

Andere Interviewpartner berichteten von der Existenz als Forschungseinrichtung getarnter ausländischer Unternehmen.[38] Dies deckt sich mit behördlichen Beobachtungen, die gerade auch im Wissenschaftskontext auf die zuvor genannten Länder hinweisen und sich daran anschließende Risiken im Bereich der Proliferation aufzeigen.[39]

3.2.2 Risiko Außentäter

Auf das Risiko, durch Außentäter ausspioniert zu werden, wurde ebenfalls häufig hingewiesen. Für die Interviewpartner spielten Cyberangriffe, Social Engineering, Phishing usw. eine größere Rolle als physische Angriffe. Die Zusammenfassung des österreichischen Gesprächspartners bezüglich seiner Wahrnehmung der Bedrohungslage im Cyberbereich ist repräsentativ für den Grundtenor der Interviews in diesem Zusammenhang:

---

36 China: Interview AUT Seq. 29; Interview DK, Seq. 11; Interview UK, Seq. 111 und 113; Interview DE 1, Seq. 48, 53, 55 und 57; Interview DE 3, Seq. 6, 16, 67, 77 und 82; Interview DE 6, Seq. 10–12; Interview DE 3, Seq. 6, 8: „Da hatten wir einen chinesischen Gast, der saß an der Universität und hier im angemieteten Institut. Er saß in meinem Bereich der Universität. Also bei uns ist es so, dass die Rechner und Server von den eigenen Mitarbeitern gewartet werden. Das machen dann immer die, die sich dafür interessieren. Und die haben gemerkt, dass er [der chinesische Gast] nachts alle möglichen Daten nach China gesendet hat. Das konnten sie auch verfolgen. […] Damals hatten wir den bayrischen Verfassungsschutz eingeschaltet. Ich weiß nicht mehr, wer es uns geraten hatte. Jedenfalls sind sie dann gekommen und haben ihn ausgewiesen. Wir haben dann gesagt, dass wir mit so jemandem nicht mehr zusammenarbeiten wollen. Er hat dann auch seine Aufenthaltsgenehmigung entzogen bekommen." Ebenfalls in Interview DE 6 wurde darauf hingewiesen, dass China ein verstärktes Interesse an einem der [institutseigenen] Forschungsbereiche habe und merklich versuche, sämtliche Forschungsergebnisse zu erhalten. Ähnliche Aussagen fanden sich auch im Interview UK, Seq. 14.

Russland: Interview AUT, Seq. 13; Interview DE 1, Seq. 53; Interview DE 3, Seq. 42, 49 und 77; Iran: Interview DE 1, Seq. 40, 46, 61, 183; Interview DE 3, Seq. 67 und 69; Interview DE 6, Seq. 21.

37 Interview DE 1, Seq. 55.

38 Interview DE 5, Seq. 32.

39 Verfassungsschutzbericht 2014, S. 149, 155, Verfassungsschutzbericht 2016, S. 281.

> Ich hätte eher Angst davor – auch vor dem Hintergrund, dass wir im Cyberkontext arbeiten – dass die kriminelle Welt aus dem Ausland angreift. Also die, die damit Geld verdienen. Organisierte Kriminalität. Da überlegen wir uns auch neue Methoden/Algorithmen, um Cyber-Angriffe zu identifizieren. Oder wir machen Verschlüsselungsverfahren, um Cloud-Anmeldungen sicher zu machen. Externe Betriebsspionage würde ich als den Super-GAU bezeichnen.[40]

Als Handlungsansatz für diese Problematik wurde von den Interviewten häufig die Aufrüstung der IT-Systeme genannt; andere hofften, dass Außentäter durch die eigenen Wissenschaftler abgewehrt werden. So wurde betont, dass gerade Angriffe im Spear-Phishing-Bereich[41] mittels Social Engineering dadurch verhindert werden können, dass Abweichungen im Kommunikationsmuster von den Wissenschaftlern als ungewöhnliches Verhalten erkannt und hinterfragt werden. [42]

Von physischer Kriminalität wurde vor allem in Form des unerlaubten Fotografierens auf dem Institutsgelände sowie dem Diebstahl von Laptops mit Forschungsdaten, Prototypen und Geräteskizzen berichtet. [43] Hinsichtlich von Präventionsmaßnahmen sind die Wissenschaftsorganisationen laut den Berichten unterschiedlich aufgestellt. Während manche Zugangskontrollen zum Gelände beschrieben,[44] schlossen das andere aufgrund der Wissenschaftsfreiheit, die den ungehinderten Zugang der Öffentlichkeit voraussetze, explizit aus.[45] Gleichzeitig wurde von bestehendem Misstrauen

---

40 Interview AUT, Seq. 21; ähnlich auch Interview DE 1, Seq. 40, 42.

41 Als „Spear-Phishing" wird ein Betrugsversuch per E-Mail bezeichnet, dessen Ziel der unerlaubte Zugriff auf Daten ist.

42 Ein Beispiel: „Da bekommt ein Wissenschaftler eine Mail, von jemanden, den er kennt, und in der Mail steht drin, ich mache da ein Forschungsprojekt und du hast da gerade ein Paper gemacht und könnte ich dieses Paper haben, weil das passt ganz gut in meinen Forschungskontext. Das Ganze ist dadurch aufgefallen, weil die beiden hatten schon zusammen publiziert. In dem einen Fall, wo die [Institution 1] betroffen war, war der Wissenschaftler in [Ort 1] und der vermeintliche Absender an der [Institution 2] hier in [Ort 2]. Und die hatten schon zusammen publiziert und das ist aufgefallen, weil die gerade dabei waren, ein Paper zu machen und der Wissenschaftler in [Ort 1] den in [Ort 2] gefragt hat, warum sagst du mir das nicht am Telefon, wieso schickst du mir dafür eine E-Mail? Und dann war in der Mail ein Link drin und falls dich das, was ich gerade mache, auch interessiert, hier ist der Link, dass du es sehen kannst. Und der Link ging auf ein Paper bei Springer-Link über die örtliche Bibliotheksmaske zum Anmelden. Da sollte das Passwort abgegriffen werden und diese Maske war nachgebaut, weil in der eigentlichen URL war ein kleiner Buchstabe. Die [Institution] hat Adressen @[institution].de und da war in [Ort] das letzte ‚e' durch ein ‚i' ersetzt. 30–40 Wissenschaftler in Deutschland haben solche Mails bekommen, die haben teilweise auf die Mails geantwortet und haben auf diese Antwort wieder eine Antwort bekommen. […] Das ist richtig gut gemacht und sowas ist für die das normale Geschäft" (Interview DE 1, Seq. 42).

43 Interview DE 5, Seq. 10–15.

44 So z.B. Interview DE 3 und 6 sowie AUT.

45 Interview DE 5, Seq. 18.

gegenüber bestimmten Gruppen von Akteuren berichtet und dass die Nationalität der Gastwissenschaftler bei Entscheidungen des Ob und darüber, an welcher Stelle gemeinsame Forschung ansetzen könne genauestens reflektiert werde.[46] Berücksichtigt würde dabei auch die schon oben genannte Praxis in gewissen Herkunftsländern, Unternehmen oder gar Geheimdienste als Forschungsinstitute zu tarnen.[47]

Als ungelöstes Problem hinsichtlich der Gefahr von Außentätern wurden in den Interviews wiederholt internationale Forschungskooperationen genannt. Im Sinne der Wissenschaftsfreiheit ist es den Wissenschaftsorganisationen freigestellt, wen sie als Kooperationspartner wählen, wobei nicht immer das notwendige Bewusstsein bezüglich etwaiger Datenausspähung bei den kooperierenden Wissenschaftlern vorhanden ist. Ein deutscher Interviewpartner wies auf den sich aus bi- und internationalen Kooperationsverträgen der Bundesregierung ergebenden Zwang zur internationalen Zusammenarbeit hin, wodurch Wissenschaftler gegebenenfalls trotz ihres Bewusstseins für Spionagerisiken zur Kooperation angehalten werden, um Forschungsgelder zu erhalten. Er betonte, dass der deutsche Staat so das Ausspionieren von Forschungsergebnissen im eigenen Land finanziere.[48]

3.3 Modi Operandi

In den vorhergehenden Abschnitten wurden diverse Modi Operandi der Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext bereits erwähnt. Detaillierte Ausführungen zur den entsprechenden Vorgehensweisen im Bereich der Wirtschaft finden sich in *Kapitel 1* des vorliegenden Bandes.[49] Da diese in den Wissenschaftskontext übertragbar sind, sei hier nur zusammenfassend darauf hingewiesen, dass sich beim unerlaubten Datenabfluss im Wissenschaftskontext zwei grundsätzliche Vorgehensweisen unterscheiden lassen: Die Täter können im Wege klassischer, physischer Kriminalität vorgehen oder im Cyberspace operieren. So können Angreifer entweder den Weg der Cyberkriminalität mit Botnetzen, Phishing, DoS-Angriffen etc. einschlagen oder Daten vor Ort durch eigene Endgeräte wie Wanzen, Kameras usw. erfassen bzw. Datenträger, Skizzen und Rezepturen kopieren oder fotografieren. All diese Vorgehensweisen fallen in den Bereich der technischen Informationsbeschaffung, sogenannte TECHINT (Technical Intelligence). Die andere mögliche Vorgehensweise stellt die persönliche Kontaktaufnahme

---

46 Interview DE 5, Seq. 27.

47 Interview DE 5, Seq. 27; Prüfung, ob und wie Gastwissenschaftler aus bestimmten Nationalitäten in Forschungsprojekte kooperieren können, Interview AUT, Seq. 20–21. Dieses Risiko betonten auch die assoziierten Partner im WiSKoS-Projekt und verwiesen dabei insbesondere auf China.

48 Interview DE 5, Seq. 26.

49 *Wallwaey & Waldheim,* Der „typische" Spionagefall? Ergebnisse einer Literaturanalyse, dort *Abschnitt 3.3* (Modi Operandi).

bzw. Anwerbung von Personen, sogenannte HUMINT (Human Intelligence), dar, die sowohl online als auch offline erfolgen kann. Eine Beschreibung der Phänomenologie anhand ausgewerteter Strafakten und exemplarischer Fallstudien findet sich in *Kapitel 2* dieses Bandes.[50]

4. Schutzniveau und Schutzbedarf in Wissenschaftsorganisationen

Bezugnehmend auf die beschriebenen phänomenologischen Ergebnisse stellt sich die Frage, wie sich Wissenschaftsorganisationen vor einem Vorfall schützen, wie sie nach einem Vorfall vorgehen, welche Erfahrungen sie mit Kooperationen gemacht haben und welcher Schutzbedarf besteht.

4.1 Status Quo des Schutzniveaus in Wissenschaftsorganisationen

Die unterschiedlichen Wahrnehmungen der Bedrohungslage spiegeln sich bei den befragten Wissenschaftsorganisationen in den unterschiedlichen Schutzniveaus bei der Abwehr von Innen- bzw. Außentätern sowie von Cyberangriffen und physischer Kriminalität wider. Intern sind Wissenschaftsorganisationen nach dem Eindruck eines Interviewpartners unterschiedlich, „von fast gar nicht bis ziemlich gut“ geschützt.[51] Die gewählten Schutzmaßnahmen scheinen dabei nicht immer mit der Attraktivität des potenziellen Angriffsziels korrespondierten.

In Bezug auf physische Schutzvorkehrungen in den Forschungseinrichtungen findet sich in den Darstellungen der Gesprächspartner, wie z.T. schon erwähnt, ein breites Spektrum: von offenen Türen in den Gebäuden, Laboren und Büros der Forscher, über Schließsysteme, vor allem für Serverräume,[52] bis hin zu Zugangskontrollen mit Lichtbildausweis und Taschenkontrolle. Während ein deutscher Interviewpartner, dessen Forschungsinstitution in der Vergangenheit bereits massiv Opfer von Wissenschaftsspionage geworden war, mit Verweis auf die Wissenschaftsfreiheit bekundete, dass es einen besonderen Zugangsschutz der Abteilung nicht gebe,[53]

---

50 *Knickmeier*, Wirtschaftsspionage und Konkurrenzausspähung kennen keine Grenzen, dort *Abschnitt 4.5* (Informationsabfluss).

51 Interview DE 1, Seq. 38–40.

52 Ein solches Schließsystem für Serverräume haben laut Aussage der Interviewpartner alle vertretenen Institutionen implementiert, teilweise mit massiven physischen Ertüchtigungen der Räumlichkeiten. Einer der Befragten beschrieb die Vorkehrungen so: „[Es gibt ein] Funkdings und ein Passwort. Die Türen sind nicht markiert und auch von außen alles stabile Wände. Mehrfach mit Metall. Kann man nicht von außen einfach so eine Wand einreißen. Das ist schon gut.” Den Funktaster und das Passwort besäßen nur drei Personen (Interview DE 4, Seq. 38 und 41).

53 Interview DE 5, Seq. 25–26.

existieren an anderen deutschen Einrichtungen entsprechende Vorkehrungen. Zum Beispiel werden teilweise die Gelände sowie die Forschungsstätten mit großem Aufwand wegen des Risikos des Verlusts hochsensibler Daten gesichert. Für Gastwissenschaftler gebe es ein Gäste-WLAN oder die Möglichkeit der Nutzung des Internet-Zugangsservices eduroam. Zudem seien IT-Konzepte auf der Grundlage der BSI-Richtlinien erstellt worden.[54]

Der dänische Interviewpartner erläuterte das an seiner Institution bestehende, nach Orten und Hierarchieebenen abgestufte Zugangssystem,[55] bei dem die physischen Schutzvorkehrungen durch technische Maßnahmen im IT-Bereich flankiert werden. Für den IT-Bereich gaben alle Interviewpartner an, ihre Systeme *de lege artis* zu schützen. Zum Beispiel würden IT-Komponenten anhand internationaler Zertifizierungen ausgewählt. Weitere mögliche Maßnahmen sind die Wahl eines nationalen IT-Providers, der bekannten Datenschutzregeln unterliegt, die Teilnahme an Veranstaltungen branchenspezifischer Netzwerke oder die Durchführung von Penetrationstests durch das Deutsche Forschungsnetzwerk (DFN).[56]

Im Vergleich zum Schutz von Unternehmensnetzwerken stehen gerade die IT-Systeme von Universitäten vor besonderen Herausforderungen. Ein Interviewpartner mit IT-Hintergrund erklärte:

> Da gibt natürlich so ein Uni-Netz sehr viel her, weil wir ja offen sind. Anders als ein Firmennetz haben wir nicht so strikte Firewall-Regeln, weil ja auch diverse Forschungsdienste ermöglicht werden sollen und wir sonst gar nicht mehr hinterherkämen, das alles zu pflegen und freizuschalten. Da muss man differenzieren, wo Sie die Schwerpunkte sehen würden.[57]

Trotz der Erkenntnis von Lücken wurde organisatorisch nicht nachjustiert. So analysierte der Gesprächspartner aus dem vorangegangenen Beispiel weiter:

> Entsprechend ist da natürlich auch das Schutzniveau unterschiedlich stark ausgeprägt. Wir können relativ viel sagen über die Maßnahmen, die wir hier bei uns ergriffen haben, wissen aber selber nicht immer sehr präzise, was die einzelnen Fakultäten und Lehrstühle vor Ort gemacht haben. Wir wissen auch nicht genau, wie die einzelnen Daten verteilt sind. Bei Forschungsdaten oder Daten im Rahmen von Firmenkooperationen also, wie viel davon wirklich bei uns liegt und wie viel bei den einzelnen Fakultäten und Lehrstühlen noch in kleinen Serverräumen vor Ort ist. Insofern ist das relativ schwierig zu beantworten.[58]

---

54 Interview DE 6, Seq. 16–17.

55 Interview DK, Seq. 90–97.

56 Interview DE 6, Seq. 33–37.

57 Interview DE 2, Seq. 10.

58 Interview DE 2, Seq. 10.

Die fehlende Kenntnis von bzw. Abstimmung mit den Handlungen anderer Abteilungen fanden die Interviewpartner häufig an den Schnittstellen zwischen technisch-organisatorischen sowie organisatorisch-personellen Schutzmaßnahmen vor. Dies betrifft bei der Ersteren z.B. mögliche Vorgaben für Wissenschaftler zur Sicherung von Daten auf besonders gesicherten Laufwerken. Ein deutscher Interviewpartner räumte zu der Frage ein:

> Wir haben noch keine Vorgaben. Das ist noch ein Defizit. Wir haben es auch erkannt.[59]

Im Hinblick auf die organisatorisch-personelle Schnittstelle wurden, wie bereits erwähnt, vor allem Bewerberüberprüfungen und Probleme bei der Gastwissenschaftlerauswahl angesprochen, bei der nachhaltiges Misstrauen gegenüber bestimmten Nationalitäten bestehe.[60]

Organisatorische Schutzmaßnahmen gibt es in unterschiedlichster Gestalt mit einer großen Spannweite beim Schutzniveau. Vorbildlich erscheint in diesem Kontext ein einheitliches Sicherheitskonzept, wie es der dänische Interviewpartner vorstellte.[61] Ihm zufolge besteht das Konzept darin, eine vorab bestimmte und geschulte „rapid reaction force" zu implementieren, die sich aus allen Fakultäten und Verwaltungsabteilungen rekrutiert, sich an den reellen Gegebenheiten vor Ort und den Kompetenzen der Mitwirkenden orientiert und deren Entwicklung durch externe Berater begleitet wird.[62]

Darüber hinaus wurden folgende Einzelmaßnahmen von den befragten Experten für sinnvoll erachtet und scheinen ohne großen Aufwand umsetzbar zu sein:

- Prüfsystem für Bewerber,[63] ggf. inkl. Sicherheitsüberprüfung;[64]
- Umgangsregeln für die Überprüfung von Gastwissenschaftlern;[65]

---

59 Interview DE 4, Seq. 29.

60 Interview DE 5, Seq. 27–28; keine Aufnahme von Gastwissenschaftlern in sensible Projekte, Interview AUT, Seq. 20–21; für Details zur Gastwissenschaftlerproblematik siehe oben unter *3.1.1*, „Risiko Innentäter".

61 In Form eines einheitlichen Sicherheitskonzeptes (Interview DK, Seq. 79–81).

62 Interview DK, Seq. 25–27: "Such an emergency response plan should be mandatory for any organisation. Such plans are often designed from a theoretical, abstract, idealised idea. The [institution]'s plan, in contrast, was designed with a pragmatic, practical, concrete focus, starting with the actual ingredients and people that are in place; not what *should* have been in place. The plan was designed in collaboration with specialised external consultants. It combines both directors and lower-level people with the requisite technical knowledge. Roles and reporting lines are pre-assigned." Eine ähnliche Darstellung findet sich auch in Seq. 79–81 desselben Interviews.

63 Interview BG, Seq. 26.

64 Interview AUT, Seq. 20–21.

65 Interview DE 6, Seq. 16, 25.

- in seltenen Fällen keine Zulassung von Gastwissenschaftlern und Praktikanten zu sensiblen Projekten;[66]
- Verschwiegenheitsverpflichtungen für Mitarbeiter;[67]
- Sensibilisierung der Mitarbeiter mittels Schulungen;[68]
- ein technisches Sicherheitskonzept (limitierte Zugriffsrechte auf Laufwerke und Daten sowie Nutzung von SharePoint-Servern);[69]
- Räumlichkeiten mit Zutrittskontrollen;[70]
- Zugriffskontrolle inkl. Freigabeprozedur für Dokumente;[71]
- Verbot des Mitbringens eigener elektronischer Geräte (sog. Bring Your Own Device – BYOD);
- regelmäßige Erfassung der (selbst ausgegebenen) Hardware;[72]
- Ranking der Sicherheitsbedürftigkeit der Projekte;[73]
- ggf. keine Aufnahme sensibler Projekte in institutsweite IT-Systeme;[74]
- Restriktion des Zugangs zu Informationen nach dem Need-to-know-Prinzip[75];
- Sicherheitsvorschriften zum Umgang mit sensiblen Daten,[76] z.B. die Vorgabe, solche Daten nicht offen per E-Mail zu verschicken und die Nutzung von Keywords zu vermeiden[77]; sowie
- der Ausschluss „gewisser Nationen“ bei der Forschung im Bereich von Dual-Use-Gütern.[78]

Zusammenfassend zeigen die Aussagen der Experten, dass zwar organisatorische, technische und personelle Schutzmaßnahmen ergriffen werden, diese aber noch den Charakter von Einzelmaßnahmen haben, also wenig miteinander verknüpft sind.

---

66 Interview AUT, Seq. 20–21.

67 Interview BG, 26–31.

68 Interview DE 1, Seq. 106.

69 Interview DE 6, Seq. 24–31 und 33–37.

70 Interview AUT, Seq. 20–21.

71 Interview AUT, Seq. 20–21.

72 Interview DE 6, Seq. 17.

73 Interview AUT, Seq. 20–21.

74 Interview AUT, Seq. 20–21.

75 Interview UK, Seq. 53–55.

76 Interview DE 6, Seq. 16–17, 24–31 und 33–37.

77 Interview BG, 26–31.

78 Interview DE 5, Seq. 19–21; Interview 6, Seq. 5.

Des Weiteren sind Schutzbedürftigkeit und Schutzniveau bisher nicht überall aufeinander abgestimmt.

4.2 Vorgehen der Betroffenen bei einem konkreten Vorfall

Über das Vorgehen bei einem konkreten Vorfall machten die betroffenen Wissenschaftsorganisationen nur wenige Angaben, zum Beispiel über die Entdeckung eines Vorfalls, den Schaden, das kurz-, mittel- und langfristige Vorgehen sowie über bestehende Kooperationen mit Behörden bzw. anderen Wissenschaftsorganisationen.

4.2.1 Entdeckung des Vorfalls

Aufgedeckt wurden Vorfälle z.B. aufgrund des Abflusses großer Datenmengen[79] oder der Meldung eines Mitarbeiters über einen fehlenden Laptop[80] bzw. von Systemstörungen,[81] oder auch aufgrund von Verstößen gegen die Nutzungsordnung für Großgeräte [82] oder weil Forschungsergebnisse plötzlich bei einer konkurrierenden Wissenschaftsorganisation auftauchten.[83] In einem Fall wurde ein Interviewpartner vom Verfassungsschutz über die eigene Betroffenheit informiert.[84]

4.2.2 Schaden

Bezüglich der eingetretenen Schadensarten finden zwei unterschiedliche Schadenskomponenten Berücksichtigung: der finanzielle Schaden, der auch Personalkosten umfasst, und der Imageschaden. Letzterer wurde als besonders gravierend empfunden, da er künftige Forschung auf Drittmittelbasis seitens der Behörden oder der Industrie beeinträchtigen kann:

> Zum prinzipiellen Thema der Sicherheit in Industrie, Wissenschaft und Forschung ist zu sagen, dass, sobald man sich fahrlässigen Umgang mit Daten oder das Bestehen von Datenlecks vorwerfen lassen muss, ein Vertrauensverlust eintritt, der sich nicht einfach wieder umkehren lässt. Man verliert die Vertrauensbasis, um im Zusammenhang mit besonderen und vertraulichen Daten mit Industriepartnern zusammenarbeiten zu können. Das wäre der Super-GAU.[85]

---

79 Interview DE 1, Seq. 7, 16, 40; Interview DE 3, Seq. 12 und 83; Interview DE 4, Seq. 8.

80 Interview DE 5, Seq. 5–6 und 10–11. Zwei andere Interviewpartner erklärten hingegen, dass das Verschwinden von Laptops an ihren Institutionen nicht auffiele (Interview DE 1, Seq. 70 und Interview DE 4, Seq. 45).

81 Interview DK, Seq. 21.

82 Interview DE 6, Seq. 13–14.

83 Interview CH, Seq. 17–18.

84 Interview DE 3, Seq. 27–38 und 42–45.

85 Interview AUT, Seq. 37; in eine ähnliche Richtung ging auch die folgende Aussage: „Ich meine, im Prinzip sprechen wir von Schwachstellen, die man offenbar hat in der eigenen

Ebenfalls genannt wurden der finanzielle Schaden aufgrund des Verlustes eines Geräts,[86] fehlinvestierte Steuergelder beim Verlust von Ergebnissen aus der Grundlagenforschung,[87] steigende Personalkosten für die Wiederherstellung oder Neugenerierung verlorener Daten[88] oder der Arbeitsaufwand zur Bearbeitung des ursprünglichen Schadensfalls (von der Anzeige und deren Bearbeitung über das Nachfragen bei der Behörde, die Meldung an die Leitungsebene der Wissenschaftsorganisation bis zur Bearbeitung der Endmeldung).[89]

In den Interviews fand sich aber auch vielfach die Feststellung, dass der Schaden gar nicht bzw. noch nicht beziffert werden könne.[90] Besonders schwierig sei die Feststellung eines Schadens, wenn es keinen unmittelbaren inhaltlichen und zeitlichen Zusammenhang zwischen dem Angriff und dem schädigenden Ereignis gebe:

> Also wir müssen davon ausgehen, dass, wenn sich das bestätigt, dass es ein Angriff war, dann sind mit Sicherheit Informationen abgeflossen. Aber welche, wie und ob das einen zurückwirft, ob die Chinesen dadurch technologisch bei der Fusionsforschung aufholen können oder nicht, das ist schwer zu bewerten. Vielleicht in fünf Jahren bis zehn Jahren.[91]

Einige Interviewpartner vertraten die Auffassung, dass kein Schaden eingetreten sein könne, wenn das Ziel, die Forschung im Interesse der Allgemeinheit voranzutreiben, erreicht worden sei – selbst wenn Daten abhandengekommen sind und diese durch Dritte veröffentlicht wurden.[92] Vor allem die IT- und Sicherheitsbeauftragten

---

Institution, wenn so etwas passiert […], dass man so einer Institution mit größerer Vorsicht begegnet, das scheint mir dann berechtigt" (Interview CH, Seq. 27).

86 Interview DE 5, Seq. 16.

87 Interview AUT, Seq. 37.

88 Sofern Daten, wie im Bereich der Forschung üblich, digital erfasst und, durch ein tägliches Back-up gesichert werden, scheint sich der Verlust auf die erwirtschafteten Daten eines Tages zu beschränken (Interview AUT, Seq. 37).

89 Ein Gesprächspartner rechnete bei den Tätigkeiten mit einem Arbeitsaufwand von insgesamt einer Woche (Interview DE 5, Seq. 16). Einige Wissenschaftler bewerteten den eigenen Arbeits- bzw. den Personalkostenaufwand für die Bearbeitung des angezeigten Schadensfalls als einzigen eingetretenen Schaden (so z.B. Interview DE 3, Seq. 53–54).

90 „Ob man so etwas jetzt monetär oder irgendwie als Schaden einordnen kann, weiß ich nicht" (Interview DE 4, Seq. 18).

91 Interview DE 1, Seq. 24–25.

92 So antwortete ein Interviewpartner auf die Frage, ob ein Schaden durch den Datenabzug und die Weiterverwendung auf chinesischer Seite eingetreten sei: „Also das ist mir nicht bekannt. Das war zumindest keine extrem kritische Sache. Es war ein *source code,* den wir selbst geschrieben haben." Und ein wenig später fügte er hinzu: „Hier gibt es eigentlich nichts zu spionieren. In dem Sinne, dass alle interessanten Inhalte nach zwei bis drei Monaten sowieso veröffentlicht werden, was eine Investition in Spionage völlig überflüssig macht" (Interview DE 3, Seq. 16–17 und 62).

der interviewten Wissenschaftsorganisationen, die nicht selbst Forschung betreiben, widersprachen dem:

> Da fehlt auch das Bewusstsein, das bei einem Forschungsprojekt mit Papern, die sowieso veröffentlicht werden sollen, die Rohdaten, aus denen diese Erkenntnisse gewonnen werden, für Dritte durchaus interessant sein können. Grade wenn das mit Firmenkooperationen ist und durchaus *intellectual property* herumliegt.[93]

4.2.3 Kurz-, mittel- und langfristiges Vorgehen

Die Experten wurden gebeten, ihr kurz-, mittel- und langfristiges Vorgehen nach einem Schadensfall zu beschreiben. Als kurzfristige Reaktionen sind Hausverbote für Mitarbeiter bzw. Gastwissenschaftler, der Entzug von Datenzugriffsrechten sowie die Erstattung von Anzeigen denkbar.

Fünf Interviewpartner gaben an, in der Vergangenheit bei den unterschiedlichsten Behörden „Anzeige erstattet" zu haben. Dabei ist zu beachten, dass es sich hier nicht um Anzeigen im streng juristischen Sinne handelt – diese können gem. § 158 Abs. 1 S. 1 der StPO nur „bei der Staatsanwaltschaft, den Behörden und Beamten des Polizeidienstes und den Amtsgerichten mündlich oder schriftlich angebracht werden" –, sondern die Meldung eines Vorfalls gegenüber einer Behörde gemeint ist. Erwähnung finden in diesem Kontext örtliche Polizeibehörden,[94] Landeskriminalämter, das Bundeskriminalamt, die Landesämter und das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, die Abteilung für Wirtschaftskriminalität der örtlichen Staatsanwaltschaft[95] sowie im Fall Österreichs das Cybercrime Competence Center.[96] Die von einem deutschen und einem dänischen Interviewpartner vertretenen Organisationen haben in der Vergangenheit bewusst Vorfälle nicht angezeigt, bei denen davon ausgegangen wurde, dass die Polizei nicht helfen könne.[97] Ein deutscher Gesprächspartner wandte sich zwar an Behörden, hielt diese Kommunikation aber nicht für eine Anzeige im juristischen Sinn; der britische Gesprächspartner gab an, mit externen Spezialisten zu arbeiten.

Die Motive für die erfolgten Anzeigen waren zum Beispiel:

- die Sorge um verlorene Daten;[98]
- eine Mahnfunktion und Ausstrahlungswirkung für das eigene Personal;[99]

---

93 Interview DE 2, Seq. 61.

94 Interview DE 1, Seq. 131, 133, 151; Interview DE 3, Seq. 77; Interview DE 4, Seq. 72; Interview DE 5, Seq. 11.

95 Interview DE 6, Seq. 45.

96 Interview AUT, Seq. 77.

97 Interview DK, Seq. 120.

98 Interview DE 5, Seq. 42; Interview DE 4, Seq. 6.

99 Interview DE 3, Seq. 82.

- die Erfüllung von Anforderungen im Rahmen des Versicherungsschutzes;
- der Umstand, dass Ersatzbeschaffung auf Institutskosten nur gegen Vorlage der Strafanzeige möglich sei;[100]
- die Einstellung, dass Straftaten stets zu verfolgen[101] und korrekte Statistiken wichtig seien, um die Bedeutung des Phänomens zu belegen.[102]

Eine Wissenschaftsorganisation, die in der Vergangenheit keine Anzeigen erstattet hatten, tat dies nach eigenem Bekunden, weil die Beobachtungen nur das Stadium eines ‚bloßen Gefühls' bzw. ‚subjektiven Empfindens' erreicht hätten und nach Einschätzung der Rechtsabteilung unter der Schwelle des Anfangsverdachts geblieben seien. In solchen Fällen sei die gegenseitige Forschertreue wichtiger als die Angriffsbedrohung.[103]

Der dänische Interviewpartner berichtete, dass physischer Diebstahl regelmäßig angezeigt würde, Cyberangriffe auf seine Wissenschaftsorganisation aber nicht, solange kein Schaden eingetreten sei.[104] Ein ähnliches Vorgehen für den Bereich des Cybercrime berichtete auch ein deutscher Interviewpartnern.[105]

Nur zwei Interviews enthielten Angaben über das mittel- und langfristige Vorgehen der Wissenschaftsorganisationen. Ein deutscher Interviewpartner erklärte, nach einem Angriff[106] bewusst keine offenkundigen technischen oder organisatorischen Maßnahmen getroffen zu haben, um die Sensibilität der entwendeten Daten sowie der durch die Wissenschaftsorganisation generell generierten Forschungsdaten zu verdecken.[107] Zudem habe die Institution einen Ausbildungsauftrag mit einer „Bringschuld gegenüber den Studenten" und sehe sich als „offenes Haus".[108] Er betonte,

---

100 Interview DE 4, Seq. 50.

101 Interview DE 4, Seq. 134; Interview DE 4, Seq. 6.

102 Interview DE 1, Seq. 135.

103 Interview DE 6, Seq. 45.

104 Interview DK, Seq. 123.

105 Interview DE 3, Seq. 108: „In einem Fall haben unsere IT-Leute gemerkt, dass sich vor Jahren jemand eingehackt hat, aber nie aktiv wurde, sodass es nicht entdeckt wurde. Das haben wir aber z.B. sonst keinem gemeldet, weil wir dachten, so wie man es in Zeitungen liest, das passiert ja ständig. Wenn das aber wichtig ist, hätten wir auch kein Problem damit, solche Fälle zur Anzeige zu bringen."

106 Aus einem unverschlossenen Labor, in dem sich viele teure Laptops befanden, wurde genau der Laptop mit sensiblen Daten entwendet.

107 Interview DE 5, Seq. 18–19.

108 Interview DE 5, Seq. 18. Die Autorin konnte, als sie den Interviewpartner ein Jahr nach dem Vorfall für ein persönliches Interview aufsuchte, das Institut, sämtliche Labore sowie das Büro des Forschers, wo sich jeweils offen zugängliche hochwertige Laptops befanden, in dessen Abwesenheit ungehindert und von den anwesenden Mitarbeitern

dass die nötige thematische Sensibilisierung auf Führungsebene bestehe.[109] Zudem werde an der Sensibilisierung der Mitarbeiter in irregulären Zyklen gearbeitet und die Erarbeitung von Vertraulichkeitsvereinbarungen erwogen. Der Gesprächspartner sei dazu übergegangen, Forschung „im stillen Kämmerlein" zu betreiben, um erst nahezu fertige Ergebnisse bekannt zu machen.[110]

Der österreichische Gesprächspartner berichtete, dass sich seine Organisation mitten in einer Generalanpassung ihres Schutzniveaus befinde. Der State-of-the-Art-IT-Schutz und einige personelle und organisatorische Schutzkomponenten. Das Schutzkonzept wird nunmehr unter Zuhilfenahme externer Berater als einheitliches Sicherheitskonzept aus einem Guss neu aufgesetzt.[111]

4.3 Kooperationserfahrungen

Ein Frageblock im WiSKoS-Projekt betraf die Kooperationsbereitschaft und die Kooperationserfahrungen vor allem mit Behörden. Von Seiten der Behörden wurde im Vorfeld des Projektes auf die Möglichkeit zur Verbesserung der Zusammenarbeit verwiesen.

4.3.1 Kooperation mit Behörden

Gegenüber der Kooperation mit Behörden waren die Gesprächspartner grundsätzlich positiv eingestellt und zeigten Interesse an staatlichen Angeboten, z.B. im Bereich Information und Aufklärung.[112] Die staatlichen Angebote stellen eine von mehreren Informationsquellen dar, spielen aus der Sicht von zwei Interviewpartnern als Quelle für aktuelle Bedrohungen jedoch eine untergeordnete Rolle.[113] Der Austausch zwischen den Wissenschaftsorganisationen und (Sicherheits-)Behörden in Visa-Fragen anlässlich der Auswahl von Gastwissenschaftlern wurde von den Interviewpartnern aus Deutschland wiederum positiv bewertet.[114] Ebenso motivierte ein als professionell wahrgenommenes Vorgehen – im einen Fall von örtlichen Polizeibehörden, im anderen vom Verfassungsschutz[115] – die Betroffenen, sich wieder an

nicht hinterfragt betreten und dort auf den Interviewbeginn warten. Die Forschung des Interviewpartners weist deutlich Dual-Use-Komponenten auf.

109 Interview DE 5, Seq. 21.

110 Interview DE 5, Seq. 24–25.

111 Interview AUT, Seq. 33–34.

112 „Was wir vom Verfassungsschutz bekommen als Indikatoren, ist in der Regel von passabler Qualität" (Interview DE 1, Seq. 169–173).

113 Interview DE 6, Seq. 18; Interview BG, Seq. 38–40.

114 Interview DE 1, Seq. 61; Interview DE 3, Seq. 69; Interview DE 6, Seq. 22.

115 Interview DE 5, Seq. 11 und Interview DE 2, Seq. 12.

die entsprechende Behörde zu wenden.[116] Als negative Erfahrungen mit Behörden wurden fehlerhafte Datenangaben, die die Betroffenen vor die Aufgabe langwieriger Kontrollarbeiten zur Entkräftung von Vorwürfen stellten, der Versuch, geschützte Information auch bei fehlender Rechtsgrundlage zu erlangen,[117] und mangelnde Kommunikation angegeben.[118]

4.3.2 Kooperation von Wissenschaftsorganisationen

Neben der Kooperation mit staatlichen Stellen gibt es auch eine Zusammenarbeit der Wissenschaftsorganisationen untereinander, zum Teil auch auf internationaler Ebene. Es bestehen Möglichkeiten eines informellen Austauschs auf allen Hierarchieebenen,[119] eines Erfahrungsaustausches in IT-Fragen[120] oder auch institutionalisierte Angebote in Form von Arbeitskreisen[121]. Ein wichtiges Forum zum Informationsaustausch und Vernetzen ist der Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF), der von den hauptamtlichen Sicherheitsbeauftragten der drei großen deutschen Forschungsinstitutionen gestützt wird[122] und an dem auch die Rechenzentren von Universitäten und Hochschulen beteiligt sind.[123] Teilweise befassen sich auch die Arbeitsgruppen der Datenschutzbeauftragten mit

---

116 „Also, damals war das mit dem bayrischen Landesverfassungsschutz eigentlich sehr angenehm. Die haben das Geschehene auch in Relation gesetzt und haben gesagt, das ist nicht in Ordnung und da sollte man etwas unternehmen“ (Interview DE 3, Seq. 104).

117 Dieser Vorwurf wurde in zwei Fällen erhoben und betraf den jeweiligen Landesverfassungsschutz (Interview DE 1, Seq. 169–173; Interview DE 5, Seq. 10–14).

118 Entsprechende Kritik kam u.a. von IT-Beauftragten für den Bereich der Cyberkriminalität. Ein Interviewpartner erklärt: „Unser Wunsch ist, die Kommunikationswege zu verkürzen und nicht per Post CDs zu bekommen, sondern geschützte Verteiler zu haben. Und auch, dass wir den Behörden Informationen liefern können, damit diese wiederum schneller reagieren können. Über welche Arten von Auffälligkeiten die gerne von uns informiert werden würden, wissen wir einfach nicht. Die Kommunikation beschränkt sich genau auf solche Meldungen, bei denen dann Hektik ausbricht, aber davon abgesehen, trifft man die Leute noch bei Konferenzen o.Ä., aber redet relativ wenig darüber“ (Interview DE 2, Seq. 55).

119 Interview DE 1, Seq. 114–118.

120 Interview DE 2, Seq. 49: „[…] Informationsaustausch. Das heißt, auf europäischer Ebene gibt es durchaus Rückmeldungen, falls Auffälligkeiten stattfinden, aber auch nicht mehr. Es ist meistens auch ein Erfahrungsaustausch über die technischen Werkzeuge, die man einsetzt, um verschiedenste Arten von Angriffen erkennen zu können, aber keine Kooperation im Fall einzelner Angriffe. Manchmal kriegt man noch kompromittierte Accounts mit, worauf wir die entsprechenden Filter aufgesetzt haben und nicht fündig geworden sind“.

121 Interview DE 1, Seq. 185.

122 Interview DE 1, Seq. 87.

123 Interview DE 2, Seq. 39–41.

dem Thema Wissenschaftsspionage. Ein Austausch dazu findet z.B. auf der jährlichen IT-Sicherheitstagung des DFN statt.[124]

4. Schutzbedarf in Wissenschaftsorganisationen

Die besonderen Herausforderungen von Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext gebieten die Entwicklung von auf den Wissenschaftskontext zugeschnittenen, besonderen Handlungsansätzen – dies gilt sowohl für die Wissenschaftsorganisationen selbst als auch parallel dazu für die Behörden. Dabei müssen die im Vergleich zur Wirtschaft deutlich anderen Hierarchiestrukturen der unabhängigen Forschungsinstitute und -gruppen sowie Lehrstühle berücksichtigt werden, die häufig Unklarheiten bezüglich interner Zuständigkeiten mit sich bringen und Informationsdefizite in der Kommunikation zwischen Lehrstuhlinhaber und Präsidialebene sowie Forscher und Institutsleitung bzw. Generalverwaltung nach sich ziehen. Zu beachten ist auch die im Wissenschaftssektor bestehende Problematik beim Umgang mit internationalen Forschungskooperationen, die unter Umständen Voraussetzung für die Zuweisung von Forschungsgeldern sind.[125]

Auf Basis der oben dargestellten Ergebnisse aus den Interviews kann vermutet werden, dass in deutschen Wissenschaftsorganisationen eine hinreichende Sensibilisierung bezüglich Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext fehlt.[126] Diese sogenannte Awareness schien zum Zeitpunkt der Interviews bis auf wenige Ausnahmen auch bei Instituten der großen deutschen Forschungsgesellschaften auf allen Hierarchieebenen gleichermaßen zu fehlen.[127] Zum Teil scheinen sich einzelne Wissenschaftler ebenso wenig potenziell betroffen oder zuständig zu fühlen wie Fakultäten und Institute, während auf Leitungsebene überraschenderweise teilweise nicht bekannt war, welche Forschung mit welchem Risikopotential in den einzelnen Lehrstühlen/Instituten betrieben

---

124 Interview DE 1, Seq. 118.

125 Siehe *Abschnitt 3.2.2* in diesem Beitrag.

126 Zur Unterstützung von Wissenschaftsorganisationen bei Schulungen oder anderen Sensibilisierungsmaßnahmen wird ein im Rahmen des WiSKoS-Projekts für diese Zielgruppe entwickelter Handlungsleitfaden auf der Projekt-Homepage (https://wiskos.de) zum Download zur Verfügung gestellt.

127 In diesem Kontext ist bezeichnend, dass die Autorin trotz entsprechender Anfragen keinen Interviewpartner im universitären Präsidialbereich oder aus einer Rechtsabteilung gewinnen konnte. Der Autorin liegt ein Schreiben der Rechtsabteilung einer deutschen Universität mit international attraktiver Forschungstätigkeit vor, in dem man sich gerne zur Teilnahme bereit erklärt, aber vorab um Informationen bittet, wie man denn überhaupt betroffen sein könnte.

wird.[128] Es mangelt hinsichtlich des Themas offenbar häufig an einer (hinreichenden) Verknüpfung der Unterabteilungen und es scheint ein internes Kommunikationsdefizit zu bestehen. Oft fehlen klar definierte Ansprechpartner. Sofern überhaupt eine Zuständigkeitsregelung existiert, nimmt sie häufig nur den IT- oder Datenschutzbeauftragten einer Einrichtung in die Verantwortung, was zu einer fehlenden umfassenden Betrachtung des Risikopotenzials führen kann. Wenn eine thematische Sensibilisierung besteht, findet diese kaum Niederschlag in adäquaten, bedarfsbezogenen Präventionsmaßnahmen.

Zusammenfassend kann festgestellt werden: In deutschen Wissenschaftsorganisationen scheint außerhalb des IT-Bereichs keine systematische Analyse des Schutzbedarfs stattzufinden, die bei größeren Einrichtungen für die Gesamtheit sowie für die Unterabteilungen, Fakultäten und Institute jeweils getrennt durchgeführt werden muss. Schutzbedarf und Schutzniveau werden nicht aufeinander abgestimmt. Statt eines einheitlichen Konzeptes finden sich viele disparate Einzelmaßnahmen. Es fehlt an einer gezielten Ausarbeitung passender Maßnahmen für organisatorische, technische und personelle Schutzaspekte, die zu einem einheitlichen Sicherheitskonzept mit holistischem Ansatz angemessen verknüpft werden.[129] Bei all diesen Punkten sollten die deutschen Wissenschaftsorganisationen nachjustieren, wenn sie mit Spitzenforschung dauerhaft international erfolgreich sein wollen.

5. Auf Best Practices basierende Handlungsansätze

Wissenschaftsorganisationen sollten sich durch die Einführung eines umfassenden Sicherheitskonzeptes vor dem unerlaubten Informationsabfluss schützen. Nach der Durchführung einer Risikoanalyse, der Ermittlung des Schutzbedarfs und eines darauf abgestimmten Schutzniveaus kann ein Sicherheitskonzept erstellt werden, das organisatorische, personelle und technische Einzelmaßnahmen verknüpft und nach seiner Implementierung kontinuierlich aktualisiert wird. Das Schutzkonzept sollte auch die Kooperation mit Sicherheitsbehörden außerhalb des Schadensfalls enthalten. Die einzelnen Komponenten des Schutzkonzeptes werden im Folgenden unter Einbeziehung von Erfahrungen aus dem Ausland näher einer näheren Betrachtung unterzogen.

---

128 Interview DE 2, Seq. 10, 61.

129 Interview DK, Seq. 76. Der britische Interviewpartner fasst die Anforderungen so zusammen: “I think that a robust security system, both physical and, you know, and technical, is really about resilience, and having a number of different layers in. And that includes not just having those measures in place, but also having things like training and awareness measures in place, as well, that support those physical and technical security measures. So, I don‘t think that anyone is more or less effective, I think that they need to be combined, you know, so a much more converged, much more holistic approach, so that you then put the resilience in place” (Interview UK, Seq. 29–32).

5.1 Risikoanalyse, Schutzbedarf, Schutzniveau

Der britische und der österreichische Interviewpartner berichteten, dass sie – veranlasst durch die Leitungsebene – für ihre Wissenschaftsorganisationen eine Risikoanalyse zur Ermittlung des Schutzbedarfs durchgeführt haben, in die sowohl die internen Mitarbeiter aller Abteilungen als auch externe Berater einbezogen wurden.[130] Auf diesem Weg wurde ermittelt, welche Forschungsprojekte und -ergebnisse in ihrer Institution welcher Bedrohung durch Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext ausgesetzt sind. Anhand des festgestellten Schutzbedarfs konnte dann für die einzelnen Forschungsbereiche, aber auch z.B. für die IT-Abteilung und, soweit dort Patentanträge bearbeitet werden, die Rechtsabteilungen und Gründungsnetzwerke, ein individuelles Schutzniveau definiert werden.

5.2 Sicherheitskonzept

Basierend auf dem als notwendig festgestellten Schutzniveau ist in einem nächsten Schritt ein einheitliches Sicherheitskonzept zu entwickeln. Der dänische Gesprächspartner definierte ein solches Sicherheitskonzept als

> coordination mechanisms and practical protocols with clear task assignment that are established in advance across the common administration and individual faculties. [131]

Einheitliche Konzepte bestehen bei deutschen Wissenschaftsorganisationen bisher nur für den IT-Bereich. Ein wirkungsvolles Sicherheitskonzept lebt aber nach Erfahrung der dänischen und britischen Interviewpartner davon, dass es zum einen personelle, organisatorische und technische Schutzmaßnahmen vorsieht und miteinander verknüpft und zum anderen auf die real existierenden Ressourcen zurückgreift, anstatt für einen z.B. auf Basis von Kosten-Nutzen-Erwägungen imaginierten Sollzustand zu planen.[132] Sinnvoll erscheint, eine Unterstützung bei der Erstellung von Behördenseite einzufordern – wie vom schweizerischen Inter-

---

130 Der österreichische Interviewpartner führte dazu aus: „[Es ist klar,] dass ich nicht meine eigenen Forscher nehmen kann, um systematisch einen Prozess zu implementieren. Da führen wir dann externe Consulter ein. Da gibt es einen, der uns begleitet, mit dem wir das dann *state-of-the-art* machen. Angereichert mit unseren Sichtweisen." Er gab an, dass es sich dabei nicht um einen Consulting-Auftrag handele, sondern um einen intensiven Diskurs mit dem betreffenden Management (Abteilungsleiter, Teamleiter) sowie mit den IT-Benutzern dahinter: „Wir diskutieren da mit allen, damit das verstanden wird […]" (Interview AUT, Seq. 61).

131 Interview DK, Seq. 25–27.

132 Interview UK, Seq. 29–32; Interview DK, Seq. 25–27: "Such an emergency response […] was designed with a pragmatic, practical, concrete focus, starting with the actual ingredients and people that are in place; not what *should* have been in place. The plan was designed in collaboration with specialised external consultants. It combines both direc-

viewpartner empfohlen[133] – und das eigene Sicherheitskonzept regelmäßig auditieren zu lassen.[134] Das Konzept sollte sowohl Maßnahmen für ein Vorgehen im Schadensfall als auch zur Prävention vorsehen. In der Wissenschaftsorganisation des dänischen Gesprächspartners ist eine „pre-determined ‚rapid-reaction force'" vorgesehen, die im Ernstfall mit erprobten Koordinationsmechanismen Verwaltung und Fakultäten bei der Aktivierung der Schutzmaßnahmen unterstützt.[135] Denkbar sind hier unter anderem die Einrichtung der Stelle eines zentralen Ansprechpartners bei Verdachtsfällen, die Sicherung einer guten Erreichbarkeit der Entscheidungsträger und IT- und Datenschutzbeauftragten sowie die Anforderung von behördlicher Unterstützung.

Basierend auf den Erfahrungen der Interviewpartner (vor allem der aus den Vergleichsländern) sollten zur organisatorischen Prävention folgende Einzelmaßnahmen erwogen werden:[136]

- Thematische Sensibilisierung und Schulung der Mitarbeiter (für Datenschutz/Datensicherheit, gegen Social Engineering);[137]
- Einstellung eines Sicherheitsbeauftragten;
- Überprüfung von Bewerbern, Gastwissenschaftlern, auffälligem Verhalten etablierter Mitarbeiter sowie Beobachtung der Karrierewege nach Verlassen der Wissenschaftsorganisation;
- Vertraulichkeitsvereinbarungen für Mitarbeiter und Kooperationspartner;[138]
- Hinzuziehung externer Sicherheitsberater;

---

tors and lower-level people with the requisite technical knowledge. Roles and reporting lines are pre-assigned."

133 Interview CH, Seq. 28–29.

134 So vorgeschlagen vom Gesprächspartner des Interviews DE 4, Seq. 71–72.

135 Interview DK, Seq. 26.

136 Die nachfolgende Aufzählung ist nicht abschließend.

137 Als sinnvoll bewertet in: Interview CH, Seq. 46; Interview DE 1, Seq. 108; Interview DE 6, Seq. 18; Interview DE 5, Seq. 34–38. Interview AUT, Seq. 48–51: „Bei der Ausbildung der Awareness geht es darum, dass der Forscher – auch wenn er es gar nicht so wahrnimmt – darüber nachdenkt, dass er gegebenenfalls mit kritischen Daten umgeht. Das ist ein Grundsatzproblem, was wir ganz massiv haben. Dazu machen wir Meetings und Workshops, in denen wir darüber diskutieren. Das zweite wäre dann, das Bewusstsein zu schärfen und auch Regeln zu definieren, um dann auch zu einem Entwicklungsprozess zu finden." Auch der schweizerische Interviewpartner betont, Sensibilisierung sei erforderlich und diene „der Bewusstseinsförderung, was eigentlich passieren kann", und begründet dies folgendermaßen: „Weil eben, glaube ich, der Wissenschaftler/die Wissenschaftlerin ist blauäugig in dem Sinne, dass eben die Vertrauensbasis sehr hoch ist, das ist richtig so, aber das sollte nicht daran hindern, dass eben doch gewisse Regeln …, dass man sich deren bewusster wird" (Interview CH, Seq. 46–47).

138 Interview BG, 26–31.

- Festsetzung einer Hierarchie der Zugangsberechtigungen für Labore, Büros und Serverräume;[139]
- technische und/oder personelle Zugangskontrollen zu den Forschungsstätten;[140]
- Vorschriften zur Überwachung der Hardware;[141]
- Limitierung von Zugriffsrechten auf Laufwerke und Daten (Rechtemanagement) sowie Einrichtung von SharePoint, ggf. mit Freigabevorgaben; Sicherheitsstufen bei Dokumenten sowie digitale Zugriffskontrolle;[142]
- Sicherheitsvorschriften im Umgang mit sensiblen Daten;[143]
- Krisenpläne („rapid reaction force") und Einübung bestimmter Verhaltensmuster in kritischen Situationen;
- Mitgliedschaft in und aktive Teilnahme an gemeinsamen Arbeitskreisen, z.B. AKIF,[144] und Tagungen, Nutzung von Newslettern.[145]

Als personelle Einzelmaßnahme sollte – angepasst an die Größe der Wissenschaftsorganisation – die Schaffung der Stelle eines haupt- oder nebenberuflichen Sicherheitsbeauftragten erwogen werden, der der Leitungsebene (Generalverwaltung oder Präsidialamt) in diesem Themenbereich zuarbeitet.[146] Dabei ist zu berücksichtigen, dass einerseits der Wille zur Risikominimierung in der gesamten Institution vorhanden sein muss und andererseits eine etwaige Verteilung von Aufgaben des Sicherheitsbeauftragten z.B. an den Datenschutz- oder IT-Beauftragten zielführend sein kann. Aufgaben des Sicherheitsbeauftragten wären die Erstellung und kontinuierliche Aktualisierung des Sicherheitskonzeptes, die Unterstützung der Leitungsebene und Verwaltung beim Umgang mit Sicherheitsbehörden, bei der Personalauswahl, beim Umgang mit Patentschutz und IT-Sicherheit sowie bei der Implementation von Zugangsberechtigungen und -kontrollen sowie Sicherheitsvorschriften.[147] Gleichzeitig wäre der Sicherheitsbeauftragte damit beauf-

---

139 Interview DK, Seq. 90–97; Interview BG, 26–31.

140 Interview DK, Seq. 90–97.

141 Problematisch im Hinblick auf Innen- wie Außentäter ist z.B. die Praxis, dass Laptops bei Ausgabe im Zuge der Anlageninventur gezählt werden, aber nicht bei Rücknahme (Interview DE 6, Seq. 17).

142 Interview UK, Seq. 53–55; Interview DE 3, Seq. 24–26.

143 Interview DE 3, Seq. 24–26.

144 Interview DE 2, Seq. 39–41.

145 Interview UK Seq. 99–100; Interview DE 2, Seq. 12; in Interview DE 2, Seq. 47 wird dies so begründet: „Den einen ‚Ort der Wahrheit', aus dem wir über alles, was irgendwie böse ist, Informationen beziehen, den gibt es nicht."

146 So z.B. Interview DE 4, Seq. 68.

147 Interview DE 1, Seq. 169–173.

tragt, regelmäßigen Kontakt zu den zuständigen Sicherheitsbehörden und anderen Wissenschaftsorganisationen über entsprechende Arbeitskreise, Konferenzen und Newsletter zu halten.[148]

Die zweite zentrale personalbezogene Einzelmaßnahme, die an der Schnittstelle zu den organisatorischen Maßnahmen angesiedelt ist, ist die schon erwähnte Sensibilisierung der Mitarbeiter für die Gefahr von Wissenschaftsspionage sowie vermeidbare Schwachstellen durch entsprechende Informationen bzw. Schulungen. Allerdings können Sensibilisierungskampagnen, wenn sie effizient sein sollen, ressourcenintensiv sein.[149] Dabei ist zu beachten, dass alle Hierarchie-Ebenen einbezogen werden und für jede Zielgruppe eine passende Ansprache gewählt wird, z.B. in Workshops, Einzelgesprächen oder durch Rundmails.[150] In Betracht kommt auch die Teilnahme an von Behörden oder Externen angebotenen Schulungen.[151]

Ein umfassendes Sicherheitskonzept bedarf auch der Einbeziehung technischer Maßnahmen, vor allem im IT-Bereich (Computersicherheit, elektronische Zugangssysteme, Netztrennung, Rechtemanagement etc.), aber auch bei physischen Zugangskontrollen.[152] Was den IT-Bereich betrifft, bestehen bei den deutschen Wissenschaftsorganisationen bereits weitreichende Ansätze.[153] Das erstellte Sicherheitskonzept sollte sodann möglichst unter Einbeziehung aller Betroffenen implementiert und regelmäßig aktualisiert werden.

---

148 Interview DK, Seq. 108–109.

149 Den Aufwand, den solche Sensibilisierungskampagnen bei den eigenen Mitarbeitern verursachen, beschreibt der dänische Interviewpartner: "User error is a big source of problems, training employees remains an open challenge. A new policy is being produced, training videos exist on the website. Most information is currently still only in Danish, making all of it available in English in their entirety is the key challenge given the large number of foreigners at the [institution]. Mandatory trainings are, unfortunately, not possible given the nature of [Institution]. The message has to change constantly, so as to remain relevant to the users, not least to different age cohorts. Characters in the videos and posters must be relatable. Survey data points to a bewildering need to adapt the same message to different audiences: men and women, young and old, Danish and foreign, academic and technical staff, etc., all this without taxing very limited absorption capacities. Being allowed to get people's attention for five minutes is an ongoing challenge. Reinforcing very common security practices that everyone applies in normal life but not in the workplace" (Interview DK, Seq. 34–37).

150 Interview DE 5, Seq. 19.

151 Interview BG, Seq. 38–40; Interview 6, Seq. 18 und 48.

152 Interview AUT, Seq. 39–43.

153 Interview DE 4, Seq. 71–72; Interview DE 1, 81–83.

5.3 Kooperation mit Behörden

Eine kontinuierliche Kooperation mit Behörden ist nicht nur im Schadensfall und im repressiven Bereich möglich und ratsam. Hier ist zu betonen, dass aufseiten der Sicherheitsbehörden besonders geschulte Ansprechpartner in Fragen von Spionage und Konkurrenzausspähung zur Verfügung stehen, die bei der Beratung und Ermittlung diskret vorgehen. Die deutschen Interviewpartner berichteten überwiegend von positiven Erfahrungen bei der Kooperation mit Behörden.[154] Nach einem Vorfall unterstützt eine Zusammenarbeit die Behörden darin, ihrer Aufgabe als Strafverfolgungsbehörde nachzukommen, aussagekräftigere Statistiken zu erstellen und bessere Abwehrstrategien für Wissenschaftsorganisationen zu entwickeln. Die Sicherheitsbehörden arbeiten aktiv daran, ihre Ansprache – die in der Vergangenheit auch bei Schulungen vorwiegend auf Wirtschaftsunternehmen zugeschnitten war – auch an die Zielgruppe der Wissenschaftsorganisationen anzupassen.[155]

Empfehlenswert ist zudem eine Kooperation mit den Sicherheitsbehörden auch im präventiven Bereich. So kann bei Erstellung eines Sicherheitskonzeptes gegebenenfalls auf Empfehlungen oder Erfahrungen von Behörden zurückgegriffen werden.[156] Denkbar wäre die Entwicklung einer einheitlichen Informationsplattform für behördliche Informationen und Ansprachen parallel zu der für Wirtschaftsunternehmen bestehenden Plattform www.wirtschaftsschutz.info.[157]

6. Zusammenfassung

Die staatlich gelenkte Wissenschaftsspionage und die von der Konkurrenz in Wirtschaft und Wissenschaft ausgehende Ausspähung im Wissenschaftskontext werden trotz teilweiser Viktimisierungserfahrungen seitens der deutschen Wissenschaftsorganisationen bisher nicht in hinreichendem Maße als Risiko für die eigene Forschung wahrgenommen. Die Analyse von elf Interviews mit im Wissenschaftssektor in verschiedenen Bereichen tätigen Experten hat gezeigt, dass in der Forschungslandschaft im europäischen Ausland mitunter eine höhere Sensibilität als in Deutschland für das Bedrohungspotenzial besteht. Während bei den ausländischen Wissenschaftsorganisationen ein gewisser ‚reaktiver Vorsprung' konstatiert werden kann, besteht bei den deutschen Wissenschaftsorganisationen konkreter Handlungsbedarf bei der Analyse des eigenen Schutzbedarfs und der Etablierung eines entsprechenden Schutzniveaus. Es wird empfohlen, die derzeit implementierten Einzelmaßnahmen durch ein umfassendes Sicherheitskonzept zu ersetzen, das organisatorische, technische und personelle Schutzaspekte vereint. Sofern deutsche Wissenschaftsorganisationen

---

154 Siehe oben unter *3.4.4,* „Kooperationserfahrungen mit Behörden".

155 Interview DE 1, Seq. 120.

156 Vgl. *Boos*, S. 68.

157 Interview DE 1, Seq. 120 und Interview DE 2, Seq. 47.

ihre Angestellten künftig für das Thema Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext sensibilisieren und infrastrukturelle Maßnahmen, die in ein Gesamtkonzept eingebettet sind, ergreifen, könnte das Bedrohungspotenzial für die deutsche Forschung nachhaltig reduziert werden.

Literatur

Bayerisches Landesamt für Verfassungsschutz (o.D.): Wirtschaftsspionage; www.verfassungsschutz.bayern.de/spionageabwehr/wirtschaftsschutz/wirtschaftspionage/index.html [05.04.2019].

Boos, R. (2012): Wissenschaftsspionage: Risiken für den Forschungsstandort Deutschland in einer offenen globalen Informationsgesellschaft, in: A. Handschuh & G. Ring (Hrsg.), Sicher forschen und entwickeln. Baden-Baden, S. 61–74.

Bundesamt für Verfassungsschutz (2016): Verfassungsschutzbericht 2016; https://www.verfassungsschutz.de/embed/vsbericht-2016.pdf [05.04.2019].

Bundesamt für Verfassungsschutz (2015): „Innentäter" – eine unterschätzte Gefahr in Unternehmen. 9. Sicherheitstagung des BfV und der ASW. Berlin.

Bundesamt für Verfassungsschutz (2014): Verfassungsschutzbericht 2014; www.verfassungsschutz.de/embed/vsbericht-2014.pdf [05.04.2019].

Bundesamt für Verfassungsschutz (2008): Spionage gegen Deutschland – Aktuelle Entwicklungen; https://docplayer.org/13995588-Spionage-gegen-deutschland-aktuelle-entwicklungen.html [05.04.2019]

Bollhöfer, E. & Jäger, A. (2018): Wirtschaftsspionage und Konkurrenzausspähung – Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Freiburg im Breisgau.

Carl, S., Kilchling, M., Knickmeier, S. & Wallwaey, E. (2017): Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – Eine rechtsvergleichende Betrachtung. Freiburg im Breisgau.

Fleischer, D. (2016): Wirtschaftsspionage. Phänomenologie, Erklärungsansätze, Handlungsoptionen. Wiesbaden.

Gude, H. (2015): 800 Euro zum Kaffee. Der Spiegel 31, S. 47.

Kilchling, M. & Carl, S. (2016): Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS), in: P. Zoche, S. Kaufmann & H. Arnold (Hrsg.), Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung. Berlin, S. 183–196.

Oehler, D. (1971): Verrat von Wirtschaftsgeheimnissen. Zeitschrift für Rechtspolitik, S. 4.

Röder, N. (2011): Industriespionage. Risikofaktor Mensch. Hannover.

Ulmer, E. (1965): Das Recht des unlauteren Wettbewerbs in den Mitgliedsstaaten der EWG. München.

Autorinnen und Autoren

Esther Bollhöfer

Prof. Dr. Esther Bollhöfer lehrt Wirtschaftsrecht und IT-Recht an der FOM – Hochschule für Oekonomie & Management gGmbH – am Hochschulzentrum Mannheim. Parallel forscht sie seit vielen Jahren für und über kleine und mittelständische Unternehmen. Das Forschungsprojekt WiSKoS leitete sie während ihrer langjährigen Tätigkeit für das Fraunhofer-Institut für System- und Innovationsforschung ISI mit.

Kontakt: esther.bollhoefer@fom.de

Sabine Carl

Dr. jur. Sabine Carl arbeitete bis August 2017 als Senior Researcher in der Abteilung Kriminologie am Max-Planck-Institut für ausländisches und internationales Strafrecht. Als Projektkoordinatorin verantwortete sie das Konsortialprojekt WiSKoS. Heute ist die promovierte Strafrechtlerin als Referentin im Bundesministerium für Bildung und Forschung, Bonn, tätig.

Kontakt: sabine.carl@googlemail.com

Fabian Fischbach

Herr Fabian Fischbach erstellte 2016/17 seine politikwissenschaftliche Masterarbeit „Explaining public and private sector cooperation in countering economic and industrial espionage“ am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe und arbeitete während dieser Zeit an dem Projekt WiSKoS mit.

Kontakt: fmfischbach@protonmail.com

Michael Kilchling

Dr. jur. Michael Kilchling ist Senior Researcher am Max-Planck-Institut für ausländisches und internationales Strafrecht in der Abteilung Recht der öffentlichen Sicherheit (bis Mai 2019: Abteilung Kriminologie) und Lehrbeauftragter an der Juristischen Fakultät der Universität Freiburg. Er war Mitinitiator und Mitautor des Forschungsdesigns des Konsortialprojekts WiSKoS, das er wissenschaftlich mit betreut hat.

Kontakt: m.kilchling@mpicc.de

Susanne Knickmeier

Frau Susanne Knickmeier, M.A., ist seit 2012 als wissenschaftliche Mitarbeiterin in der Abteilung Kriminologie am Max-Planck-Institut für ausländisches und interna-

tionales Strafrecht beschäftigt. Zunächst arbeitete sie in dem EU-Forschungsprojekt Fiducia und ab 2015 in dem Projekt WiSKoS, dessen Koordination sie 2017 übernahm. In ihrer wirtschaftskriminologischen Dissertation untersucht sie die Phänomenologie von sowie Erklärungsansätze zu Wirtschaftsspionage und Konkurrenzausspähung.

Kontakt: s.knickmeier@mpicc.de

Binia Sonnen

Frau Binia Sonnen ist wissenschaftliche Hilfskraft am Lehrstuhl für Mikroökonomik, insb. Energie- und Ressourcenökonomik, der Westfälischen Wilhelms-Universität Münster. 2016/17 erstellte sie ihre Bachelorarbeit am Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, und arbeitete dort zusätzlich als wissenschaftliche Hilfskraft am Projekt WiSKoS mit.

Kontakt: binia.sonnen@uni-muenster.de

Lisa Waldheim

Frau Lisa Waldheim studierte nach ihrem Bachelorstudium der Politikwissenschaft und Psychologie an der Universität Freiburg in dem Masterstudiengang Internationale Studien / Friedens- und Konfliktforschung in Frankfurt a.M. Während eines Praktikums am Max-Planck-Institut für ausländisches und internationales Strafrecht arbeitete sie im Rahmen des Projektes WiSKoS an den qualitativen Literaturanalysen mit.

Kontakt: lisa.waldheim@freenet.de

Elisa Wallwaey

Frau Elisa Wallwaey, M.A., war von 2015 bis 2019 als wissenschaftliche Mitarbeiterin in der Abteilung Kriminologie des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Projekt WiSKoS tätig. Seit Februar 2019 arbeitet sie am Fraunhofer Institut für System- und Innovationsforschung ISI im Competence Center Politik und Gesellschaft, Geschäftsfeld Politikdesign und Bewertung. Ihr dortiger Arbeitsschwerpunkt liegt in der Evaluation nationaler wie internationaler forschungs- und innovationspolitischer Maßnahmen.

Kontakt: elisa.wallwaey@isi.fraunhofer.de

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden fünf Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“,
- „Kriminologische Forschungsberichte“,
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“
- „Publications of the Max Planck Partner Group for Balkan Criminology“ sowie
- „Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung“.

Diese Publikationen können direkt über das Max-Planck-Institut unter www.mpicc.de oder über den Verlag Duncker & Humblot unter www.duncker-humblot.de erworben werden.

Darüber hinaus erscheinen im Hausverlag des Max-Planck-Instituts in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen sind unter www.mpicc.de abrufbar.

Research Series of the Max Planck Institute for Foreign and International Criminal Law

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following five subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht/Research Series of the Max Planck Institute for Foreign and International Criminal Law”, which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law),
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology),
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology),
- “Publications of the Max Planck Partner Group for Balkan Criminology“, and
- “Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung” (Collection of Foreign Criminal Laws in German Translation).

These publications can be ordered from the Max Planck Institute at www.mpicc.de or from Duncker & Humblot at www.duncker-humblot.de.

Two additional subseries are published directly by the Max Planck Institute for Foreign and International Criminal Law: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications can be found at www.mpicc.de.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aktueller Publikationen aus der kriminologischen Reihe BC und der interdisziplinären Reihe I:

BC 2 *Sunčana Roksandić Vidlička*
Prosecuting Serious Economic Crimes as International Crimes
A New Mandate for the ICC?
Berlin 2017 • 530 Seiten • ISBN 978-3-86113-264-6 € 44,-

BC 1 *Anna-Maria Getoš Kalac, Hans-Jörg Albrecht, Michael Kilchling* (eds.)
Mapping the Criminological Landscape of the Balkans
A Survey on Criminology and Crime
with an Expedition into the Criminal Landscape of the Balkans
Berlin 2014 • 540 Seiten • ISBN 978-3-86113-248-6 € 44,-

I 25 *Chenguang Zhao*
The ICC and China
The Principle of Complementarity and National
Implementation of International Criminal Law
Berlin 2017 • 245 Seiten • ISBN 978-3-86113-266-0 € 35,-

I 24 *Ulrich Sieber* (Hrsg.)
Strafrecht in einer globalen Welt
Internationales Kolloquium zum Gedenken an Professor Dr.
Hans-Heinrich Jescheck vom 7. bis 8. Januar 2011
Berlin 2016 • 200 Seiten • ISBN 978-3-86113-259-2 € 30,-

I 23 *Hans-Jörg Albrecht* (Hrsg.)
Kriminalität, Kriminalitätskontrolle, Strafvollzug und Menschenrechte
Internationales Kolloquium zum Gedenken an Professor Dr.
Günther Kaiser am 23. Januar 2009
Berlin 2016 • 176 Seiten • ISBN 978-3-86113-258-5 € 30,-

I 22 *Claudia Carolin Klüpfel*
Die Vollzugspraxis des Umweltstraf- und Umweltordnungs-widrigkeitenrechts
Eine empirische Untersuchung zur aktuellen Anwendungspraxis
sowie Entwicklung des Fallspektrums und des Verfahrensgangs
seit den 1980er Jahren
Berlin 2016 • 278 Seiten • ISBN 978-3-86113-257-8 € 35,-

I 21 *Tanja Leibold*
Der Deal im Steuerstrafrecht
Die Verständigung gemäß § 257c StPO in der Systematik des formellen
und materiellen Rechts
Berlin 2016 • 254 Seiten • ISBN 978-3-86113-256-1 € 35,-