Management Summary

Zwahlen, Fabienne, Marti, Irene, Richter, Marina, Konopatsch, Cathrine & Hostettler, Ueli (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Bern: University of Bern – Institute for Criminal Law and Criminology.

Background

Economic espionage is a complex issue (see Fleischer 2016; Tsolkas & Wimmer 2013). Firstly, the dividing line between economic espionage and industrial espionage is not a clear one in practice, there being close links between state and private-sector activities in many areas. Secondly, there is a lack of reliable data on the number of cases, perpetrators and the actual damage caused. Furthermore, it is difficult for the businesses affected to differentiate between economic espionage on the one hand and industrial espionage or other criminal activities (e.g. extortion) on the other. It is often difficult to identify the perpetrators and their intentions, and so in many cases attacks go entirely unnoticed. Moreover, many companies are reluctant to report any suspicions they have or incidents of espionage they discover, fearing damage to their reputation or economic losses should such information become public. Many cases thus go undetected, and knowledge about economic espionage is correspondingly sparse (see Kaspar 2014; Wimmer 2015).

In addition to studies by consulting firms such as KPMG and PWC (KPMG 2019; PWC 2016), for the German-speaking countries there is currently one up-to-date academic study on this topic, which was carried out by the Max Planck Institute for Foreign and International Criminal Law together with the Fraunhofer Institute for Systems and Innovation Research. The WISKOS study (Bollhöfer & Jäger 2018) shows that in the past, one in three SMEs in Germany was the victim of economic espionage or was affected by competitive intelligence. There are currently no such studies for Switzerland. In order to investigate the extent of economic espionage in Switzerland more thoroughly, the Federal Intelligence Service (FIS) commissioned the School of Criminology, International Criminal Law, Corporate Crime and Criminal Policy at the University of Bern to conduct a study on this topic among companies in Switzerland. The aim of the study was to draw up a detailed inventory of the subject, to assess the financial and other damage and to determine the quality of cooperation between companies and the authorities. The results also provide the FIS with information which aids counter-espionage efforts and the further development of the prevention and awareness programme Prophylax. On the basis of the results it is hoped specifically to improve protection against espionage, for example by raising awareness among businesses and the research community in Switzerland.

Study design and methodology

There were two parts to the study:
1) A **qualitative survey**: one-to-one interviews conducted with key players
2) A **quantitative survey**: random sampling among representative businesses of varying size and across a range of fields.

The survey tools (guidelines for interviews and online questionnaire) were developed in conjunction with the FIS.

Table 1: Overview of data for sub-study 1 (qualitative)

	Number	Number of participants/Interview length
Specialists	8	8 * 60-90 mins
SMEs	27	27 * 60-90 mins
Corporations	13	15 * 60-90 mins
Universities/Research institutes	3	4 * 60-90 mins

Study «Wirtschaftsspionage in der Schweiz», University of Bern, 2020

Table 2: Overview of data for sub-study 2 (quantitative)

	Number	Percent
Sample	**3065**	**100%**
Response	**362**	**12%**
By economic sector	Number	Percent
Primary sector (raw material extraction)	19	5%
Secondary sector (manufacturing/material processing)	145	40%
Tertiary sector (services)	156	43%
No data	42	12%
By company size	Number	Percent
Very small: fewer than 10 employees	33	9%
Small: 10-49 employees	250	69%
Medium: 50-249 employees	62	17%
Large: more than 250 employees	14	4%
No data	3	1%

Study «Wirtschaftsspionage in der Schweiz», University of Bern, 2020

Cases of espionage and suspected espionage in companies

Of the companies surveyed, **15%** stated in the quantitative study that they had experienced an incident involving economic espionage. In the one-to-one interviews it was found that **one third of all companies** have been the **victim of economic espionage** at least once. These are incidents that have been identified by the company itself and/or by the FIS as cases of economic espionage. The size of the company does not appear to play a significant role: both SMEs and large companies are affected by economic espionage. The results of this study show that economic espionage particularly affects the following sectors: construction, information, communication and publishing, mechanical engineering

and industry, aerospace technology, defence industry, pharmaceuticals and life sciences, electronics and metrology. The mechanical engineering and industrial sectors (result of quantitative study) and the pharmaceutical and life science sectors (result of qualitative study) are most affected by specific incidents of espionage.

When there is a case of espionage, the question of damage quickly arises. It is very difficult for either the affected party or external specialists to quantify the extent of the damage. Some studies attempt to make estimates for individual sectors, the national economy or society as a whole (e.g. Bitkom 2016; PWC 2016), but these are unreliable for practical and methodological reasons and should therefore be treated with caution. It is easier to quantify the direct material damage, such as loss of production, the loss of a transaction or additional expenditure on combating espionage, such as the cost of IT and communications, etc. By contrast, it is difficult to quantify the long-term damage to reputation that occurs when a case becomes public. Reputational damage may result in a major material loss if orders and customers move away in the long term. In our survey, 11% of the companies that had been aware of a case of espionage said that it had jeopardised the existence of the company. This indicates the ability of economic espionage to cause serious damage.

Prevention

The companies surveyed consider internal prevention to be much more important than support from external specialists or government agencies. They make use of various forms of prevention (structural aspects and organisational regulations, training and awareness-raising among employees, IT and telecommunications measures as well as physical and technical security). However, the degree of prevention varies greatly and is strongly related to the size of the company and thus also to the resources available for espionage prevention. Moreover, SMEs in particular often have very little awareness of the risks associated with data exchange and digital communication (such as email).

Future developments

The companies surveyed mentioned in particular the issues of digitalisation and globalisation when asked about future developments. Digitalisation poses new challenges for companies with regard to the secure management of digital data (e.g. production data, customer data). A large number of attacks already occur electronically, and this is likely to be more of a problem in future. Globalisation also poses a challenge. As markets become more global, new questions regarding international patent protection arise.

At the same time, business partners, suppliers and customers are becoming increasingly international in nature, and so the continued existence of different national legal contexts and business cultures causes difficulties. Finally, companies now employ staff from all over the world. While some companies have stated that their strategy is primarily to recruit people with personally known referees, this limits the pool of qualified employees that they can draw on. SMEs in particular therefore find it much harder to guarantee security when recruiting new staff. Finally, there is the question of the political significance of the issue and the tasks and corresponding institutional and personnel resources required by federal and cantonal agencies. According to the experts we interviewed, Switzerland disposes of rather fewer institutional and material resources for preventing and combating espionage than other countries.

Bibliography

Bollhöfer, Esther & Jäger, Angela (2018). Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Band A 8 09/2018. Freiburg i. Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

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

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

KPMG (2019). Wirtschaftskriminalität und was man dagegen tun kann. *Audit Committee News – Risk Management & Compliance*. 66 (Q3 2019): 1–6. https://home.kpmg/content/dam/kpmg/ch/pdf/wirtschaftskriminalitaet-was-man-dagegen-tun-kann-de.pdf [accessed on 16.7.2019].

PWC (2016). Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. https://www.pwc.de/wirtschaftskriminalitaet. [accessed on 16.7.2019].

Tsolkas, Alexander & Wimmer, Friedrich (2013). Wirtschaftsspionage und Intelligence Gathering. Neue Trends der wirtschaftlichen Vorteilsbeschaffung. Wiesbaden: Springer.

Wimmer, Bruce (2015). Business Espionage. Risk, Threats, and Countermeasures. Waltham, MA: Elsevier.