INSTITUTE FOR EMPLOYMENT RESEARCH
The Research Institute of the Federal Employment Agency

IAB Short Policy Report

Up-to-date analyses by IAB

2|2025

In brief

- Industrial and economic espionage are serious issues that can result in significant financial damage – not only for the companies directly affected but for the economy as a whole.
- New survey data from the IAB show that 9 percent of all establishments in Germany have fallen victim to an espionage attack in the past five years. Around 12 percent of establishments reported at least one suspected incident or confirmed attack (see Figure A1).
- More than half of all suspected cases involved hacking of IT systems, while for confirmed attacks the share was close to two-thirds.
- In over one-fifth of businesses that were targeted, data were stolen.
- Both suspected and confirmed cases of espionage were particularly common in the information and communication sector and in the wholesale trade.
- Innovative and export-oriented firms in competitive markets were especially likely to be affected by industrial or economic espionage.

Survey on industrial and economic espionage in Germany

Nine percent of businesses fall victim to espionage

by Albrecht Glitz, Susanne Kohaut and Iris Möller

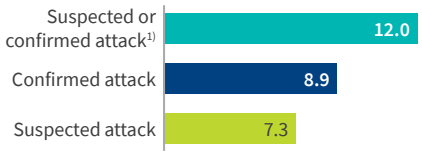
Industrial and economic espionage – rival companies or intelligence services gaining unauthorised access to business information – is seen by businesses as a growing threat. For the first time, representative data from the 2023 IAB Establishment Panel are now available on this topic for Germany. It shows that around 12 percent of businesses – across all sectors and company sizes – report being affected by industrial or economic espionage.

These forms of espionage (see Info Box 1) are not new phenomena; evidence of them can be found as far back as ancient and medieval times (Norwich 1990; Ben-Atar 2004). It is thought that industrial and economic espionage are widespread in many industrialised and emerging economies today, and there are indications that this kind of activity is currently intensifying: the majority of companies in Germany rate the threat posed by industrial espionage (in the broadest sense) as high or very high and expect it to increase further in the future (Bitkom 2023).

A1

Industrial or economic espionage affects around one in ten businesses

Data from the businesses, shares in percent



[1)] Attack and suspicion can be reported simultaneously.

Source: IAB Establishment Panel 2023, weighted values. © IAB

1

Definition

The terms economic espionage and industrial espionage are often used interchangeably in everyday language, but they actually refer to different phenomena: industrial espionage refers to actions undertaken by individual companies against their competitors for commercial purposes, whereas economic espionage refers to actions carried out in the economic sphere on behalf of a foreign intelligence service and for reasons that are not purely commercial in nature (Nasheri 2005).

Estimates suggest that the economic damage caused by espionage – broadly defined – amounts to roughly 400 billion dollars annually in the United States (IP Commission 2017), equivalent to about 2.1 percent of GDP. The figure for Germany is estimated at around 200 billion euros (Bitkom 2023), or roughly 4.8 percent of GDP. However, due to the limited data available and the fundamental difficulty of quantifying the potential harm (Kasper 2015), such estimates vary widely depending on the study.

2

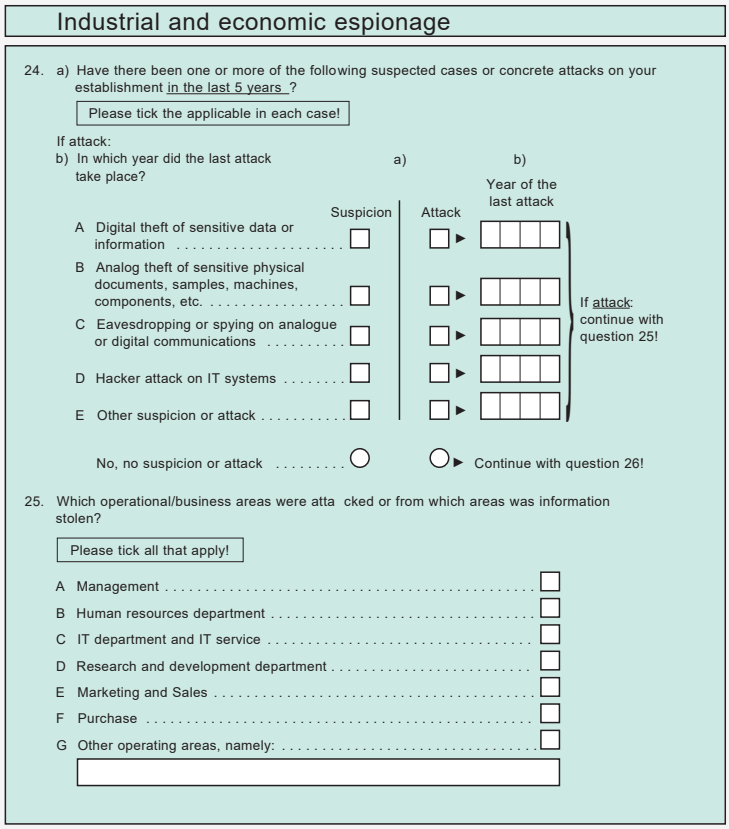
The IAB Establishment Panel

The IAB Establishment Panel is a representative employer survey on business-level determinants of economic activity. Around 15,000 establishments of all sizes and from all sectors are surveyed each year. The population covered consists of establishments with at least one employee subject to social security contributions. The survey has been conducted since 1993 in the western German federal states and since 1996 in the eastern German federal states. As a comprehensive longitudinal dataset, it serves as a key resource for researching the demand side of the labour market. In 2023, response rates were approximately 70 percent among establishments surveyed repeatedly and around 11 percent among first-time respondents.

For more information on the IAB Establishment Panel, see Ellguth et al. (2014) or the IAB website (http://www.iab.de/de/erhebungen/iab-betriebspanel/).

Data access to the IAB Establishment Panel: https://fdz.iab.de/betriebsdaten/iab-betriebspanel-iab-bp-version-9321-v1/ (doi.org/10.5164/IAB.FDZD.2316.de.v1).

Specific survey question on the topic of "Industrial and Economic Espionage" in the 2023 IAB Establishment Panel:



Industrial and economic espionage

24. a) Have there been one or more of the following suspected cases or concrete attacks on your establishment in the last 5 years ?

Please tick the applicable in each case!

If attack:
b) In which year did the last attack take place?

	Suspicion	a) Attack	b) Year of the last attack
A Digital theft of sensitive data or information	☐	☐ ▶	
B Analog theft of sensitive physical documents, samples, machines, components, etc.	☐	☐ ▶	
C Eavesdropping or spying on analogue or digital communications	☐	☐ ▶	
D Hacker attack on IT systems	☐	☐ ▶	
E Other suspicion or attack	☐	☐ ▶	
No, no suspicion or attack	○	○ ▶ Continue with question 26!	

If attack: continue with question 25!

25. Which operational/business areas were atta cked or from which areas was information stolen?

Please tick all that apply!

A Management ☐
B Human resources department ☐
C IT department and IT service ☐
D Research and development department ☐
E Marketing and Sales ☐
F Purchase ☐
G Other operating areas, namely: ☐

China and Russia are frequently accused of conducting systematic economic espionage on a large-scale (IP Commission 2021; Verfassungsschutz 2024), but such activities are thought to occur between allied countries, too, as part of general intelligence gathering. This is suggested, for instance, by the 2013 WikiLeaks revelations in 2013 concerning the surveillance activities of the National Security Agency (NSA) —the largest foreign intelligence agency of the United States— in France, Germany and Japan (Corporate Trust 2017a).

Military and defence technology has traditionally been of particular interest to foreign intelligence services engaged in economic espionage. But other areas are frequently targeted too, such as aerospace, advanced electronics, telecommunications, nanotechnology, biotechnology, energy and financial services (Corporate Trust 2017a). These are all sectors which are closely involved with technology and innovation, where business secrets are vital – making them especially attractive targets for industrial espionage by commercial competitors as well.

Despite its economic importance, industrial and economic espionage remains difficult to assess with any certainty, as reliable data are scarce. Whether committed by competitors or foreign intelligence services, many attacks go undetected by the targeted organisations. Even when attacks are detected, they are often not disclosed due to fears of reputational damage among investors, customers and staff (Office of the National Counterintelligence Executive 2011).

Most empirical data on this issue in Germany published to date have come from studies carried out by private consultancy and security firms such as Ernst & Young, KPMG, PricewaterhouseCoopers and Corporate Trust. One major issue with these studies – as in many other countries (European Commission 2018) – is the fact that they are often too small and not representative. Typically, the number of businesses successfully surveyed is in the low hundreds, with response rates often below 10 percent (Kasper 2015). This limited evidence base makes it difficult to draw robust conclusions about the nature and extent of industrial and economic espionage.

To help fill this gap and gain new insights into this complex area, the 2023 IAB Establishment

Panel included a dedicated survey module on industrial and economic espionage (see Info Box 2). The IAB Establishment Panel covers businesses of all sizes and operating in all industry sectors in Germany. This includes smaller companies – a major strength as compared to previous studies.

Nine percent of businesses in Germany report espionage attacks

The 2023 IAB Establishment Panel asked whether any suspected or confirmed cases of espionage had occurred in the businesses surveyed over the preceding five years (see Info Box 2). In total, 12 percent of respondents reported one or more suspected or confirmed espionage incidents affecting their business or office (see Figure A1). These establishments employ around 22 percent of the country's workforce.

The proportion of confirmed espionage attacks (8.9 percent) is slightly higher than that of suspected incidents (7.3 percent).[1] As such, these figures are significantly lower than those reported by the German Association for Information Technology, Telecommunications and New Media (Bitkom), which has regularly surveyed German businesses on economic security since 2015.

In Bitkom's most recent study (Bitkom 2024), 81 percent of industrial companies surveyed said they had fallen victim to data theft, industrial espionage or sabotage in the preceding twelve months. This substantial discrepancy is partly due to the broader scope of the Bitkom survey. Moreover, it only covers industrial firms with at least ten employees and an annual turnover of one million euros or more (N = 1,002), which likely contributes to the higher share of affected companies.

The results of the IAB Establishment Panel are more in line with those of the most recent short study on industrial espionage carried out by the international security consultancy Corporate Trust. In the latter survey, 29.1 percent of companies reported that they had been targeted by espionage or other forms of information leakage in the preceding three years (Corporate Trust 2017b). Here again, only companies with at least ten employees and annual revenue of at least one million euros were included in the study (N = 356). In both the Bitkom and Corporate Trust surveys, selection bias among participating companies cannot be ruled out.

Hacker attacks on IT systems are the most common form of espionage

Espionage can take many forms, but hacker attacks[2] on IT systems are the most frequently reported: half of all establishments that suspect espionage incidents cite hacker attacks (50.8 percent – see Table T1). Among those that experienced a confirmed attack, 61.5 percent said it had taken the form of a hacker attack on IT systems. This means that 5.5 percent of all businesses in Germany experienced hacker attacks, while 3.7 percent suspected they had.

Over a third of companies with suspected cases believed sensitive digital data or information had been stolen (36.1 percent), which equates to 2.6 percent of all businesses in Germany. Among those affected by confirmed attacks, more than a fifth (21.4 percent) reported data theft – 1.9 percent of all companies nationwide. Whether all of these cases qualify as industrial or economic espionage in the strict sense remains uncertain.

T1

Type and manner of the suspected or confirmed espionage

Data from the businesses, shares in percent

	Suspected attack		Confirmed attack	
	Share of ...		Share of ...	
	... businesses with suspected attack	... all businesses	... businesses with confirmed attack	... all businesses
Hacker attack on IT systems	50.8	3.7	61.5	5.5
Digital theft of sensitive data or information	36.1	2.6	21.4	1.9
Eavesdropping or spying on analogue or digital communications	17.3	1.3	9.4	0.8
Analogue theft of sensitive physical documents. samples. machines. components. etc.	10.3	1.3	18.4	1.7
Other suspicion or attack	31.0	2.3	16.8	1.5

Quelle: IAB-Betriebspanel 2023, gewichtete Werte. © IAB

[1] Note that businesses report confirmed and suspected attacks separately (see Info Box 2), with many reporting both. As a result, the figures of 8.9 percent and 7.3 percent do not add up to the total of 12 percent referred to above. In what follows, we report figures for confirmed and suspected attacks separately.

[2] It cannot be ruled out that respondents included ransomware under "hacker attacks on IT systems," even though this does not constitute espionage in the strict sense. Ransomware refers to malicious software that restricts or blocks access to data and systems, with a ransom demanded in exchange for restoring access.

Reports of wiretapping or surveillance of analogue or digital communication are much less common. Of the businesses with suspected cases, 17.3 percent reported possible wiretapping; among those with confirmed incidents, the share was 9.4 percent. Across all businesses, this equates to 1.3 percent reporting suspected cases of wiretapping or surveillance and 0.8 percent confirmed cases.

Businesses are somewhat more frequently exposed to analogue theft – of sensitive physical documents, prototypes, machinery or components – but are somewhat less likely to express suspicions to this effect. One in ten businesses with suspected espionage believes it was the victim of theft, while almost one in five businesses that experienced a confirmed attack was in fact stolen from. Across all establishments, 1.3 percent suspected such theft and 1.7 percent actually experienced it.

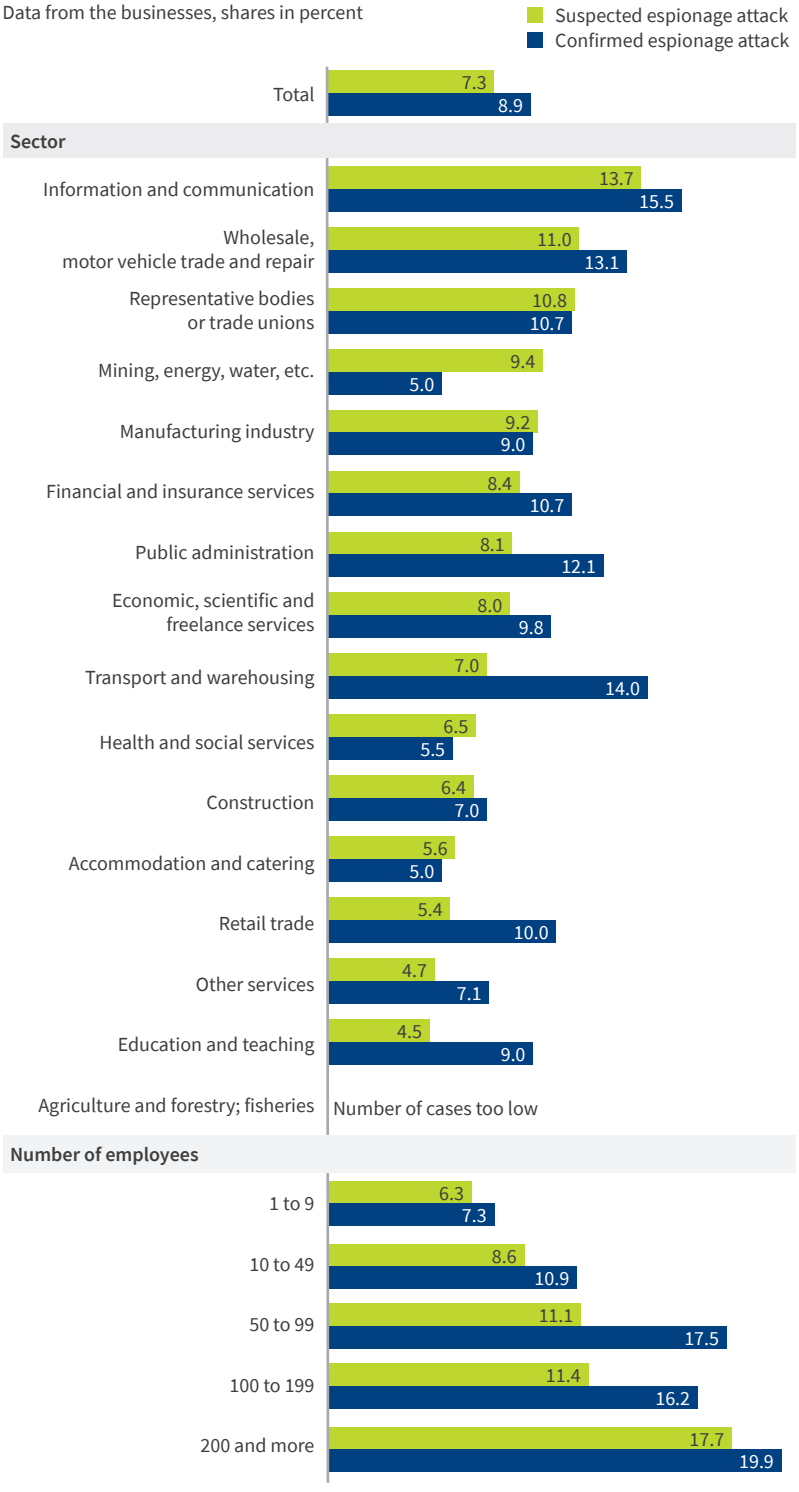
The category "Other suspicion" is the third most frequently cited among companies reporting suspected incidents (31 percent – see Table T1). This indicates that many suspicions fall outside the predefined categories. Among companies with confirmed attacks, the share that ticked "Other attack" is significantly lower, at 16.8 percent. The exact nature of these incidents remains unclear. Across all establishments, "Other suspicion or attack" accounts for 2.3 percent (suspected) and 1.5 percent (confirmed) respectively.

Overall, the findings suggest that industrial and economic espionage primarily occurs through digital channels, e.g. in the form of cyberattacks or digital surveillance.

A2

Businesses are affected by espionage to varying degrees depending on their sector and size

Data from the businesses, shares in percent



Source: IAB Establishment Panel 2023, weighted values. © IAB

Companies in the information and communications sector are most frequently targeted

Espionage is most frequently reported in the information and communications sector: 13.7 percent of businesses in this field report suspected cases and 15.5 percent confirmed attacks (see Figure A2). Suspected and confirmed incidents are also common in the wholesale sector, the motor vehicle trade and repair sector (11 percent suspected, 13.1 percent confirmed), as well as among representative bodies or trade associations (around 11 percent for both).

Above-average rates of confirmed attacks are also found in transport and logistics (14 percent), public administration (12.1 percent), and financial and insurance services (10.7 percent). In manufacturing, there are almost equal numbers of sus-

pected and confirmed cases, at 9.2 and 9.0 percent respectively.

In principle, no sector appears completely immune from industrial and economic espionage. Notably, it is not just manufacturing that is affected: many service and public-sector organisations are targeted, too. This aligns with Bitkom's findings, which likewise show espionage, sabotage and data theft across all industries.

Company size is a factor

In addition to the sector, company size also significantly influences vulnerability to espionage. Small establishments with up to nine employees report lower levels of suspected attacks (6.3 percent) and confirmed attacks (7.3 percent), while nearly one in five large businesses (200+ employees) has actually experienced an attack (19.9 percent) or at least suspects one has occurred (17.7 percent – see Figure A2). In general, the larger the company, the higher the risk of becoming a target.

Innovative, exporting, and research-driven businesses in competitive markets are especially affected

Not all businesses are equally affected by espionage activities. It can be assumed that espionage primarily occurs when the target offers a strategic competitive advantage. This is particularly true in research-oriented and innovative businesses operating in competitive environments. Among companies engaged in research and development, 17.8 percent reported suspicions of espionage and 22 percent say they experienced confirmed attacks – much higher than the respective shares for non-R&D companies (6.8 percent and 8.3 percent respectively – see Table T2).

Exporting firms are also more affected by espionage activities: 12.2 percent reported suspected espionage incidents, compared to roughly half that amount among non-exporters. Meanwhile, confirmed attacks were reported by 14.4 percent of exporters versus only 7.9 percent of non-exporters. This is plausible, since exporters tend to be more productive and innovative, making them more attractive targets for espionage.

One key finding is that innovative companies are significantly more likely to be targeted. For example, 13.5 percent of companies with product innovations[3] reported attacks, compared to 5.7 percent of those without. The differences are even starker when it comes to process innovations[4]: both suspected and confirmed attacks are more than twice as common in innovative firms (14.2 vs 6.4 percent and 16.7 vs 7.7 percent).

Companies subject to significant competitive pressure are likewise more commonly affected (see Table T2). As competition intensifies, so does the proportion of firms reporting suspected incidents or actual attacks. Among firms under considerable pressure, 12.6 percent experienced attacks – more than double the rate among those under no pressure (5.7 percent). A likely explanation is that in highly competitive markets, the incentive for industrial espionage is greater, as it may provide

T2

Suspicion of espionage and attack according to business criteria

Data from the businesses, shares in percent

		Espionage	
		Suspected attack	Confirmed attack
Research and development	yes	17.8	22.0
	no	6.8	8.3
Exporting firm	yes	12.2	14.4
	no	6.4	7.9
Product innovations	yes	9.5	13.5
	no	5.8	5.7
Process innovations	yes	14.2	16.7
	no	6.4	7.7
Competitive pressure	none	5.6	5.7
	low	5.8	6.9
	medium	8.2	9.6
	high	8.8	12.6
Total		7.3	8.9

Note: Probit estimates show significant differences for the variables shown in this table.
Source: IAB Establishment Panel 2023, weighted values. © IAB

[3] Businesses are considered innovative if they have introduced product or process innovations. If, in the preceding financial year, a business improved or further developed a product or service it offered previously, added a product or service already available on the market to its range, or introduced an entirely new product or service requiring the creation of a new market, it is regarded as being engaged in product innovation.

[4] Businesses that have developed or introduced new processes that significantly improve production procedures or the provision of services are considered to be engaged in process innovation.

critical knowledge that helps companies survive or catch up with market leaders.

These findings are a clear indication that industrial and economic espionage is strategically focused, especially targeting technologically advanced businesses engaged in international competition.

IT departments are most frequently targeted

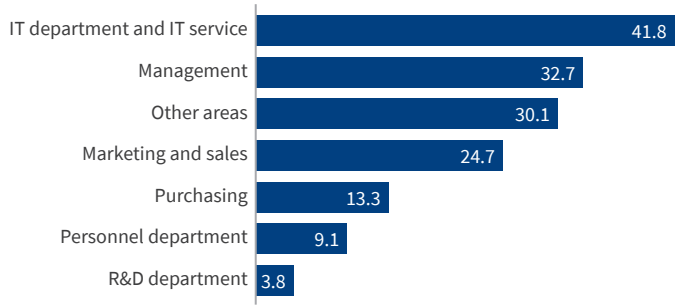
Within affected businesses, not all departments are equally targeted. The most frequently mentioned target is the IT department and IT service (41.8 percent – see Figure A3). Almost one third (32.7 percent) report attacks on the management. The category "Other departments" was mentioned in third place (30.1 percent), followed by marketing and sales in a quarter of businesses (24.7 percent). Procurement (13.3 percent) and HR (9.1 percent) were less frequently affected.

Research and development was rarely cited (3.8 percent), partly because only 5 percent of all businesses engage in R&D. But among R&D firms, 13.4 percent reported that their research departments were targeted.

A3

Espionage attacks most frequently target IT departments in companies

Data from the businesses, shares in percent



Source: IAB Establishment Panel 2023, weighted values. © IAB

Conclusion

Industrial and economic espionage can cause significant harm, both to individual businesses and the economy at large. Despite their economic significance, it has so far been difficult to form a reliable picture of these phenomena, as no representative data have been available.

The 2023 IAB Establishment Panel helps close this gap. The new data provide an overview of the prevalence of espionage in Germany in recent years, with 12 percent of businesses reporting suspected or confirmed attacks in total. Most incidents are digital in nature – cyberattacks or digital surveillance. However, the true extent is likely to be much greater, since many businesses may be unaware that they have been targeted by espionage.

Not all businesses are equally affected: large firms with 200+ employees are far more likely to fall victim to industrial and economic espionage. Moreover, innovative firms operating under competitive pressure are also more frequently targeted. A likely explanation is that in highly competitive markets, rivals have greater incentives to engage in industrial and economic espionage, since it may yield critical knowledge that helps companies survive or catch up with market leaders. The findings highlight that industrial and economic espionage is not only widespread but also strategically targeted.

With geopolitical tensions rising and rapid advances in areas such as AI, bioengineering, robotics and nanotechnology, the incentives for industrial and economic espionage are likely to increase. For Germany as a business location, it will become even more important in the future to monitor developments in this area and implement effective countermeasures in order to limit damage to the economy as a whole.

Literature

Ben-Atar, Doron S. (2004): Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power. Yale University Press.

Bitkom (2023): Wirtschaftsschutz 2023. Study retrieved at http://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf on 15 January 2025.

Bitkom (2024): Wirtschaftsschutz 2024. Study retrieved at http://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf on 15 January 2025.

Corporate Trust (2017a): NSA Report. Systemische Analyse der Snowden-Dokumente zum Schutz der deutschen Wirtschaft. Study retrieved at www.corporate-trust.de/wp-content/uploads/2023/11/NSA-Report.pdf on 15 January 2025.

Corporate Trust (2017b): Future Report. Weltweite Mega-Trends und Ihre Sicherheitsherausforderungen. Study retrieved at www.corporate-trust.de/wp-content/uploads/2023/11/Future_report_2017.pdf on 15 January 2025.

Ellguth, Peter; Kohaut, Susanne; Möller, Iris (2014): The IAB Establishment Panel – methodological essentials and data quality. Journal for Labour Market Research, 47, p. 27–41.

European Commission (2018): The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber. Study retrieved at https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1 on 15 January 2025.

IP Commission (2017): Update to the IP Commission Report – The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy.

IP Commission (2021): The IP Commission 2021 – Updated Recommendations.

Kasper, Karsten (2015): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse, Bundeskriminalamt 2015.

Nasheri, Hedieh (2005): Economic Espionage and Industrial Spying. Cambridge University Press.

Norwich, John Julius (1990): Byzantium – The Early Centuries. Penguin Books.

Office of the National Counterintelligence Executive (2011): Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage. Study retrieved at https://nsarchive.gwu.edu/document/21451-document-55 on 15 January 2025.

Verfassungsschutz (2024): Verfassungsschutzbericht 2023.

Albrecht Glitz*), PhD

is Associate Professor at Universitat Pompeu Fabra and affiliated professor at the Barcelona School of Economics, IPEG and the ROCKWOOL Foundation Berlin.

albrecht.glitz@upf.edu

Dr. Susanne Kohaut

is a researcher of staff at the Research Department "Establishments and Employment" at the IAB.

susanne.kohaut@iab.de

Dr. Iris Möller

is a researcher of staff at the Research Department "Establishments and Employment" at the IAB.

iris.moeller@iab.de

*) Albrecht Glitz thanks the ROCKWOOL Foundation Berlin for the financial support of the project (Project number 2006, „Economic Espionage, Globalization and Welfare").

Imprint | IAB-Kurzbericht (IAB Short Policy Report) No. 2, May 30, 2025 | Publisher: Institute for Employment Research (IAB) of Bundesagentur für Arbeit, 90327 Nürnberg | Editor: Martina Dorsch | Graphic layout: Nicola Brendel | Foto: Wolfram Murr, Fotofabrik Nürnberg and private | Rights: This publication is published under the following Creative Commons License: Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) https://creativecommons.org/licenses/by-sa/4.0/deed.de | IAB on the Internet: http://www.iab.de. You can download this Report and other publications from here free of charge | Inquires: IAB.Kurzbericht@iab.de | ISSN 0942-167X | DOI 10.48720/IAB.KB.2502.en