ZIVILE SICHERHEIT 13

Peter Zoche, Stefan Kaufmann, Harald Arnold (Hg.)

Grenzenlose Sicherheit?

Gesellschaftliche Dimensionen der Sicherheitsforschung

LIT

Wirtschaftsspionage im globalen Markt: Sind die Ermittlungsstrukturen in Deutschland noch zeitgemäß?

Michael KILCHLING & Sabine CARL

1. Einleitung

Wirtschaftsspionage in ihren verschiedenen Ausprägungen und Fragestellungen ihrer (straf-)rechtlichen Kontrolle sind empirisch bislang wenig erforscht. Mit dem internationalen Verbundprojekt „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS)“ soll dieser Kriminalitätsbereich einer systematischen Analyse unterzogen werden. Das Projekt wird in Kooperation des Max-Planck-Instituts für ausländisches und internationales Strafrecht (MPICC), Freiburg, mit dem Fraunhofer-Institut für System- und Innovationsforschung (ISI), Karlsruhe, durchgeführt. Als assoziierte Partner sind ferner das Bundeskriminalamt, das Landeskriminalamt Baden-Württemberg sowie die Polizeihochschule Sachsen beteiligt. Es wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Förderlinie ‚Zivile Sicherheit – Schutz vor Wirtschaftskriminalität‘ finanziell gefördert.

Das WiSKoS-Projekt untersucht, ob die gegenwärtigen Regelungs- und Kontrollstrukturen auf dem Gebiet der Wirtschaftsspionage und Konkurrenzausspähung (nachfolgend: Wirtschaftsspionage im weiteren Sinne [i.w.S.]) im Hinblick auf die Rahmenbedingungen in der globalisierten Wirtschaft noch zeitgemäß sind oder einer grundlegenden Neukonzeption bedürfen. Hierfür werden der rechtliche und rechtstatsächliche Status Quo, einschließlich der staatlichen Ermittlungsstrukturen in Deutschland und Europa, systematisch ebenso analysiert wie die innerbetrieblichen Erkennungs- und Präventionsstrategien.

2. Begriffsklärung

Im Kriminalitätsbereich der Wirtschaftsspionage und Konkurrenzausspähung gibt es weder in der englischen noch in der deutschen Sprache eine einheitliche Terminologie. Je nach Motivation und Hintergrund der Autoren finden für die Wirtschaftsspionage i.w.S. Begrifflichkeiten wie Betriebsspiona-

ge, Geheimnisschutz (materiell und personell), illegaler Wissensabfluss, Industriespionage, Know-how-Schutz, Sabotageschutz, ungewollter Informationsabfluss, Werksspionage, wirtschaftliche Kriegsführung, Wettbewerbsspionage, Wissensdiebstahl oder Wissensabschöpfung – und im Englischen economic espionage in a wider sense, industrial espionage, corporate espionage, economic intelligence oder data theft – Verwendung. Die Wirtschaftsspionage im engeren Sinne (i.e.S.), die in Deutschland auch als staatsverstärkte Kriminalität bezeichnet wird, wird im Englischen als economic espionage, economic warfare oder digital sovereignty beschrieben (Naucke 1996).

In dem Forschungsprojekt werden die Begriffe Wirtschaftsspionage und Konkurrenzausspähung (Wirtschaftsspionage i.w.S.) verwendet. Nach dem einheitlichen Verständnis der Sicherheitsbehörden in Deutschland ist Wirtschaftsspionage die staatlich gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen, Betrieben und Forschungseinrichtungen (BT-Drs. 18/2281 [2014], S. 2f.). Die Wirtschaftsspionage, deren Ziel die Förderung der Wirtschaft eines fremden Staates ist, wodurch auch politische Interessen involviert sind, gehört in den Bereich der Staatsschutzkriminalität und damit in das klassische Strafrecht.

Unter Konkurrenzausspähung fällt die private Ausforschung eines konkurrierenden Unternehmens (vgl. Dannecker 1987). Letztere verfolgen kommerzielle Interessen und sind an einer produktbezogenen Informationsbeschaffung interessiert. Im Gegensatz zur unerlaubten Informationsbeschaffung und -auswertung ist das reine Sammeln, Aggregieren und Auswerten öffentlich zugänglicher Daten (die sogenannte Competitive Intelligence) im Rahmen bestehender Datenschutzgesetze rechtmäßig (Röder 2011; Scherf 2013).

3. Stand der Forschung

Wissenschaftliche Studien zur Wirtschaftskriminalität i.w.S. liegen nur in begrenztem Umfang vor. Sie können vier Kategorien zugeordnet werden: (1.) normativ orientierte Publikationen, (2.) Artikel mit polizeiorientiertem Schwerpunkt, (3.) wirtschaftsnahe Studien sowie (4.) empirische Forschungsstudien. Dieser Mangelzustand erschwert die empirische Annäherung an das Phänomen und den Vergleich der jeweils präsentierten Daten.

Die normative Literatur beschränkt sich in der Hauptsache auf die Erörterung rechtlicher Fragestellungen (z.B. Oehler 1978). Einschlägig ist neben (wirtschafts-)strafrechtlich orientierten Titeln vor allem die wettbewerbsrechtliche Literatur. Soweit der normative Reformbedarf in Deutschland erörtert wird, überwiegt mit Verweis auf die Veränderungen in der Tatphänomenolo-

gie die Schlussfolgerung, dass die aktuelle Rechtslage den Veränderungen in den Vorgehensweisen (modi operandi) und den Bedürfnissen der Akteure (Betroffene wie auch Behörden) nicht mehr angemessen sei (z.B. Többens 2000). Insgesamt sind Titel zu dem hier behandelten Deliktspektrum gemessen an der vor allem wirtschaftlichen Bedeutung auffällig unterrepräsentiert.

Empirisch ausgerichtete Forschungsarbeiten sind zumeist auf die qualitative und quantitative Analyse des Hellfeldes und Probleme der internen und externen Kontrolle und Intervention fokussiert. Hierzu liegen zum einen polizeiorientierte Literaturquellen vor, die primär kriminalistische und technische Spezialfragen behandeln. Einige andere Publikationen haben konkrete Fallbeschreibungen zum Gegenstand (z.B. Engberding 1993, Nathusius 2001, Fritsche 2001). Auch wenn diese mitunter temporäre Erscheinungsformen adressieren, vermitteln sie im Zeitverlauf einen nützlichen Einblick in die phänomenologischen Entwicklungsprozesse. In jüngerer Zeit erschließen sich die mit der Entwicklung im Bereich der IuK- bzw. Cyber-Kriminalität verbundenen Zuordnungsprobleme im Hellfeld auch aus den in den Lagebildern des BKA präsentierten Daten (Lagebilder Cybercime und Wirtschaftskriminalität) sowie übergreifend in der Polizeilichen Kriminalstatistik (PKS). Obwohl es sich hier um statisches Material im engeren Sinne handelt, können diese Quellen der polizeiorientierten Literatur mit zugeordnet werden, da sie die Arbeitsabläufe der Polizeibehörden widerspiegeln. Einen ergänzenden Einblick erlauben ferner einige regional begrenzte Sonderveröffentlichungen von Verfassungsschutzbehörden (z.B. baden-württembergisches Landesamt für Verfassungsschutz 1997, 1998, 2006). Insgesamt stützen die verfügbaren Quellen die forschungsleitende Annahme, dass die in der PKS ausgewiesenen Daten das aktuelle Hellfeld der Wirtschaftsspionage i.w.S. für Deutschland zum Teil unzutreffend und insgesamt nur unvollständig abbilden. Diese Schlussfolgerung gilt erst recht angesichts des Umstandes, dass die projektrelevante, in § 99 Strafgesetzbuch (StGB) normierte ‚klassische' Wirtschaftsspionage, in Form der Agententätigkeit (Wirtschaftsspionage i.e.S.) nicht in der PKS ausgewiesen wird, sondern einer der Öffentlichkeit und der Forschung unzugänglichen Polizeilichen Kriminalstatistik Staatsschutz (PKS-S) vorbehalten ist.

Zum Dunkelfeld im Bereich der Wirtschaftskriminalität existieren einige neuere Publikationen wirtschaftsnaher Einrichtungen. Mit den Studien von KPMG (2006), PricewaterhouseCoopers (PwC) (2011, 2016) und Corporate Trust (CT) (2012, 2014) liegen mehrere zeitlich unterschiedlich aktuelle Untersuchungen zum Dunkelfeld im Bereich der Wirtschaftskriminalität mit dem Fokus auf der Viktimisierungsperspektive von Unternehmen vor. Danach ist von einem hohen Bedrohungspotenzial auszugehen: 13 % der von PwC Be-

fragten berichteten für das Jahr 2011 von konkreten Verdachtsfällen in ihrem Unternehmen bezogen auf Industrie- und Wirtschaftsspionage, weitere 23 % bezogen sich auf Diebstahl vertraulicher Unternehmensdaten; 31 % bzw. 37 % schätzen die Häufigkeit dieser Delikte als hoch oder sehr hoch ein. KPMG (e-Crime-Studie, 2010) und CT (2012) lassen das Dunkelfeld unter Einbeziehung von Cyber- bzw. IuK-Kriminalität insgesamt, die allerdings über das hier relevante Deliktsspektrum hinausgeht, noch wesentlich größer erscheinen. Die letztgenannten Studien präsentieren auch einige Daten zum Anzeigeverhalten. Danach scheint die Furcht vor Reputationsschäden oder möglicher Regressforderungen die Anzeigebereitschaft häufiger negativ zu beeinflussen als grundsätzliche Berührungsängste mit Behörden. Faktisch werden im Schadensfall weit häufiger externe Sicherheitsspezialisten eingeschaltet als Sicherheitsbehörden (CT 2012, 2014). Aber auch andere Motive können handlungsleitend sein. Die Schaffung bedarfsgerechter organisatorischer Kooperationsgrundlagen mit den Sicherheitsbehörden bildet denn auch eine der Kernforderungen des Bundesverbands der Deutschen Industrie (BDI) (Positionspapier 2012). Die präsentierten Befunde unterstreichen den Bedarf an einer vertiefenden, speziell auf den Bereich der Wirtschaftsspionage i.w.S. ausgerichteten wissenschaftlichen Exploration.

Breiter angelegte und speziell auf Betriebs- bzw. Wirtschaftsspionage fokussierte empirische Studien liegen schließlich aus den 1970er (z.B. Amelunxen 1977) und 1980er Jahren (z.B. Liebl 1987, Tuck/Liebl 1988) vor. Diese sind allerdings sowohl im Hinblick auf die Tatphänomenologie als auch auf die Bedrohungsszenarien nicht mehr aktuell. Der Vergleich der heutigen Situation mit den dort beschriebenen Szenarien vermag freilich die signifikanten Veränderungsprozesse in dem untersuchten Bereich anschaulich zu illustrieren. Darüber hinaus unterstreicht der Vergleich die Überfälligkeit einer neuen, umfassend angelegten Untersuchung, die neben den Veränderungen in der Tatphänomenologie auch die heutigen gesellschaftlichen und politischen Rahmenbedingungen berücksichtigt.

4. Aktuelle Situationsbeschreibung

Beleuchtet wird ein Deliktsbereich, der empirisch bislang nur rudimentär erforscht ist. Dies betrifft die normative Ebene ebenso wie die phänomenologische und anwendungspraktische. Das Vorhaben ist erforderlich, um die Herausforderungen an die (unternehmens-)interne und externe (staatliche) Kontrolle praxisnah zu analysieren und Möglichkeiten einer Optimierung zu untersuchen. Der Fokus wird dabei bewusst nicht auf große Industrieunter-

nehmen bzw. sogenannte global player gerichtet, da diese häufig die eigene Angriffsanfälligkeit und drohende Schadenssummen bewusst kalkulieren und dementsprechend selbst aktiv für Präventions- und Kontrollmechanismen sorgen. Sie handeln im Falle eines Angriffs also häufig autonom, d.h. ohne Einschaltung (nationaler) Strafverfolgungsbehörden (Bundesamt für Verfassungsschutz [BfV], Juli 2014, S. 6). Stattdessen richtet sich der Blickwinkel im WiSKoS-Projekt auf kleine und mittelständische, deutsche Unternehmen (KMU), die als sog. hidden champions durchaus am internationalen Markt agieren können.[1] Wenn KMU von Spionageaktivitäten betroffen sind, sind sie eher auf eine Kooperation mit staatlichen Behörden angewiesen als Großkonzerne (Bundesamt für Verfassungsschutz, Juli 2014, S. 6).

Betrachtet man die Ausgangslage der Materie, ist zunächst festzustellen, dass diese an der Schnittstelle zwischen (traditioneller) Staatsschutz- und (moderner) Wirtschaftskriminalität angesiedelt ist. Das Grundverständnis der zu untersuchenden Deliktsformen ist ebenso wie der gesetzliche Rahmen und die organisatorische Zuständigkeitsverteilung zwischen den Strafverfolgungsbehörden noch wesentlich von der bis zum Ende der 1980er Jahre dominierenden Ost-West-Konfrontation geprägt. Seit dem Ende des sog. Kalten Krieges haben sich die politischen Rahmenbedingungen grundlegend verändert. Ehemalige politische Fronten haben sich aufgelöst und wurden in vielen Fällen durch wirtschaftliche Kooperationen abgelöst. Gleichzeitig sind jedoch auch neue Freund-Feind-Schemata entstanden, die sich an den jeweils aktuellen politischen Interessen orientieren und Angriffe auf Unternehmens-Know-hows aus bestimmten Regionen weiterhin der Staatskriminalität zuordnen, während Täter aus dem befreundeten Ausland als „friendly spies“ (Schweizer 1993) erscheinen und entsprechende Vorfälle – wenn überhaupt – nur sehr zögerlich verfolgt werden.

Gleichzeitig kann die unreflektierte Subsumtion dieser Deliktsphänomene unter das klassische Verständnis der Staatsschutzkriminalität im Hinblick auf die politische Entwicklung in Europa immer weniger überzeugen. Nach der weitgehenden Vollendung des gemeinsamen europäischen Marktes stellt sich beispielsweise die Frage, ob die nationale Volkswirtschaft vor dem Hintergrund der heutigen europarechtlich bestimmten Wirtschaftsverfassung überhaupt noch ein tragfähiges Rechtsgut im Sinne der traditionellen deutschen Strafvorschriften zur Wirtschaftsspionage (vgl. § 99 StGB) sein kann (Metzler

[1] Laut einer Sekundäranalyse des Bundeskriminalamts (BKA) aus dem Jahr 2014, treten KMU hinter großen Unternehmen in der Forschung zurück (vgl. *Kasper* 2014). Für mehr Informationen über *hidden champions* vgl. *Simon* (2007); Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Archiv/1097117105/hidden-champions-v1.html [10.05.2016].

1990). Unabhängig von dieser Frage dürfte heute den nichtstaatlich initiierten Formen des illegalen Knowhow-Abzuges, die in Deutschland unter den Straftatbestand der Konkurrenzausspähung (vgl. § 17 Gesetz gegen den unlauteren Wettbewerb [UWG]) subsumiert werden, sehr viel größere praktische Relevanz zukommen. Dies legen die insgesamt lückenhaften statistischen Zahlen zum Fallaufkommen für Deutschland sowohl in der PKS wie auch im Lagebild Wirtschaftskriminalität ebenso nahe wie verschiedene einschlägige Viktimisierungsbefragungen aus der Wirtschaft.

In Anbetracht dieser rechtstatsächlichen Entwicklung ist ferner zu fragen, ob die in Deutschland bis dato tradierte Unterscheidung entlang der staatlichen (nachrichtendienstlichen) bzw. nicht-staatlichen (kommerziellen) Urheberschaft von Angriffen einschließlich der damit einhergehenden verfahrensrechtlichen Differenzierungen aus Sicht der betroffenen Unternehmen – soweit die konkrete Urheberschaft für die Betroffenen überhaupt erkennbar wird – nicht weithin irrelevant ist. Handlungsleitend dürften aus Betroffenensicht primär die eingetretenen oder befürchteten materiellen und immateriellen Schäden sein. Angesichts der etablierten Strukturen mit verschiedenen Zuständigkeiten, die sich teilweise ergänzen (z.B. verschiedene Behördenebenen innerhalb eines Landes), teilweise aber auch exklusiven Charakter haben (zentrale Ermittlungskompetenz des Generalbundesanwaltes, vgl. § 142a Gerichtsverfassungsgesetz [GVG]), könnte sich aus Sicht der Strafverfolgungsbehörden die Unterscheidung sogar als kontraproduktiv darstellen. All dies nährt die Frage, ob diese Unterscheidung in Anbetracht der weitgehenden Identität der Angriffsziele wie auch der Durchführung (modi operandi) noch zielführend ist. Die gegenwärtigen Strukturen können nicht nur die effektive innerstaatliche Verfolgung erschweren, sondern auch die internationale und grenzüberschreitende Zusammenarbeit einschließlich der Rechtshilfe.

Mit der fortschreitenden Entwicklung von IT und korrespondierender IT-Kriminalität hat sich in den letzten Jahren zugleich das Erscheinungsbild der Wirtschaftsspionage grundlegend verändert. Die Materie weist heute signifikante Bezüge zur sog. Informations- und Kommunikations (IuK)- oder Cyber-Kriminalität auf. Die Schnittmenge ist weithin unbekannt, dürfte aber beachtlich sein (KPMG 2010, CT 2014, PwC 2016). Dadurch dürfte das statistische Abbild der Wirtschaftsspionage (Hellfeld) nicht unwesentlich verzerrt werden. So können Fehlzuordnungen beispielsweise überall dort auftreten, wo kein konkreter Datenabfluss festgestellt wird, oder in Situationen, wo der (vermeintliche) nachrichtendienstliche Bezug von IT-Angriffen unerkannt bleibt. Dies gilt insbesondere bei Zugriffsversuchen, die erfolgreich abgewehrt werden und daher als (bloße) Sabotagefälle oder Hackeraktivitäten erscheinen

können. Deren eigentliche Zielrichtung bleibt in der Regel unbestimmbar (vgl. Bundeskriminalamt, Lagebild Cybercrime 2011, S. 9). Noch schwerer erkennbar sind Abgriffe über die (mobile) Telekommunikation, die (erst) außerhalb der technisch kontrollierten Infrastruktur der Unternehmen ansetzen (KPMG 2010). Die Digitalisierung hat im Übrigen auch den physischen Diebstahl über Datenträger signifikant erleichtert: Das offene (USB-Stick, Handy, iPod) und getarnte Mitführen von Speichermedien (Autoschlüssel bzw. Schlüsselattrappen, u.v.a.m.) ist per se nicht unbedingt verdachtsauslösend und nicht flächendeckend kontrollierbar. Dies kann zur Folge haben, dass eigentlich relevante Fälle aufgrund bestimmter phänomenologischer und/oder prozessualer Charakteristika in den offiziellen Statistiken unter Kategorien ausgewiesen werden, die die Zielsetzung oder den phänomenologischen Kontext nicht bzw. nicht mehr erkennen lassen. Man könnte diesbezüglich von einem ‚verborgenen Hellfeld' sprechen. Theoretisch kann jeder Angriff bzw. Zugriff auf ein IT-System von außen einen Zusammenhang mit Wirtschaftsspionage i.w.S. aufweisen. Weil jedoch gerade die Zielsetzung, die normativ das entscheidende rechtliche und zuständigkeitsbestimmende Unterscheidungsmerkmal darstellt, der am schwierigsten festzustellende Aspekt ist, dürfte die abschließende statistische Erfassung – besonders in Unbekannt-Fällen – nicht selten zufallsbestimmt sein.

Charakterisiert wird der Deliktsbereich ferner durch ein doppeltes Dunkelfeld. Neben den erwähnten Problemen der Erkennbarkeit sind die Betroffenen auch im Verdachtsfall mit spezifischen Reaktionsüberlegungen konfrontiert, die die Option der Nichtanzeige aus Unternehmenssicht unter verschiedenen Aspekten – z.B. Furcht vor Reputationsschaden, Gefährdung von Betriebsgeheimnissen, etc. – als vorzugswürdige Reaktion erscheinen lassen. Entsprechend schwierig kann sich die Kooperation der Unternehmen mit den Strafverfolgungsbehörden gestalten (und umgekehrt).

5. Regulatorischer Rahmen in Deutschland und Konsequenzen für die Praxis

Gegenwärtig ist der regulatorische Rahmen in mehrfacher Hinsicht als fragmentiert zu bezeichnen. Bei der ‚klassischen' Wirtschaftsspionage i.e.S., normiert in § 99 StGB als geheimdienstliche Agententätigkeit, handelt es sich um Staatsschutzkriminalität. Die Planung und Ausführung wird organisiert durch oder für einen fremden Staat und dient breit angelegter Informationsbeschaffung – wobei sowohl eine positive Zielsetzung (Akquise von Daten für den Drittstaat) als auch eine negative Zielsetzung (Sabotage wirtschaftlicher Ak-

tivitäten im angegriffenen Staat) in Betracht kommt. Der Tatbestand ist als Offizialdelikt ausgestaltet und sieht im Strafmaß eine Freiheitsstrafe bis zu zehn Jahren vor. Es besteht eine Sonderzuständigkeit des Generalbundesanwalts gem. §§ 74a, 142a GVG. Weiterhin liegen konkurrierende Aktivitäten der Dienste vor und der Einfluss politischer Ermittlungsvorbehalte ist zumindest nicht auszuschließen.

Die Konkurrenzausspähung ist außerhalb des StGB in den §§ 17 ff. UWG normiert und dem Bereich der Wirtschaftskriminalität zuzuordnen. Sie dient zuallererst der produktbezogenen Informationsbeschaffung, deren Planung und Ausführung durch bzw. für einzelne, konkurrierende Unternehmen im In- oder Ausland erfolgt. Darüber hinaus sind auch sämtliche Geschäftsgeheimnisse im weiteren Sinne stets ausspährelevant, sobald sie unberechtigten Dritten irgendeine Aussicht auf einen kommerziellen Nutzen bieten (Kundenverzeichnisse, Preiskalkulationen, Strategiepapiere, Marktanalysen, u.v.a.m.). Auch der Staat selbst kann z.B. bei Patentgerichten, Aufsichts- oder Wettbewerbsbehörden, Ausschreibungs- und Vergabestellen, etc. Zielobjekt der Ausspähung sein. Der Tatbestand sieht im Strafmaß eine Geld- oder Freiheitsstrafe bis zu fünf Jahren vor und ist als Antragsdelikt ausgestaltet, wobei das Antragserfordernis bei Bestehen eines öffentlichen Interesses an der Strafverfolgung behördenseitig ersetzt werden kann. Es besteht eine Sonderzuständigkeit gem. § 74c GVG bei den Schwerpunktstaatsanwaltschaften.

Charakteristisch für den Deliktsbereich sind zum einen die weithin identischen modi operandi und die Zielsetzung der illegalen Beschaffung von Knowhow und sonstigen Informationen, zum anderen die weitgehende Identität der Angriffsziele – nämlich die Eigentümer von geistigem Eigentum wie Betriebs- und Geschäftsgeheimnissen –, die nicht nur aus der Wirtschaft, sondern auch aus Wissenschaft und Forschung stammen können. Der Unterschied zwischen Wirtschaftsspionage und Konkurrenzausspähung liegt auf der inhaltlichen Ebene allein in der unterschiedlichen Motivation, die einmal auf einen wirtschaftlichen Vorteil, einmal auf politischen Nutzen gerichtet ist.

Daraus ergeben sich kriminologische und (rechts-)politische Folgefragen:

- Ist die traditionelle Unterscheidung der beiden Deliktsbereiche aus Opfersicht relevant?
- Ist sie im Angriffsfall überhaupt erkennbar?
- Ist sie im globalisierten Wirtschaftsraum noch zeitgemäß?
- Ist der Bezug ökonomischer Interessen zur nationalen Sicherheit noch begründbar? Verweist der Rekurs auf die nationale Volkswirtschaft im gemeinsamen Markt der EU nur mehr auf ein fiktives Rechtsgut? Wie lassen sich Zuständigkeiten bei multinationalen Unternehmen bestimmen?

– Ist die Unterscheidung in Wirtschaftsspionage und Konkurrenzausspähung auf Grund des beschriebenen Zuständigkeitssplittings bei den Behörden ggf. sogar kontraproduktiv?

In der Praxis haben die beschriebenen regulatorischen Rahmenbedingungen mitunter weitreichende Konsequenzen. So ergibt sich aus dem Zuständigkeitssplitting auch eine Zuständigkeitskonkurrenz, die in ‚unklaren' Fällen, in denen Urheber und Zielsetzung unbekannt oder zweifelhaft sind, praktische Probleme bereitet. Ist der Urheber ein ausländischer Geheimdienst, ein Konkurrenzunternehmen, ein (ggfs. ehemaliger) Mitarbeiter, ein Lieferant oder nur ein privater (Freizeit-) Hacker? Eine mögliche Konsequenz dieser Unsicherheit kann die Einstellung von Ermittlungen und Verfahren sein. Daraus wiederum leiten sich Folgeproblematiken für die statistische Erfassung ab. Aufgeklärte Fälle liegen nur in geringem Maße vor und können als statistisch unterrepräsentiert angesehen werden. Die statistische Erfassung ‚unklarer' Fälle erfolgt häufig ohne Bezug zur Wirtschaftsspionage (i.w.S.) – z.B. als (versuchter oder vollendeter) Diebstahl, Untreue oder Cyberkriminalität – und ist mitunter zufallsgeleitet. Dadurch entsteht ein ‚verborgenes' Hellfeld: Obwohl die Fälle formal erfasst werden, wird die Zuordnung zu dem Phänomen Wirtschaftsspionage (i.w.S.) nicht erkennbar, sodass ihre tatsächliche quantitative Relevanz in den Kriminalstatistiken nicht abgebildet wird.

6. Ausblick: das Projekt WiSKoS

Alle hier angesprochenen Punkte sollen in dem Projekt WiSKoS untersucht werden. Im Hinblick auf die weit fortgeschrittene Entwicklung des gemeinsamen europäischen Marktes wurde die systematische Untersuchung europaweit angelegt. Neben einer Bestandsaufnahme des rechtlichen und rechtstatsächlichen Status Quo im Inland umfasst der Forschungsplan die Suche nach möglichen Alternativmodellen und -strategien im europäischen Ausland. Insgesamt werden drei Zielsetzungen verfolgt:

– Die systematische Analyse der heute im gemeinsamen europäischen Wirtschaftsraum implementierten Systeme zur Kontrolle der Wirtschaftsspionage i.w.S. (Prävention und Repression).
– Die empirische Ausleuchtung des Hell- und Dunkelfeldes in Deutschland, insbesondere die durch verschiedene empirische Zugänge abgesicherte Analyse der gegenwärtigen Bedrohungslage und der quantitativen Relevanz der wichtigsten modi operandi, wobei die erstere Analyse die Einschätzung der Wirtschaft hinsichtlich der Bedrohungslage einerseits und der Zusam-

menarbeit zwischen Unternehmen und staatlichen Organen andererseits einschließt.
– Die Suche nach anderen, gegebenenfalls vorzugswürdigen Präventions- und Verfolgungsstrategien in ausgewählten europäischen Rechtsordnungen und ihre Bewertung aus der Sicht der wichtigsten Stakeholder in Deutschland. Diese sind die betroffenen Unternehmen (unter Berücksichtigung der Wissenschaft) sowie die Strafverfolgungsbehörden. Dabei ist das Ziel die Entwicklung optimierter, aufeinander abgestimmter Schutz- und Reaktionskonzepte für diese Endnutzergruppen.

Das Vorhaben ist in drei Module (M 1 bis M 3) unterteilt (siehe Abbildung 1), die in sich abgeschlossen Arbeitseinheiten mit jeweils eigenständigem inhaltlichen und geographischen Fokus sowie spezifisch darauf zugeschnittener Methodenwahl bilden. Zugleich sind die Inhalte der Module eng aufeinander abgestimmt und bauen aufeinander auf. Untergliedert ist das Projekt ferner in insgesamt neun Arbeitspakete (A 1 bis A 9). Die Projektkonzeption ist auf die europäische Anschlussfähigkeit hin ausgerichtet. Die speziell auf Deutschland zugeschnittenen Arbeitspakete können mit passender europäischer Anschlussfinanzierung gegebenenfalls in anderen Ländern repliziert werden.

Im ersten Modul geht es zunächst um ein Screening der in den 28 EU-Mitgliedsstaaten sowie (stellvertretend für die eng mit der EU verbundenen EFTA-Länder) der Schweiz implementierten nationalen Regelungen und eine (Grob-)Einordnung der jeweiligen Bedrohungslage auf der Grundlage existierender statistischer Materialien. Diese Feldbeschreibung ist methodisch deskriptiv und normativ angelegt und schließt eine sozio-kulturelle Analyse des Verhältnisses von Staat und Wirtschaft ein.[2] Die Analyse dient weiterhin der Identifizierung exemplarischer Länder, die im zweiten Modul als Vergleichsgruppe mit Deutschland kontrastiert werden. Identifiziert werden sollen hierfür Länder, die sich von Deutschland im Hinblick auf die grundsätzliche Wirtschaftsverfassung (Verhältnis Staat – Wirtschaft), auf die Art der (strafrechtlichen und außerstrafrechtlichen) Regulierung der Wirtschaftsspionage i.w.S. und auf die konkrete Bedrohungslage, die sich sowohl aus der Existenz bestimmter Industrie- und Wirtschaftszweige und der daraus resultierenden potenziellen Attraktivität der Angriffsziele (Dunkelfeld) als auch aus Hellfelddaten (also der tatsächlichen Anzahl und der Struktur von offiziell registrierten Verdachtsfällen) ergeben kann, unterschieden.

[2] Das Ergebnis des Länderscreenings wird voraussichtlich im 2. Halbjahr 2016, als erste von mehreren WiSKoS-Meilensteinpublikationen, hrsg. v. den Verf., als Band K 176 der Kriminologischen Forschungsberichte aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht, erscheinen.

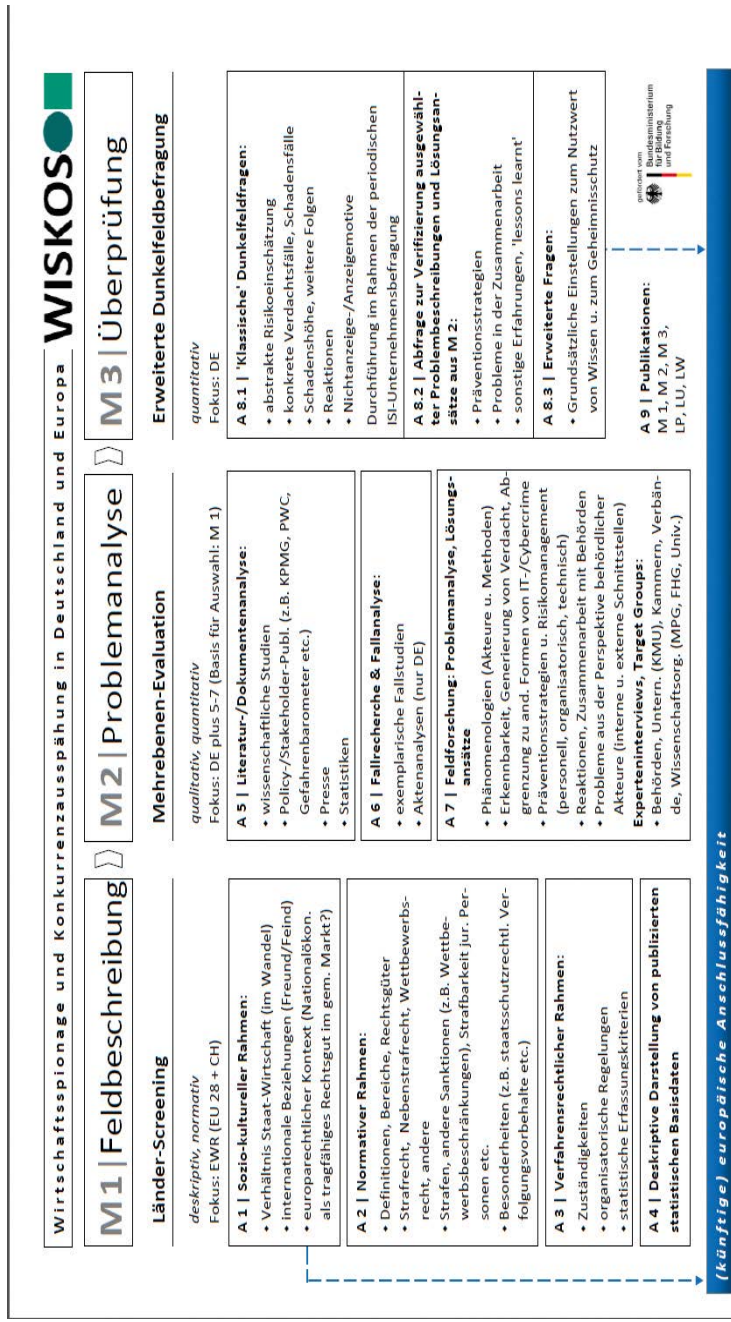

Abb. 1: WiSKoS-Projektdesign

Die im Zuge des Länder-Screenings identifizierten Länder sollen im Rahmen mehrerer Arbeitspakete im zweiten Modul sodann einer ausführlichen Mehrebenen-Evaluation unterzogen werden. Diese Problemanalyse kombiniert sowohl qualitative als auch quantitative Untersuchungsmethoden. Neben der Analyse relevanter Literatur- und Dokumentenquellen sollen konkrete Fallanalysen einen Einblick in Fälle und Praktiken der polizeilichen und justiziellen Aufklärungsarbeit einschließlich der jeweiligen Problemkonstellationen geben. Für Deutschland kann Letzteres mit dem Mittel einer detaillierten Aktenanalyse geleistet werden, für die ausländischen Rechtsordnungen wird sich die Analyse auf die Identifizierung und Auswertung exemplarischer Fallstudien beschränken müssen.

Ein weiteres wesentliches Element wird eine empirische Feldforschung sein, welche auf der Basis von Workshops und ergänzenden qualitativen Interviews Szenarien, Probleme und Lösungsansätze aus der Perspektive der wichtigsten Stakeholder aus den zu untersuchenden Ländern analysieren soll. Der Fokus liegt neben Behördenvertretern auf Wirtschaftsunternehmen ausschließlich der Rüstungsindustrie, die eine Sonderrolle einnimmt. Der Schwerpunkt soll auf dem Bereich der KMU liegen. Explizit einbezogen werden soll darüber hinaus aber auch der Wissenschaftssektor einschließlich der aus der Wissenschaft hervorgehenden Start-ups. Neben Deutschland werden fünf im Projektverlauf zu selektierende Länder rechtsvergleichend auf die dortige Lage hin untersucht.

Das dritte Modul dient schließlich der Überprüfung der im zweiten Modul erarbeiteten Situations- und Lösungsbeschreibungen. Die identifizierten Probleme und kontrastierenden Lösungsansätze auf der Gesetzgebungs- und der Anwenderebene (unternehmerische und behördliche Stakeholder) in den untersuchten ausländischen Rechtsordnungen sollen auf ihre mögliche Übertragbarkeit auf Deutschland hin analysiert werden. Dies dient, mit dem expliziten Fokus auf die hiesigen Endnutzer, der Rückkopplung der vorherigen Ergebnisse und generiert zugleich die endnutzerbezogenen Endprodukte (Nutzerleitfäden mit Empfehlungen für Unternehmen, Wissenschaft und Behörden), die die wissenschaftlichen Publikationen ergänzen sollen. Die hierfür am besten geeignete Methode ist eine erweiterte Dunkelfeldbefragung, die sich aus drei Elementen zusammensetzt. Neben der quantitativen Aufhellung des Dunkelfeldes sollen zunächst einige ‚klassische' Dunkelfelditems abgefragt werden, die im Bereich der Wirtschaftsspionage i.w.S. relevant sind. Mit einem kleinen Bündel von grundsätzlichen Einstellungsfragen zum Geheimnisschutz sowie zum Nutzwert abgezogenen Wissens soll dann die traditionelle Opferperspektive erweitert und um den Aspekt abstrakter unternehmerischer

Kosten-Nutzen-Abwägungen in dem Bereich der Konkurrenzausspähung ergänzt werden. Schließlich soll das Meinungsbild der deutschen Unternehmen zu einer möglichen Übertragbarkeit der Schlüsselbefunde aus den ausländischen Problem- und Problemlösungsschilderungen erfragt werden ("Proof-of“-Konzept).

Literatur

Amelunxen, C. (1977): Spionage und Sabotage im Betrieb, Heidelberg: Kriminalistik-Verlag.

Bundesamt für Verfassungsschutz (Juli 2014): Wirtschaftsspionage. Risiko für Unternehmen, Wissenschaft und Forschung, www.verfassungsschutz.de/de/download-manager/_broschuere-2014--07-wirtschaftsspionage.pdf [10.05.2016].

Bundesministerium für Bildung und Forschung (BMBF), Referat Sicherheitsforschung (2012): Forschung für die zivile Sicherheit 2012–2017. Rahmenprogramm der Bundesregierung, Bonn, www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf [10.05.2016].

Bundesverband der Deutschen Industrie e.V. (2012): Positionspapier Wirtschaftsschutz in der deutschen Industrie stärken, Berlin 2012, www.bdi.eu/download_content/Marketing/Positionspapier_online(2).pdf [10.05.2016].

CorporateTrust (2012): Cyberwar – Industriespionage 2012, München 2012, www.corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf [10.05.2016]. (Zit. CT 2012)

CorporateTrust (2014): Cybergeddon – Industriespionage 2014, München 2014, www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf [10.05.2016]. (Zit. CT 2014)

Dannecker, G. (1987): Der Schutz von Geschäfts- und Betriebsgeheimnissen, Betriebsberater 1987, S. 1614ff.

Engberding, R. (1993): Spionageziel Wirtschaft. Technologie zum Nulltarif, Düsseldorf: VDI-Verlag.

Fritsche, K.-D. (2001): Wirtschaftsspionage: Schutz der deutschen Wirtschaft vor Ausspähung und Know-how-Abfluss, Kriminalistik 2001, S. 476ff.

Kasper, K. (April 2014): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse, Bundeskriminalamt (BKA), www.bka.de/DE/Publikationen/Publikationsreihen/SonstigeVeroeffentlichungen/SonstigeVeroeffentlichungen__node.html?__nnn=true [10.05.2016].

KPMG (2006): Studie 2006 zur Wirtschaftskriminalität in Deutschland, Köln: KPMG, www.kpmg.de/Presse/3021.htm [10.05.2016].

KPMG (2010): e-Crime-Studie 2010, Computerkriminalität in der deutschen Wirtschaft, [o.O.], www.kpmg.de/docs/20100810_kpmg_e-crime.pdf [10.05.2016].

Liebl, K. (Hrsg.) (1987): Betriebsspionage – Begehungsformen, Schutzmaßnahmen, Rechtsfragen, Ingelheim: Peter Hohl Verlag.

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

Nathusius, I. (2001): Wirtschaftsspionage: Der Versuch sachlicher Analyse eines häufig dämonisierten Phänomens, Kriminalistik 2001, S. 243ff.

Naucke, W. (1996): Die strafjuristische Privilegierung staatsverstärkter Kriminalität, Juristische Abhandlungen Band 29, Frankfurt am Main: Klostermann Verlag.

Oehler, D. (Hrsg.) (1978): Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der Europäischen Gemeinschaft sowie in Österreich und der Schweiz, Band I und II, Köln u.a.: Heymanns.

PricewaterhouseCoopers (2011): Wirtschaftskriminalität 2011, 2. aktualisierte Aufl., Halle-Wittenberg: Martin-Luther-Universität. (Zit. PwC 2011)

PricewaterhouseCoopers (2016): Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016. Halle-Wittenberg: Martin-Luther-Universität. (Zit. PwC 2016)

Röder, N. (2011): Industriespionage. Risikofaktor Mensch. Masterarbeit, Fachhochschule Hannover, http://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/298 [10.05.2016].

Scherf, A. (2013): Gefahren der Wirtschaftsspionage und Auswirkungen auf das IT-Projektmanagement, www.pst.ifi.lmu.de/Lehre/wise-12--13/jur-pm/ausarbeitung-zum-vortrag-am-08.01.2013-a.-scherf [21.04.2016].

Schweizer, P. (1993): Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets. NY: Atlantic Monthly Press.

Simon, H. (2007): Hidden Champions des 21. Jahrhunderts: die Erfolgsstrategien unbekannter Weltmarktführer. Frankfurt: Campus.

Többens, H. (2000): Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, NStZ 2000, S. 505ff.

Tuck, J., Liebl, K. (Hrsg.) (1987): Direktorat T – Industriespionage des Ostens, Heidelberg: Kriminalistik-Verlag.