Security Journal (2020) 33:6–26
https://doi.org/10.1057/s41284-019-00199-1

ORIGINAL ARTICLE

Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries

Susanne Knickmeier[1]

Published online: 24 September 2019

Abstract
Industrial and economic espionage are underestimated criminal offences. Although the phenomena are diffuse and ambiguous, they can result in enormous material and immaterial damage. Referring to results from the German research project WISKOS, the phenomenon of obtaining trade secrets (including the offenders, modi operandi, affected trade secrets, outflow of trade secrets and detection abilities) are described, as too are possible countermeasures and associated law enforcement difficulties. Considering the phenomenological results, potential preventive measures based on the situational crime prevention and deterrence strategies are listed. Legal regulations and sanctions in Austria, Bulgaria, Denmark, Germany, Switzerland and the United Kingdom are compared. Lastly, based on the outcomes of criminal proceedings, it is discussed whether the existing criminal law is an appropriate measure to deter potential offenders.

Keywords Criminal proceedings · Deterrence strategies · Economic espionage · Industrial espionage · Trade secrets

Introduction

Over the past months, possible acts of economic espionage by the Chinese company Huawei have been discussed by the European Union (EU). Moreover, the European Commission has considered proposals to exclude Huawei from the continent's 5G network (Emmott et al. 2019). A few years ago, the American National Security Agency (NSA) was accused of engaging in economic espionage in Europe and passing secret information to national companies (Thomson 2015).

✉ Susanne Knickmeier
s.knickmeier@mpicc.de

[1] Department of Criminology, Max Planck Institute for Foreign and International Criminal Law, Günterstalstr. 73, 79100 Freiburg, Germany

In 2011, an engineer employed by AMSC Windtec GmbH, an Austrian subsidy of the American AMSC group, was arrested for passing important source code to the Chinese company Sinovel (Zirm 2013). In this case, the Chinese company took advantage of a situation in which they became aware of an unsatisfied and disgruntled employee (Budras 2014). They offered him a large payment and a new job in China. In return, the Austrian offender copied secret source code and passed it on to Sinovel, which enabled them to build wind farms and power plants on their own (Hofer and Weiß 2016, p. 1).

Referring to evidence presented at trial in the US, AMSC lost around one billion dollars in shareholder equity and around 700 jobs worldwide (US Department of Justice 2018a). This publicly well-documented case comprehensively illustrates how the straightforward disclosure of data can cause enormous damage (including the loss of many jobs), as well as how such data breaches can be detected by attentive employees. But it also points out the (legal) limitations of international law enforcement (e.g., missing international judicial agreements). While the Austrian employee was imprisoned for 3 years and fined €200,000 in Austria (Zirm 2013), it was impossible to sentence the Chinese offenders in Austria, since there is no extradition agreement between China and Austria and no legal ability to judge them in absentia in Austria. Nor could the offenders be sentenced in absentia in the US. Due to the *ne bis in idem* principle, regulated in Art. 6 of the Extradition Agreement between Austria and the US, the Austrian offender was not extradited from Austria to the US. In 2018, Sinovel was convicted of conspiracy to commit trade secret theft, theft of trade secrets, and fraud by an American court (US Department of Justice 2018a). The court imposed the maximum statutory fine of 1.5 million dollars (US Department of Justice 2018b).

Such cases of economic and industrial espionage serve as a reminder about the potential risks, difficulties in law enforcement, and necessity to combat the phenomenon. However, the phenomenon is diffuse and ambiguous and many unanswered questions exist: What do we mean, when we talk about economic and industrial espionage? Who are the offenders, what are their motives and modi operandi? Are there convincing detection systems? Which legal and preventive measures are available to combat acts of espionage? What are the challenges for criminal and procedural law?

Referring to case studies conducted in six European countries (Austria, Bulgaria, Denmark, Germany, Switzerland, and the United Kingdom (UK)) that were part of the German research project WISKOS, this article discusses how to combat and prevent economic and industrial espionage. To begin with, the phenomenon of obtaining trade secrets is described: including the offenders, modi operandi, affected trade secrets and detection abilities. Thereafter, the development of preventive measures, as well as the use of criminal proceedings and deterrents, will be discussed.

Definition of, and differentiation between, economic and industrial espionage

Distinguishing between economic and industrial espionage is vital, as it leads to various legal consequences and responsibilities of authorities. However, in each of the (abovementioned) surveyed countries, the terms ‘economic’ and ‘industrial’

espionage are not consistently applied or legally defined in law. Rather, different criteria are used to differentiate and define the phenomena.

In England, a variety of terms are used in legal terminology and everyday language, for example, economic espionage, industrial espionage, or cyber espionage. In official documents, industrial espionage is described as being different from state espionage, but clear-cut lines are missing (Button et al., forthcoming). In Bulgaria, the distinction depends on the type of concerned secret information (state secret, trade secret, official secret, private secret) (Petrova et al., forthcoming). The other surveyed countries delineate according to the kind of offender. In Germany, economic espionage includes state-induced acts of spying conducted by foreign intelligence agencies, whereas industrial espionage is defined as spying directed towards discovering the secrets of a rival industrial company (Deutscher Bundestag 2014, p. 2). The same is true for Austria and Denmark (Konopatsch and Hilf, forthcoming; Afsah, forthcoming). In Switzerland, it is a case of economic espionage if a foreign state or a foreign company commits the offence (Konopatsch et al., forthcoming). Consequently, in Switzerland, it is a case of economic espionage if an employee of a German company spies and discloses a Swiss trade secret while, in Germany, it is a case of industrial espionage if a Swiss company spies on a German enterprise.

These distinctions define the legal basis upon which the conduct in question is prosecuted. Furthermore, the legal competences of relevant law enforcement and intelligence agencies depend on it, which is why both phenomena have to be delimited. In Germany, for example, the Offices for the Protection of the Constitution are responsible for the prevention of economic espionage but not industrial espionage. The police force is responsible for the prevention and criminal prosecution of both economic espionage and industrial espionage. This distinction is noteworthy, as the German police system is based on the principle of legality (Art. 152 Sec. 2 German CPC[1]), which is not applicable to the secret service. As soon as an offence or suspicion is reported, police and prosecution services must start an investigation, while members of the secret service, in cases of economic espionage, can simply observe and collect information. From the perspective of a company, it can be more advantageous to cooperate with the secret service (as there is no possibility of mandatory prosecution) rather than reporting incidents to the police and starting a public criminal proceeding. Such a differentiation between the roles and responsibilities of authorities is not unique to Germany, but exists throughout the EU and might complicate (international) cooperation.

Background research

Despite of the (assumed) scope of potential threats, the phenomena of industrial and economic espionage have historically been underexplored.

[1] CPC: Criminal Procedure Code.

Previous research

Some issues have been discussed in legal research (e.g., Aldoney Ramírez 2009; Föbus 2011; Metzler 1990; Nestoruk 2003; Sule 2006; Werner 2014), but relevant literature (e.g., Heickerö 2015; Hofer and Weiß 2016; Styles 2013; Tsolkas and Wimmer 2013) and current empirical findings (e.g., Röder 2011; Zwickl 2015) remain limited. Some (international) studies about economic crime or cybercrime have included questions referring to economic and industrial espionage. But usually these studies are conducted by business consultancies or trade associations, for example by KPMG, PwC, Corporate Trust, Bitkom, Ernst & Young. Two studies commissioned (2014) and conducted (2010) by the Sicherheitsforum Baden-Württemberg analysed potential threats caused by the loss of expertise and possible preventive measures (Kahle and Merkel 2004; Sicherheitsforum Baden-Württemberg 2010). Kasper (2014) conducted a secondary analysis and evaluated German 27 studies (primarily published by the aforementioned consultancies and associations). His analysis focused on the perception of threats, concerned German companies, offenders, damages, and security measures implemented by companies (Kasper 2014). The WISKOS project conducted a bibliometric analysis as well as a qualitative literature review of articles and findings published between 2000 and 2015 (Wallwaey and Waldheim, forthcoming). The latter included 58 European publications (written in English or German) that were focused on prevention measures, particularly technical measure for computer security as well as on status reports (from law enforcement agencies) and overviews about the phenomenon, including information (seldom empirically based) on offenders and affected companies (Wallwaey and Waldheim, forthcoming).

Research project WISKOS

As there has only been a relatively small current empirical knowledge on economic and industrial espionage, the WISKOS project aimed to provide empirical information through the extensive collection and analysis of qualitative and quantitative data, to systematically analyse the threat, prevention, and law enforcement of economic and industrial espionage in Germany and Europe. WISKOS was funded by the German Ministry of Education and Research from 2015 to 2018 and conducted by a research partnership between the Max Planck Institute for Foreign and International Criminal Law and the Fraunhofer Institute for Systems and Innovation Research. The following associate partners supported the project: the Federal Criminal Police Office, the regional Criminal Police Office of Baden-Wuerttemberg, and the Saxon University of Applied Police Science.

Data collection occurred in three modules:

1. The first module provided a systematic analysis of the relevant laws in all member states of the EU and Switzerland.

2. The second module consisted of a multi-level evaluation. Austria, Bulgaria, Denmark, Switzerland, and the UK were selected to be contrasted with Germany. The countries were selected for the following reasons: Austria due to its similar legal system that treats matters of industrial espionage differently, Bulgaria as an eastern European country with numerous small and medium-sized enterprises (SMEs), Denmark due to its exemplary cooperation between authorities and companies, Switzerland as a non-EU country, and the UK due to its common law system. The evaluation referred to quantitatively analysed case files ($n = 713$) in Germany, exemplary case studies ($n = 50$) in the selected countries, and qualitatively analysed interviews ($n = 62$) with experts from government authorities, SMEs, and scientific organisations.
3. Due to the extent of unreported cases, the third module focused on an extended survey of unreported crimes. In 2017, SMEs with less than 250 employees ($n = 583$), mainly coming from the industry sectors "production" and "service companies", were surveyed about aspects of the threat level, presumed perpetrators, and countermeasures to prevent physical crime and cybercrime. (The results of the study are published by Bollhöfer and Jäger 2018).

Methodology

Including the study's finding, the aim of this article is to highlight possible deterrence measures to counter economic and industrial espionage.

Theoretical considerations

Based on the *rational choice theory* and the concept of the *homo oeconomicus*, instrumental measures focus on the risk of deterrence and the threat of punishment for illegal actions (Feuerbach 1801). Rational choice theory is, *inter alia*, based on the assumption that potential offenders balance advantages and disadvantages before deciding how to act. Referring to this idea, people comply with the law and are deterred from violating rules, if the costs of criminal offences are higher than the advantages (Becker 1968, p. 207). In the line of rational choice, the situational crime prevention theory proposes measures that reduce the opportunity for crime and increase the risk of detection (Clarke 1980, pp. 140, 141). For the development of suitable preventive strategies, the section about phenomenological aspects includes information about offenders, their motives, and modi operandi as well as the way trade secrets are accessed and information on how attacks are detected. In addition to the detection risk, the risk and cost of punishment should motivate potential offenders to comply with the law (Roxin 1997, p. 50). On the basis of the collected data, it is discussed whether the outcomes of criminal proceedings are appropriate to deter offenders and which factors hamper criminal proceedings.

Data collection

The analysed data come from the second module of the WISKOS project. In Germany, 713 files of offences against Arts. 17–19 German AAUC[2] (industrial espionage) were analysed. Cases concerning economic espionage could not be included, as they are classified. The analysed cases occurred in a time period from 2008 to 2016 and covered all German federal states except Bremen and Saarland (files were not assessable in these two states). The exemplary case studies conducted in Austria, Bulgaria, Denmark, Switzerland, and the UK were selected by national experts. Selection criteria were cases with extraordinary difficulties in prosecution, evidence gathering, or international cooperation. In Austria, Bulgaria, and Switzerland, access to case files was available, so long as no foreign secret service was involved; the Danish and British experts had to refer to publicly available cases, published by newspapers or in official reports. These exemplary cases also include offences committed by foreign secret services. While in Germany 713 cases were analysed, the exemplary case studies include, all in all, only 50 cases. Although results from qualitative research based on such a small number are not representative enough to allow for any generalization or statistical extrapolation, they are nevertheless able to provide an insight into the phenomenon and the associated criminal proceedings.

Data analysis

The collected data were analysed by frequency to obtain information about the threat of industrial espionage and to evaluate suitable preventive strategies. Frequency analyses are part of content analyses: a technique to analyse a document through structuring it and systematically analysing the text on the basis of categories (Gläser and Laudel 2009, p. 197; Häder 2015, p. 333). Categories included: offenders, their motives, their modi operandi, the relationship between offenders and companies, cooperation between law enforcement agencies on national and international level, and criminal proceedings. In addition to standardized questions, each category also contained a description field for additional (unanticipated) information to be recorded.

Extent of economic and industrial espionage

Ascertaining the scope of industrial and economic espionage is challenging in Europe, as researchers are faced with a lack of statistical data. Offences of industrial espionage are usually only recorded if they are reported to the police. Concerning the German file analysis, 92.9% of all investigations were initiated after an offence was reported. Reasons for not reporting offences or suspicions are manifold. Some companies prefer to take measures on their own,

[2] AAUC: Act against Unfair Competition.

Table 1 Reported offences to the police in Germany and Switzerland (Bundesamt für Statistik, Bundesministerium des Inneren)

Year	2011	2012	2013	2014	2015	2016	2017
Germany, Art. 17 AAUC (industrial espionage)	500	525	425	397	396	397	322
Switzerland, Art. 162 CC (industrial espionage)	34	27	35	32	39	36	26
Switzerland, Art. 273 CC (economic espionage)	2	2	4	1	10	1	1

CC = Criminal Code

for example disciplinary action or consequences under labour law; other companies seek external advice and solutions. Unreported crimes pose a particular problem in this regard. Crimes can remain unreported for several reasons, for example, when victims refrain from reporting offences or when the offence goes unnoticed. Moreover, due to fragmented legal regulations, offences may not be similarly recorded: it is, for example, possible to classify industrial espionage as cybercrime in official statistics if an attack via electronic systems is involved. In many countries, including the selected countries, the recorded numbers of offences of economic espionage are not made public because they are considered as crimes against the state and must, therefore, be classified.

Given these caveats, the number of reported offences published in German and Swiss police crime statistics are not high compared to other criminal offences and appear, over time, to be quite stable (see Table 1). In Austria, no data concerning industrial espionage is listed in statistics, as industrial espionage is a case of private prosecution without police investigations. In Bulgaria, no data from police statistics is available. In the UK, neither economic nor industrial espionage are codified offences. Therefore, there are no statistics available (Button et al, forthcoming).

In addition to statistical data, studies can also be used to determine the extent of the phenomena. As mentioned previously, such studies are mostly published by professional service companies (e.g., KPMG, Ernst and Young, PricewaterhouseCoopers) or trade associations. They are usually about economic crime and partly include questions on threats to companies due to data theft and disclosure of trade secrets. In 2017, Ernst and Young published a survey saying that 44% of the surveyed companies ($n = 450$) had evidence of cyberattacks or theft of data in the last 3 years (Ernst and Young 2017, p. 13). Referring to the survey of unreported crimes conducted in the WISKOS project, 50% of the SMEs with 50 or more employees and 38% of SMEs with less than 50 employees reported being affected or assumed being affected (Bollhöfer and Jäger 2018, p. 32). When only taking German SMEs of the industry sectors "production" and "service companies" into account (around 23,5000 enterprises) (Bollhöfer and Jäger 2018, p. 32), the number of affected companies is assumed to be between 9000 and 11,500. Considering that in surveys up to 50% of the companies reported being affected, the number of reported crimes published in police statistics do not appear to reflect the real extent of crimes.

Table 2 Sex and age of suspects

Sex	
Male	78.8%
Female	19.7%
n.a.	1.5%
Age (years)	
< 30	73.4%
> 30	8.3%
n.a.	18.3%

N = 1085 suspects

Table 3 Duration of the employment of internal offenders

Duration of employment (months)	
< 12	19.1%
12–60	36.5%
> 60	44.4%

N = 178 internal offenders

Phenomenological aspects of economic and industrial espionage

The classification of the threat of crime and the development of countermeasures and enforcement strategies requires empirically-based knowledge of the phenomenon at hand: Who are the offenders and how do they operate? What kind of trade secrets and companies are concerned? How are attacks detected?

Offenders

According to the research findings of Sutherland and numerous other scholars, the "typical" white-collar criminal is a well-educated middle-aged man, who is settled down in business (e.g., Sutherland 1949, pp. 234; Piquero and Benson 2004, pp. 154). At least traditionally, offenders in the analysed German cases (see Table 2) and exemplary case studies were male, aged 30 years or older, and had business experience. As visible in Table 3, nearly half of the internal offenders in Germany (whose information is available) were employed longer than 5 years by the aggrieved company.

In cases of industrial espionage, an important issue pertains to whether the offender is internal or external. Offenders are not always unknown strangers, but regularly internal employees, trainees, or contractors. Due to their insider knowledge, the activities of internal offenders can be particularly risky. This is also true for social engineering or other methods of manipulation used to induce the disclosure of trade secrets or other information that is not publicly available (Röder 2011, p. 27). In recent last years, open source intelligence (OSINT) has become popular, as professionals commonly publish their occupational activities

online (Röder 2011, p. 22). This is one way that potential (external) offenders can check on who may have the information they need, before they contact the internal. Referring to the German file analysis, 43% of the offenders were internal, 31% external, and 23% were considered as both internal and external.[3] The latter group included people who, for example, backed-up data as internal offenders and used or disclose the data after leaving the company.

Motives

The offender's motives were diverse, though examples from the case files included the dissatisfaction with their current (or previous) employer and the prospect of financial gain (for themselves or for another company). Siphoning information and expertise is also a method commonly used by states to support their economies or by other companies to enable them to underbid their competitors (e.g., eavesdropping at Siemens by Alstom (Sule 2006, p. 42).

Modi operandi

Despite the digital environment in which much espionage activity takes place, physical crimes, as well as cybercrimes, occurred in the analysed cases. Cyberattacks bring about special risks and are often difficult to detect. Cybercriminals can often repeatedly access secret data over several months before an attack is detected and are particularly focused on the exploitation of software vulnerabilities and integrated networks (Bollhöfer and Jäger 2018, p. 21).

In the analysed cases, (internal) offenders had been known to send trade secrets in emails, to copy them to USB sticks, or to photocopy or photograph (physical) documents.[4] SMEs, surveyed in the third module of the WISKOS project, discovered that a quarter of the attacks occurred in connection with the use of private devices, like smartphones or tablets (Bollhöfer and Jäger 2018, pp. 40, 41).[5] In this context, emails with critical content files play an important role, as 66% of the SMEs reported that such emails were connected to an incident (Bollhöfer and Jäger 2018, pp. 40, 41).[6]

Affected trade secrets and companies

Referring to the German case file analysis and exemplary case studies, the affected trade secrets included customer data, internal data, contracts, business strategies, and technical knowhow. The most affected companies belonged to the service

[3] The numbers are based on cases that resulted in a court judgement, penal order, or provisional dispensing with court action (Art. 153a German CPC).

[4] The information is based on cases that resulted in a court judgement, penal order, or provisional dispensing with court action (Art. 153a German CPC).

[5] Multiple responses possible.

[6] Multiple responses possible.

Table 4 Outflow of trade secrets in German cases

Transmission of electronic data (via email or cloud)	21.3%
Storage and removal of digital data	32.5%
Removal of physical documents	13.3%
Removal of copied or photographed data and information	14.3%
Siphoning of data	1.0%
Miscellaneous	4.4%
n.a.	13.3%

$N = 203$, multiple responses possible. Data based on cases that resulted in a court judgement, order, or provisional dispensing with court action (Art. 153a CPC)

industry, followed by insurance and real estate companies, engineering companies, logistics companies, and export/trading companies. The concerns of the service industry were expected, as it is a knowledge-intensive sector that places high value on customer data.

Interestingly, this outcome differs from that of the survey (module 3), where next to the service and trading sector, the construction industry was one of most concerned sectors (Bollhöfer and Jäger 2018, p. 34). The divergent results could be put down to the unwillingness of the construction sector to report incidents (only 2% of criminal charges of the German cases were filed on behalf of the construction industry).

Outflow of trade secrets

Considering the damaging consequences of economic and industrial espionage, to develop effective countermeasures it is necessary to know more about how protected trade secrets flow out of companies and how such breaches are discovered. Based on the findings of German case file analysis, Table 4 provides an overview of how documents and trade secrets were accessed and removed.

In the survey (module 3 of the WISKOS project), the SMEs were asked about observed illegal activities. The most frequent response was the opening of critical emails (66%).[7] Further activities were: use of private devices (24%), visitors (21%), announcement of recently developed products (10%), trips abroad (7%), trade fair attendance (6%), university cooperation (5%), and participation in a trade delegation (3%) (Bollhöfer and Jäger 2018, p. 41).

Detection of attacks

As seen in Table 5, in most cases the offence was discovered via information provided by an employee or external contact (e.g., customer, client, external collaborator). Cyberattacks were found to pose a particular challenge as they are quick and stealthy. In addition to attentive employees, routine inspections of data and computer

[7] Multiple responses possible.

Table 5 Detection of attacks in German cases (5 most frequently responses)

Information provided by an external contact associated with the business	23.1%
Information provided by an employee	13.7%
Information provided by an external contact not associated with the business	5.7%
Monitoring inconsistencies in the behaviour of employees	5.7%
Routine inspections of data and computer logs	5.3%
Miscellaneous	24.9%
n.a.	8%

$N = 225$, multiple responses possible. The data are based on cases that resulted in a court judgement, order, or provisional dispensing with court action (Art. 153a CPC)

logs are useful methods to detect cyberattacks. Further actions might include monitoring inconsistencies in data or the (unusual) behaviour of people. It is rare for companies or law enforcement authorities to receive external tip-offs on cyberattacks. In one case, Danish authorities received information about an affected company from US authorities.

Offences can also be detected accidentally. For example, in one of the case study files, an offender forgot to remove illegally copied documents from the photocopier. Something similar happened in the well-known McLaren/Ferrari case, when the McLaren Formula One team received confidential technical information from the Ferrari team. It was assumed that the information was provided to Mike Coughlan (McLaren team) by Nigel Stepney, who was dissatisfied with his job at Ferrari. Ferrari was unaware that their technical information had been stolen until they received a tip off from an employee in a photocopying shop where Coughlan's wife copied the protected information. The employee randomly read some of the copied pages and decided to inform Ferrari (Goren and Noble 2007).

Prevention

Given the information outlined above, the development of internal preventive measures and security strategies has become increasingly important. Companies need to be increasingly aware of the threat posed by economic and industrial espionage and the necessity to adopt preventive measures.

Whereas large companies have generally reacted accordingly and installed internal control systems and prevention measures, SMEs, which regularly focus only on their day-to-day business, have been found to have treated security matters with secondary rather than primary importance (Sonnen and Bollhöfer, forthcoming). Volkswagen, for example, stated in 2016 that the company was faced with more than 6000 cyberattacks per day (Manager Magazine 2016). Compared with SMEs, large companies, like Volkswagen, have security departments, (cyber-)security strategies, and routine controls of computer activities (Thieme 2008). If an incident occurs, large companies usually react immediately to close the information leak. On the other hand, 18% of enterprises with less than 50 employees (surveyed in

the WISKOS project) had no strategy for dealing with physical or cyber espionage. SMEs with more than 50 employees reported having strategies to protect against physical espionage (91%) and cybercrime (94%) (Bollhöfer and Jäger 2018, p. 44). Contractors and companies in the field of product innovation had a much higher level of awareness about the dangers of espionage (and countermeasures) than other businesses (Bollhöfer and Jäger 2018, p. 20).

Following situational crime prevention theory, companies should actively reduce opportunities for crimes and increase their detection efforts (Clarke 1980, pp. 140, 141). With regard to the abovementioned phenomenological results, suitable strategies that could be easily adopted include:

- Better control of access to the physical workplace,
- Restricted access to (electronic) data,
- Regular updates to security regulations and security measures,
- Regular staff training courses and awareness-raising actions,
- Stronger confidentiality obligations,
- Monitoring of espionage indicators, e.g., social engineering, extensive data transfers, presence of employees outside working hours, applications from students and trainees from relevant countries (e.g., China or Russia) (Bollhöfer and Jäger 2018, p. 46).

In addition to internal control and prevention measures, aggrieved parties can take legal action. This can include compensation claims, disciplinary actions (under labour law), or the reporting an offence to police to initiate a criminal investigation.

Criminal proceedings and legal challenges

Deterrence strategies focus not only on the risk of being detected but also on the risk of (serious) punishment. Evaluating the severity of punishments requires an assessment of the following aspects: the legally-regulated threat of punishment, the outcomes of criminal proceedings, and the question, whether these outcomes are appropriate to deter offenders. Based on results from the analysed cases, numerous procedural obstacles hamper efficient law enforcement and criminal proceedings.

Legal protection of trade secrets

Given the lack of a homogeneous definition for economic and industrial espionage, the regulation of the phenomenon within the EU and its member states is characterised by fragmented official responsibilities and legislation. Based on its competency to establish and ensure the functioning of the internal market (Art. 114, Art. 294 TFEU[8]), the European Commission proposed (and the European Parliament approved) the *Directive (EU) 2016/943 on the protection of undisclosed know-how*

[8] TFEU: Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01) of 26 October 2012.

and business information (trade secrets) against their unlawful acquisition, use and disclosure[9], which should allow for greater harmonised protection within the EU and its single market. Since the protection of trade secrets does not fall within the area of serious or organised crime listed in Art. 83 TFEU, the European Parliament has no power to harmonise and establish minimum rules concerning criminal offences and sentencing. Therefore, the criminal law protection of trade secrets is still fragmented within the EU. Consequently, most European countries have no single offence of industrial or economic espionage but refer to several legal regulations and protected rights.

Criminal complaint and private prosecution

Economic espionage is an ex-officio crime in all European member states and Switzerland. As soon as authorities are made aware of a case of economic espionage, an investigation must begin. Industrial espionage, in turn, is an ex-officio offence in Bulgaria; in other European states, for example, Austria, Germany, and Switzerland, the aggrieved party has to file a criminal complaint ("Antragsdelikt") before an investigation can begin. In Germany, a complaint by the affected company is not required if the public prosecutor assumes a particular public interest in prosecution (No 260a Sec. 1 RiStBV[10]).

In Austria (Art. 71 Austrian CPC), Germany (Art. 374 seq. German CPC), and Switzerland (Art. 118 seq. Swiss CPC), aggrieved parties can initiate private prosecutions in cases of industrial espionage. This is the case in Germany and Switzerland if the public prosecutor decides not to prosecute. In Austria, certain offences (e.g., industrial espionage pursuant to Art. 123 Austrian CC or Art. 11 Austrian AAUC) have to be prosecuted privately (Art. 71 Austrian CPC). In cases of private prosecution, the aggrieved company appears in court as the prosecutor. Even though the public prosecutor is not involved, the German prosecution service can take over the prosecution at any point in the criminal proceedings (Art. 377 Sec. 2 German CPC). In Austria, the aggrieved party is completely responsible for cases of private prosecution including permitted investigative measures (Art. 71 Austrian CPC). Generally, companies refrain from private prosecutions, as they are both risky and costly.

Threat of punishment

As mentioned, the regulation of criminal offences and sanctions concerning trade secrets remains the responsibility of national legislatures. Consequently, the threat and severity of punishment differ from country to country. Denmark, for example, provides a comprehensive legal framework for the protection of trade secrets and

[9] Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, L 157/1.

[10] RiStBV: Richtlinien für Straf- und Bußgeldverfahren (Guidelines for Criminal and Fine Proceedings).

Table 6 Outcome of investigation procedures in Germany

Outcome	Freq.	Perc.
Prosecution refused to start an investigation (Art. 152 Sec. 2 CPC)	79	7.1
Non-prosecution of a petty offences (Art. 153 CPC)	118	10.6
Dismissal of criminal proceedings (Art. 170 Sec. 2 CPC or Art. 376 CPC)	640	57.6
Provisional dispensing with court action (Art. 153a CPC)[a]	98	8.8
Penal order[b]	80	7.2
Public charge	39	3.1
Other outcomes[c]	57	5.13

$n = 1111$ decisions

[a]Art. 153a, Sec 1, S. 1 German CPC: In a case involving a misdemeanour, the public prosecution office may, with the consent of the accused and of the court competent to order the opening of the main proceedings, dispense with preferment of public charges and concurrently impose conditions and instructions upon the accused if these are of such a nature as to eliminate the public interest in criminal prosecution and if the degree of guilt does not present an obstacle

[b]Art. 407, Sec 1 CPC: In proceedings before the criminal court judge and in proceedings within the jurisdiction of a court with lay judges, the legal consequences of the offence may, in the case of misdemeanours, be imposed, upon written application by the public prosecution office, in a written penal order without a main hearing. The public prosecution office shall file such application if it does not consider a main hearing to be necessary given the outcome of the investigations. The application shall refer to specific legal consequences. The application shall constitute preferment of the public charges

[c]Other outcomes occur, for instance, if an offender violates several laws or the offence is not commensurate with the expected penalty

is, in cases of cybercrime, more focused on information sharing and cooperation than on sentencing (Afsah, forthcoming). The maximum penalties applicable for industrial espionage range (in the surveyed countries) from 18 months in Denmark (Art. 37 Sec. 4, Art. 23 Danish Marketing Practices Act) to 5 years imprisonment in Bulgaria (Art. 224 Sec. 1 Bulgarian CC). Even in cases of economic espionage, in Bulgaria the sentences are significantly more severe than in other European countries. While the applicable penalties range from 10 years to life-long imprisonment in Bulgaria (Art. 104 Sec. 1 Bulgarian CC), in Austria and Switzerland, the threat of punishment ranges from a fine up to 3 years imprisonment (Art. 256 Austrian CC, Art. 273 Swiss CC).

Outcome of criminal proceedings

Referring to the concept of general deterrence, potential offenders should refrain from committing crimes due to the threat of being punished. This punishment must also be enforceable (Roxin 1997, pp. 48). This raises the question whether the outcomes of criminal proceeding are currently suitable to deter potential offenders.

In the analysed six countries, criminal proceedings in cases of industrial espionage were regularly closed or suspended by the public prosecution before the conclusion of a trial. Table 6 sheds light on the suspensions, criminal orders, and public charges of the German cases. Although the file analysis included 713 cases, it

Table 7 Outcomes: selection of non-appealable rulings in Germany

	Freq.	Perc. of all offenders
Provisional dispensing with court action, fine (Art. 153a CPC)	124	11.2%
Warning (Art. 59 Criminal Code)	3	0.3%
Fine	55	5.0%
Suspended prison sentence	5	0.5%
Acquittal	9	0.8%
Other	13	1.2%

$n = 1111$

covered 1085 accused persons with 1111 decisions, as in some cases, more than one suspect was involved and more than one law was violated: this resulted in numerous decisions.

As can be seen, cases of industrial espionage were regularly closed or suspended by the public prosecution before the conclusion of a trial. How can this be explained?

A refusal to prosecute (Art. 152 Sec. 2 German CPC) can only be made in exceptional circumstances. Therefore, the number of cases ($n = 79$, 7.1%) is quite remarkable. One explanation might be the reporting of irrelevant actions in cases of labour law, such as if one party tries to boost its claims by bringing a criminal charge against another party. At 57.6%, dismissal of criminal proceedings is the primary reason for a trial not being concluded. Reasons for dismissal may include innocence of the suspect, but also difficulty in proving that an offence was committed and difficulty in identifying the offender(s); the public prosecutor may also drop the case and refer the aggrieved party to private prosecution. Another reason for the closure of an investigation pursuant to Art. 170 Sec. 2 German CPC is the withdrawal of the criminal complaint by the victim. Often, the parties involved have reached an agreement under civil or labour law and agreed to terminate criminal proceedings. After the withdrawal of the criminal complaint, the prosecution service dismisses the proceedings due to the lack of a public interest in prosecution.

Cases involving a misdemeanour can be provisionally dispensed in Germany when the court and the public prosecution are in agreement (Art. 153a German CPC). This option is frequently chosen to avoid a lengthy trial (and the associated comprehensive gathering of evidence). In only 119 cases (10.3%), did investigations concluded with a penal order or public charge.

Regarding the outcomes of non-appealable rulings in Table 7,[11] the proceeding is regularly dealt with in a summary manner when an offender agrees to pay a fine

[11] Referring to German criminal procedure law, a refusal to prosecute or a decision to dismiss criminal proceedings cannot be appealed. That said, so long as the statute of limitations does not preclude it, an investigation can be restarted at a later date. Therefore, Table 3 only includes a selection of decisions.

in cases of provisional dispensing (Art. 153a CPC). This often occurs in cases that are considered minor offences. Compared to fines and prison sentences, provisional dispensing is not registered in the German Central Criminal Register and—more importantly for offenders—not listed in a police clearance certificate. In total, 55 offenders (5.5% of all cases) received a fine and in only five cases did the court decide to impose a custodial sentence with probation.

Despite some legal differences, these outcomes are, in general, transferrable to Austria and Switzerland. Conversely, in Bulgaria, far more severe penalties are applied. In the Danish case studies that included cases of economic espionage, prison sentences without probation were imposed. Due to the low number of analysed cases in the surveyed countries and the requirement to select interesting and comprehensive cases, the outcomes cannot be compared.

Obstacles to law enforcement and criminal proceedings

Considering the high number of dismissals of criminal proceedings and the low number of fines and (suspended) prison sentences, the question is raised, which obstacles hamper criminal law enforcement and criminal proceedings.

Legal obstacles

As seen above, a noteworthy number of German cases existed in which the public prosecutor declined to prosecute or dismissed a prosecution. In addition to the reasons described above (e.g., withdrawal of criminal complaint, reference to private prosecution), one difficulty in maintaining a prosecution was that even if the aggrieved party classified the stolen information as a very important trade secret, the stolen information did not fulfil the necessary legal definitions and requirements to be treated as such by criminal law (e.g., the requirements of Directive (EU) 2016/943). Additionally, a trade secret can be, under certain circumstances, legally disclosed.

Cross-border cooperation in criminal proceedings

Cross-border investigations that require cooperation with foreign law enforcement authorities or companies could have taken longer than expected or were unsuccessful due to time-consuming requirements and missing legal leverage. For example, police requests for legal assistance to get information about an email account in another country can take months (though one respondent in the WISKOS interviews noted that the time such requests take can depend on the long-time relationship of the parties involved) and may result in the sought-after data being removed or destroyed due to data protection regulations. In an effort to reduce such procedural inefficiencies, in Germany a cost–benefit analysis can be discussed in international cases, resulting in a provisional dispensing with court action (Art. 153a German CPC).

Cross-border investigations are further hampered when cooperation agreements between countries do not exist. Additionally, missing bilateral agreements aggravate the sentencing of offenders abroad. This was seen in the AMSC case, where the Chinese accomplices could not be sentenced in the US or Austria, as there was no extradition treaty or legal foundation to start a trial in absentia.

On occasion, German authorities have demanded the provision of security deposits (bonds) in cases of industrial espionage: if an offender returns to his/her country and cannot be prosecuted in a German court, the case is dispended and the security deposit used to pay a sum of money pursuant to Art. 153a Sec. 1 German CPC.

Evidential difficulties

The identification of offenders is often a complex issue, as is the ability to gain enough evidence that an offence has occurred. For example, in a German case, an employee was suspected of illegally transferring secret information abroad via a mobile phone, however, a digital-forensic examination of the mobile phone did not indicate that any such transfer had occurred. Without evidence the case must be dismissed, although there were several suspicious facts. Prove the involvement of foreign intelligence services—whose espionage skills are often outstandingly—is also exceedingly difficult (in all surveyed countries). Consequently, such cases are treated as industrial espionage and regularly dismissed or referred to private prosecution, but are not prosecuted ex-officio as economic espionage (and liable to more serious punishment).

Obstacles in the area of cybercrime

The same is true in the field of cybercrime. In addition to difficulties associated with their detection, the findings show that it is often a significant problem for investigators to secure electronic evidence, especially when the rules of legal procedure require that evidence be handled in a certain way to ensure a (necessary) fair trial or if the gathering is dependent on international judicial assistance. Additionally, electronic evidence can be disrupted or manipulated, making it difficult to identify (Momsen and Hercher 2013, pp. 178). In 2018, the European Commission (COM (2018) 225 final) proposed a (highly disputed) Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. The Directive seeks to facilitate the timely and effective securing of electronic evidence among EU member states.

Conclusion

In conclusion, the title of this article asks whether spies can operate without (legal) borders? Are they truly able to obtain access to secret information without being detected and able to transfer this information without being interrupted? Are they immune to the threat of punishment? While properly responding to industrial and economic espionage is difficult, what is certain is that opportunity cost of

committing offences, as well as the risk of being detected and punished, must be increased.

Based on the WISKOS findings, up to 18% of SMEs have no strategy against physical espionage or cybercrime. Moreover, of the measures that do exist, they are often insufficient. Though firewalls, virus scanners, and spam filters are used by nearly all SMEs, several other measures, such as external staff checks, the separation of internal and external IT networks, and legal provisions concerning personal devices and social media networks are too often missed (Bollhöfer and Jäger 2018, p. 45, 46). Strategies to prevent industrial and economic espionage should integrate the phenomenological findings on offenders (externals and internals), known modi operandi, affected trade secrets (customer data, internal data, contractual contents, business strategies, technical knowhow), the outflow of trade secrets and possibilities to detect attacks. Internal awareness programs must focus on how to prevent and better detect attacks.

Considering the high number of unreported crimes as well as the high number of dismissals of criminal proceedings, the low number of fines and (suspended) imprisonment, and the numerous obstacles that hamper criminal proceedings, it has to be asked whether the criminal law is too blunt an instrument to tackle the phenomenon or if the threat posed by economic and industrial espionage is perhaps exaggerated. The latter could be supported by the surprisingly high number of refused investigation processes and dismissals. While some crime reports may be legitimately refused further investigation due to their bogus nature or incorrect legal classification of trade secrets, dismissals pursuant to Art. 170 Sec. 2 German CPC also include cases in which the criminal complaint is withdrawn by the victim and in which the aggrieved party is referred to private prosecution (which is also a problem in Austria and Switzerland). Regarding the fact that only 10.3% of the investigated procedures result in a penal order or public charge, and in another 8.8% a provisional dispensing pursuant to Art. 153a German CPC, the criminal law does not seem appropriate to deter potential offenders, as the possibility of being fined or receiving a (suspended) prison sentence is less than 5% in Germany and similar in the surveyed countries. In addition, given the difficulties associated with identify offenders who commit cyber-attacks, those acting from another country without judicial extradition agreements do not, in all likelihood, have to worry about the threat of criminal proceedings.

Based on the results yielded by the case studies, it would be an appropriate move to abolish private legal actions (in Austria, Germany, Switzerland) in order to strengthen the state's approach to industrial espionage (a measure that could also lead to more reported crimes). Spying on trade secrets is not a minor offence as it can seriously impact the affected company. The various espionage activities of offenders (be they internal, external, or state-sponsored) lead to the creation of a differentiation between economic and industrial espionage in all surveyed countries. This differentiation is generally irrelevant, if not incomprehensible, as the same actions have different legal consequences only due to the fact that the offender is a foreign secret service, a foreign company (only in Switzerland), or a competitor. Referring to the legal obstacles that often hamper prosecution, possible improvements could include better cross-border cooperation, faster international judicial assistance, and improved measures for the correct gathering of electronic evidence

(although some facts—such as affiliation with a foreign secret service—will invariably remain difficult to prove).

References

Afsah, E. forthcoming. Country report: Denmark. In: S. Carl and M. Kilchling, (eds.) Economic and industrial espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin: Duncker & Humblot.

Aldoney Ramírez, R. 2009. *Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen*. Kenzingen: Centaurus-Verlag.

Becker, G.S. 1968. Crime and punishment: An economic approach. *Journal of Political Economy* 78: 169–217.

Bollhöfer, E., and A. Jäger. 2018. *Wirtschaftsspionage und Konkurrenzausspähung—Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung*. Freiburg: Arbeitsberichte Band A 8, Max-Planck-Institut für ausländisches und internationales Strafrecht.

Budras, C. 2014. Der Feind sitzt im Büro nebenan. Frankfurter Allgemeine Zeitung, 23 May, https://www.faz.net/aktuell/wirtschaft/wirtschaftsspionage-frustrierte-mitarbeiter-sind-ein-risiko-12944343.html. Accessed 24 July 2019.

Bundesamt für Statistik. 2012–2018. Polizeiliche Kriminalstatistik 2011–2017, www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht.html. Accessed 24 July 2019.

Bundesministerium des Inneren. 2012–2018. Polizeiliche Kriminalstatistik 2011–2017, www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html. Accessed 24 July 2019.

Button, M., A. Wakefield, and K. Larkins. forthcoming. Country report: United Kingdom. In: S. Carl and M. Kilchling, (eds.) Economic and industrial espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin: Duncker & Humblot.

Clarke, R.V.G. 1980. "Situational" crime prevention: Theory and practice. *British Journal of Criminology* 136: 136–147.

Deutscher Bundestag. 2014. Drucksache 18/2281, Geheimdienstliche Angriffe und Spionage bei deutschen Unternehmen, 5 August, http://dipbt.bundestag.de/dip21/btd/18/022/1802281.pdf. Accessed 24 July 2019.

Gläser, J., and G. Laudel. 2009. *Experteninterviews und qualitative Inhaltsanalyse*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Emmott, R., F. Y. Chee, and J. Plucinska. 2019. Exclusive: EU considers proposals to exclude Chinese firms from 5G networks, 30 January, https://uk.reuters.com/article/uk-usa-china-huawei-tech-europe/eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUKKCN1PO2MJ. Accessed 24 July 2019.

Ernst and Young. 2017. Datenklau: Virtuelle Gefahr, echte Schäden, www.ey.com/Publication/vwLUAssets/ey-datenklau-virtuelle-gefahr-echte-schaeden-2/$FILE/ey-datenklau-virtuelle-gefahr-echte-schaeden-2.pdf. Accessed 15 Mar 2019.

Feuerbach, P. J. A. von. 1801. Lehrbuch des gemeinen in Deutschland geltenden Peinlichen Rechts, www.deutschestextarchiv.de/feuerbach_recht_1801. Accessed 24 July 2019.

Föbus, N. 2011. *Die Insuffizienz des strafrechtlichen Schutzes von Geschäfts- und Betriebsgeheimnissen nach § 17 UWG*. Frankfurt et al.: Lang.

Goren, B., and J. Noble. 2007. Spy case court hearing adjourned. autosport 10 July, www.autosport.com/f1/news/60690/spy-case-court-hearing-adjourned. Accessed 24 July 2019.

Kahle, E., and W. Merkel. 2004. Fall- und Schadensanalyse bezüglich Know-how-/Informationsverlusten in Baden-Württemberg ab 1995, www.connect-community.de/Events/rheinland2008/vortraege/Studie-Uni-Lueneburg.pdf. Accessed 24 July 2019.

Häder, M. 2015. *Empirische Sozialforschung - eine Einführung*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Heickerö, R. 2015. Industrial espionage and theft of information. In: N. Abouzakhar (ed.) Proceedings of the 14th European conference von cyber warfare and security 2015; 2–3 July, Hatfield, UK. Sonning Common: Academic Conferences and Publishing International Limited, pp. 85–94.

Hofer, A., and M. Weiß. 2016. *Wirtschafts- und Industriespionage—Informationsgewinnung, Management, Kompetenz*. Wiesbaden: Springer.

Kasper, K. 2015. Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes, Ergebnisbericht einer Sekundäranalyse, www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Wirtschaftsschutzallgemein/SpioForschung_lang.pdf?__blob=publicationFile&v=3. Accessed 24 July 2019.

Konopatsch, C., M. Rentsch, P. Stocker, and M. Hilf. forthcoming. Country report: Switzerland. In: S. Carl and M. Kilchling (eds.) Economic and industrial espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin: Duncker & Humblot.

Konopatsch, C., and M. Hilf. forthcoming. Country report: Austria. In: S. Carl and M. Kilchling (eds.) Economic and industrial espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin: Duncker & Humblot.

Manager Magazin. 2016. Volkswagen muss täglich 6000 Cyber-Attacken abwehren. 06 September, www.manager-magazin.de/digitales/it/volkswagen-muss-taeglich-6000-cyber-attacken-abwehren-a-1111054.html#ref=rss. Accessed 24 July 2019.

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

Momsen, C., and N. Hercher. 2013. Digitale Beweismittel im Strafprozess – Eignung, Gewinnung, Verwertung, Revisibilität. In: Strafverteidigervereinigungen (ed.) Die Akzeptanz des Rechtsstaats in der Justiz. Berlin: Strafverteidigervereinigungen, pp. 173–196.

Nestoruk, I.B. 2003. *Strafrechtliche Aspekte des unlauteren Wettbewerbs. Strafrecht und Schutz der Wirtschaftsordnung*. Heidelberg: Müller.

Petrova, T., D. Yordanova, S. Petrov, and P. Boyadjiyski. forthcoming. Country report: Bulgaria. In: S. Carl and M. Kilchling, (eds.) Economic and industrial espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin: Duncker & Humblot.

Piquero, N.L., and M. Benson. 2004. White-collar crime and criminal careers. Specifying a trajectory of punctuated situational offending. *Journal of Contemporary Criminal Justice* 20 (2): 148–165.

Röder, N. 2011. Industriespionage—Risikofaktor Mensch. Master thesis, University of Applied Science Hanover.

Roxin, C. 1997. *Strafrecht Allgemeiner Teil*. München: Beck.

Sicherheitsforum Baden-Württemberg. 2010. SiFo-Studie 2009/2010. Know-how-Schutz in Baden-Württemberg, www.sicherheitsforum-bw.de/pb/,Lde/Startseite/Das+Sicherheitsforum+Baden_Wuerttemberg/SiFo_Studie. Accessed 24 July 2019.

Sonnen, B., and E. Bollhöfer. forthcoming. 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. In: E. Wallwaey, E. Bollhöfer and S. Knickmeier (eds.) Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin: Duncker & Humblot.

Styles, M. 2013. Constructing positive influences for user security decisions to counter corporate or state sponsored computer espionage threats. In: L. Marinos and I. Askoxylakis (eds.) Human aspects of information security, privacy, and trust. HAS 2013. Lecture Notes in Computer Science, vol. 8030. Berlin, Heidelberg: Springer.

Sule, S. 2006. *Spionage*. Baden-Baden: Nomos-Verlag.

Sutherland, E. 1949. *White collar crime*. New York: The Dryden Press.

Thieme, M. 2008. Das verschwiegene Netzwerk. Frankfurter Rundschau, 12 June, www.fr.de/wirtschaft/verschwiegene-netzwerk-11600414.html. Accessed 24 July 2019.

Thomson, I. 2015. WikiLeaks docs show NSA's 10-year economic espionage campaign against France. The Register, 29 June, www.theregister.co.uk/2015/06/29/wikileaks_docs_show_nsa_vs_france. Accessed 24 July 2019.

Tsolkas, A., and F. Wimmer. 2013. *Wirtschaftsspionage und Intelligence Gathering*. Wiesbaden: Vieweg und Teubner.

US Department of Justice. 2018a. Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets. Press release, 24 January, www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets. Accessed 24 July 2019.

US Department of Justice. 2018b. Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets. Press release, 6 July, www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets. Accessed 24 July 2019.

Wallwaey, E. and L. Waldheim. forthcoming. Der „typische“Spionagefall? Ergebnisse einer Literaturanalyse. In: E. Wallwaey, E. Bollhöfer and S. Knickmeier (eds.) Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin: Duncker & Humblot.

Werner, S. 2014. *Unternehmenskriminalität in der Bundesrepublik Deutschland*. Ostfildern: Thorbeke.

Zirm, Jakob. 2013. Spionage: „Das war versuchter Firmenmord“. Die Presse, 22 August, https://diepresse.com/home/wirtschaft/international/1444292/Spionage_Das-war-versuchter-Firmenmord. Accessed 24 July 2019.

Zwickl, J. 2015. *Industriespionage im deutschen Mittelstand*. München: Grin-Verlag.