An unacknowledged crisis – economic and industrial espionage in Europe

SABINE CARL
Dr. jur., Senior Researcher at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany; Project Co-ordinator, 'Economic and industrial espionage in Germany and Europe (WiSKoS)'

Introducing an Unacknowledged Crisis

Whilst espionage is not a new occurrence, it has received remarkably little research attention in Europe. Espionage crimes are of a mixed character and encompass two separate phenomena: 'classic' or economic espionage by intelligence agencies of a foreign state, and incidents of competitive corporate or industrial espionage, commercial spying or industrial theft. Both phenomena are characterized by essentially identical modi operandi, the aim of illegal obtainment of know-how and other information as well as the largely identical targets or victims in form of the owners of know-how and/or intellectual property such as business and trade secrets. The latter may stem either from the economy or science. In substance, the difference between economic and industrial espionage is only the different motivation – in achieving either a political or an economic advantage. Both forms of espionage are located at the intersection of conventional (physical) crime and cybercrime.

The basic understanding of these crimes, their legal framework as well as the organisational design of administrative competences and jurisdictions is still largely shaped by the Cold War period.[1] Legal modernisations have not kept pace with the changing political conditions. Former political frontlines were dissolved and in some cases re-

[1] Metzler 1990.

placed by economic cooperation. At the same time, new friend-foe patterns evolved along the fluid lines of contemporaneous political interests. While attacks on economic know-how originating from some regions are still persecuted as state crime, delinquents originating from friendly nations are termed to be 'friendly spies' and only hesitatingly prosecuted – if at all.[2] In light of the ongoing developments in the European political arena, an un-reflected classification of these phenomena as state crime (in Germany punishable under § 99 of the German Criminal Code) is increasingly less compelling. Independent of any legal considerations, it stands to reason that non-state initiated modes of illegal know-how obtainment prosecuted as industrial espionage (in Germany punishable as 'Konkurrenzausspähung' under § 17 of the German Unfair Competition Law) are of larger practical significance. In Germany, this assumption may be based on the available albeit incomplete statistical data drawn from the Polizeiliche Kriminalstatistik (police crime statistics), the Lagebild Wirtschaftskriminalität (situation picture on economic crime) as well as the scarce relevant victimization studies conducted by economic research institutes.[3]

The clean legal differentiation does not translate well into everyday practice. The different criminal provisions amount to separate jurisdictions for economic and industrial espionage. In Germany, structures developed for law enforcement agencies with varying responsibilities which are in part complementary to each other (e.g. different administrative levels within a federal state) and in part exclusive (investigative powers of the Attorney General, cf. § 124a German GVG). This competency problem is exacerbated by the fact that in many cases, not only in the area of cybercrime, the origins and aims of attacks remain undiscovered. The subsequent uncertainty as to the competent authority puts espionage cases at risk of untimely closure of investigations. This, in turn, leads to problems with statistical recording. Solved cases are rare and quite likely statistically underrepresented. Unclear cases are

[2] Schweizer 1993.

[3] KPMG 2006, KPMG 2010, PwC 2011, Corporate Trust 2012, Corporate Trust 2014, PwC 2016.

more likely to be counted without reference to economic or industrial espionage as theft, breach of trust or cybercrime.

In addition to this statistical difficulty with reported cases, the criminal area at hand is characterized by unreported cases. While cases in all areas of crime go undetected to varying degrees, even discovered cases of espionage may go unreported due to the affected companies fearing (further) reputational damage and endangerment of their business secrets. These considerations hamper the cooperation of businesses with law enforcement agencies.

It is to be questioned if the distinction between governmental (intelligence-led) and non-governmental (corporate) inducement of attacks along with the procedural differentiation depending on the affected know-how is actually relevant. From the point of view of targeted businesses, the actual or anticipated economic damages determine their reactions. These considerations amplify doubts if the distinction in the approach can still be considered expedient. The current structures might not only diminish effective domestic prosecution but also negatively impact international and cross-border cooperation including legal assistance.

Starting by clearing up the terminology, this article will examine the current state of research, describe the approach of an on-going research project and end with a succinct quantification of the current state of crisis.

1. *Defining espionage*

Considering the long history of the crime in question it may be considered surprising that a proper definition of espionage is still a necessity. This is due to the inconsistency in the terminology for the discussion of economic and industrial espionage in at least English and German. The backgrounds and motivations of the individual authors seem to determine their choice of vocabulary. Not all terms are always used in the same way or with the same meaning. In German the terminology originates from such diverse backgrounds as business administration, the technical appliance industry, the computer industry, the security

industry, law and history.[4] In English, there are terms generally used for describing industrial espionage including corporate espionage, economic intelligence or data theft and terms mostly used to describe economic espionage such as economic warfare or digital sovereignty.[5]

Economic espionage can be defined as acts of spying conducted by and for state agents targeting economic enterprises, business and research institutions (BT-Drs. 2014, S. 2, 3). Economic espionage aims to aid the economy of a foreign state, is motivated by political interests and belongs to the area of state crime and thus 'classical' criminal law.

Industrial espionage is defined in accordance with The Oxford English dictionary as 'spying directed towards discovering the secrets of a rival industrial company, manufacturer, etc.'(BT-Drs.2014, S. 2, 3). It serves economic interests and focuses on acquiring product-related know-how. Unlike illegal information procurement of secret information, the collection and evaluation of publicly accessible information through so called competitive intelligence is legal within the limits of existent data protection law.[6]

2. *Current state of research*

Academic research on economic and industrial espionage is currently lacking, both in quantity and quality. The research that does exist is fraught by the above-mentioned inconsistent terminology which makes it difficult to compare empirical studies and country-specific data.

Generally speaking the scarce scientific literature is by and large limited to the discussion of questions that were relevant at the time of the conceptualization and implementation of the corresponding regu-

[4] „Betriebsspionage", „Geheimnisschutz", „illegaler Wissensabfluss", „Industriespionage", „Know-How-Schutz", „Sabotageschutz", „ungewollter Informationsabfluss", „Werksspionage", „wirtschaftliche Kriegsführung", „Wettbewerbsspionage", „Wissensdiebstahl", „Wissensabschöpfung" as well as „staatsverstärkte Kriminalität".

[5] Naucke 1996.

[6] Röder 2011; Scherf 2013.

lation.[7] In addition to literature on economic crime and its penal regulation, titles on competition law are also relevant.[8] As the modi operandi and thus the phenomenology of economic and industrial espionage change, the normative need for reform becomes evident. In the recent literature the conclusion prevails that the current legal situation is no longer appropriate.[9]

3. *The WiSKoS-Project*

To close this research gap is the purpose of a current research project of the Max Planck Institute for foreign and international criminal law (MPICC) in Freiburg, Germany, called "Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS)" or in English "WiSKoS – Economic and industrial espionage in Europe". The project is part of a research program launched by the German Federal Ministry of Education and Research on civil security.[10]

WiSKoS is a joint project in which the MPICC cooperates with the Fraunhofer Institute for Systems and Innovation in Karlsruhe, Germany. Associate partners of the project are the Federal Criminal Police Office (Bundeskriminalamt), the State Criminal Police Office Baden Wuerttemberg (Landeskriminalamt Baden-Württemberg) und the Saxon "Police University" (Sächsische Hochschule der Polizei). The first two act as consultants to the project as well as being end users. The Sächsische Hochschule der Polizei also plays an advisory role in the evaluation of state prosecution files. In addition to the planned publication of three books, guidelines will be formulated for three end-

[7] Cf. e.g. Dannecker 1987; *Schönecker/Schmidt/Oehler* 1981 give an overview for Europe; for a current overview see *Carl/Kilchling* 2016 or *Kilchling/Carl* 2016.

[8] The latest publication on comparative law in the field of economic and industrial espionage is the doctoral thesis by Föbus 2011; earlier works include Amelunxen 1977, Liebl 1987 and Tuck & Liebl 1988 all of which focus on now out-dated scenarios.

[9] Cf. Többens 2000.

[10] German: ‚Forschung für die zivile Sicherheit, cf. Bundesministerium für Bildung und Forschung', *Referat Sicherheitsforschung*, 2012.

user groups: small and medium-sized enterprises (SMEs)[11], the scientific research sector, and domestic law enforcement and intelligence agencies. The first two groups will receive a manual for dealing with economic espionage in a wider sense, while the authorities will obtain guidance notes on how to improve cooperation with their end-users.

This set-up was selected to best further the research interest of the project. WiSKoS aims to provide an overview of the threat level posed by economic and industrial espionage in Germany and across Europe. Apart from taking stock of the status quo, the need for optimization is to be assessed. This includes the search for alternative models and strategies in other European countries. Effective control is highly important for Germany as a scientific and a business location.

The focus of the project is not on large industrial companies – so-called "global players" – who often calculate their own levels of risk and financial vulnerability and, consequently, actively integrate internal systems of prevention and control into the running of their businesses. These companies act autonomously once a threat surfaces (i.e., without requesting the intervention of (national) law enforcement agencies).[12] Instead, WiSKoS focuses on the impact of economic and industrial espionage on SMEs that in some cases are the holders of vast special know-how as so-called "hidden champions".[13] While SMEs are frequently internationally active, due to their size, they are far more dependent on cooperation with (national) law enforcement agencies and other state authorities when affected by industrial espionage.[14] WiSKoS also includes the European sector of scientific research in its study since there threat levels and the awareness thereof are frequently

[11] Based on a secondary analysis conducted by the Bundeskriminalamt (BKA, Federal Criminal Police Office) the focus of research is large enterprises and not SMEs (cf. Kasper 2014).

[12] Cf. *Bundesamt für Verfassungsschutz* March 2010: pp. 6-7; *Bundesamt für Verfassungsschutz*, November 2008: p. 10.

[13] The defining criteria of *hidden champions* are contested. This publication defines *hidden champions* as SMEs that are leading in Europe or even worldwide in their niche sector (cf. Springer Gabler Verlag undated (a) or *Simon* 2007, p. 15).

[14] Cf. *Bundesamt für Verfassungsschutz* July 2014, p. 6.

mismatched.[15] The final two groups to be included in the project are domestic law enforcement and intelligence agencies, which constantly monitor economic and industrial espionage. These agencies have discovered that in the past the willingness to report suspected espionage to the police is considerably lower than for other offenses.[16] WiSKoS will analyse the current state of detection and prevention measures on an international scale and make suggestions on how to improve cooperation between companies and state regulatory and law enforcement authorities.

The project is divided into three modules which constitute self-contained units of research with an independent content and geographical focus as well as specifically tailored methodical approaches. At the same time, the modules are closely aligned and logically linked to each other.

Module 1, which has already been completed, provides a broad screening of national laws and the classification of threat levels (based on statistical material) among the current member states of the European Union (EU)[17] and the European Free Trade Association (EFTA). The module utilizes a descriptive-normative approach and includes a socio-cultural analysis of the relationship between the state and the economy. In addition to a comprehensive overview of the current status quo in the 28 EU member states as well as Switzerland (as a representative of the EFTA member states), the research conducted in this module was used to identify countries that are being contrasted with Germany in Module 2. WiSKoS identified as relevant differences 1) the scope of the country's economy, 2) the nature of the regulation of economic and industrial espionage inside and outside criminal law, and 3) the concrete threat level.[18] The classification of the latter is based on the

[15] This was communicated in preliminary conversations with possible interview partners prior to the interviews with German scientific organizations for the second module of the project.

[16] This was communicated by the Federal Criminal Police Office.

[17] "Current" pertains to the British EU referendum, the so called 'Brexit'.

[18] For details see Carl & Kilchling 2016. The concrete selection criteria are included in Section 4 in the chapter on comparative law.

existence of specific industries and economic sectors as well as on the potential attractiveness of targets.[19] The application of these criteria led to the selection of Austria, Bulgaria, Switzerland and the United Kingdom as countries suitable for an in-depth comparative analysis.

Module 2, which is currently in progress, deals with a detailed multi-level evaluation of the countries functioning as a contrast group to Germany. The problem analysis combines qualitative and quantitative research methods. In addition to the scrutiny of relevant literature and documentary sources, specific case analyses are selected to provide insight into cases as well as practices of the case work of police forces and law enforcement agencies. In Germany the case analysis is done by conducting an extensive file analysis. Concerning the foreign legal systems the analysis is restricted to the identification and interpretation of exemplary case studies. Another crucial element of the empirical fieldwork are workshops and complemental qualitative interview scenarios designed to analyse problems and solution approaches from the perspective of the most relevant stakeholders in the selected countries. The focus is on government representatives, SMEs as well as the scientific sector.

The aim of Module 3, which is currently in the planning stage, is to validate the situation description resulting from the second module. It deals with contrasting the solution approaches on the legislative and end user levels thus serving as a feedback mechanism for the previous findings. The method which is best suitable to achieve this goal is an extended survey of the area of unreported cases, which will be conducted by means of two independent surveys. This will be complemented via a 'proof-of'-concept that collects the opinion of German businesses on the possibility of transferring key findings, which are taken from the foreign countries' description of problems and solution approaches.

[19] For details see Carl & Kilchling 2016 which contains the findings of Module 1.

4. *Quantifiying the state of crisis*

Since the WiSKoS project commenced its research in 2015 some findings are already available.[20] The comparative analysis of the twenty-nine country reports showed economic and industrial espionage to be a universal threat. However, the perceived significance of the phenomenon varies notably. Only nine country experts reported that their nations were actively targeted by espionage and nine felt that the threat level was increasing. Economic and industrial espionage is punishable in twenty-five countries, all of which are civil law countries. In the common law countries included in the study, the United Kingdom and Ireland, as well as the countries with mixed legal system, Malta and Cyprus, there are no explicit penal provisions for economic and industrial espionage. No country expert reported the existence of legal definitions of either phenomenon. While the range of punishment varies considerably between the researched countries, it becomes evident that the punishment for economic espionage, which is an offense against state security, is always higher than that for industrial espionage, which is an offense against fair competition. The punishment is usually imprisonment and / or a fine. The hypothesized scarcity of statistical data was reflected in the county reports. Where crime statistics are available, the explanatory power of those statistics varies noticeably in its make-up and depth and provides extremely limited information on economic and industrial espionage. Relevant cases are frequently subsumed under "economic crime" in general. These findings display the current state of crisis and prove the necessity for further in-depth research on economic and industrial espionage that will be henceforth be conducted through the WiSKoS project.[21]

[20] All findings of Module 1 are presented in Carl & Kilchling 2016.

[21] Frequently updated information on the continuing research is available through http://wiskos.de/en/home.html.

Bibliography

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

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

Bundesamt für Verfassungsschutz (March 2010): ‚Proaktiver Wirtschaftsschutz: Prävention durch Information', Tagungsband zur 4. Sicherheitstagung des BfV und der ASW am 18.03.2010 in Köln.

Bundesamt für Verfassungsschutz (November 2008): *Spionage gegen Deutschland– Aktuelle Entwicklungen*, bfv-Themenreihe, Cologne.

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

Carl, S. & Kilchling, M. (eds.)(2016): *Economic and Industrial Espionage in Germany and Europe*, Vol. 1 Field Description (schedule for printing).

Corporate Trust (2012): 'Cyber war – Industriespionage 2012', München 2012, http://www.corporate-trust.de/pdf/CT-Studie-2012.pdf [10.05. 2016]. Zit. CT 2012.

Corporate Trust (2014): 'Cybergeddon – Industriespionage 2014', München 2014, http://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.

Föbus, *N.* (2011): ‚Die Insuffizienz des strafrechtlichen Schutzes von Geschäfts- und Betriebsgeheimnissen nach § 17 UWG', Dissertationsschrift, Frankfurt a.M.

Kasper, K. (April 2014): ‚Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse, Bundeskriminalamt (BKA)', http://www.bka.de/DE/Publikationen/Publikationsreihen/SonstigeVeroeff

entlichungen/SonstigeVeroeffentlichungen__node.html?__nnn=true [10.05.2016].

Kilchling, M. & Carl, S. (2016): ‚Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS)', in: P. Zoche, S. Kaufmann & H. Arnold (eds.): *Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung*, Berlin: Lit-Verlag (in print).

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

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

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

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

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', http://www.pst.ifi.lmu.de/Lehre/wise-12-13/jur-pm/ausarbeitung-zum-vortrag-am-08.01.2013-a.-scherf [21.04.2016].

Schönecker, L., Schmidt, E. & Oehler, D. (ed., 1981): Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der Europäischen Gemeinschaft sowie in Österreich und der Schweiz. Mit Hinweisen auf die neuere Gesetzgebung in den nordischen Staaten, in: Kölner Studien zur Rechtsvereinheitlichung.

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 a.M. / New York.

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.