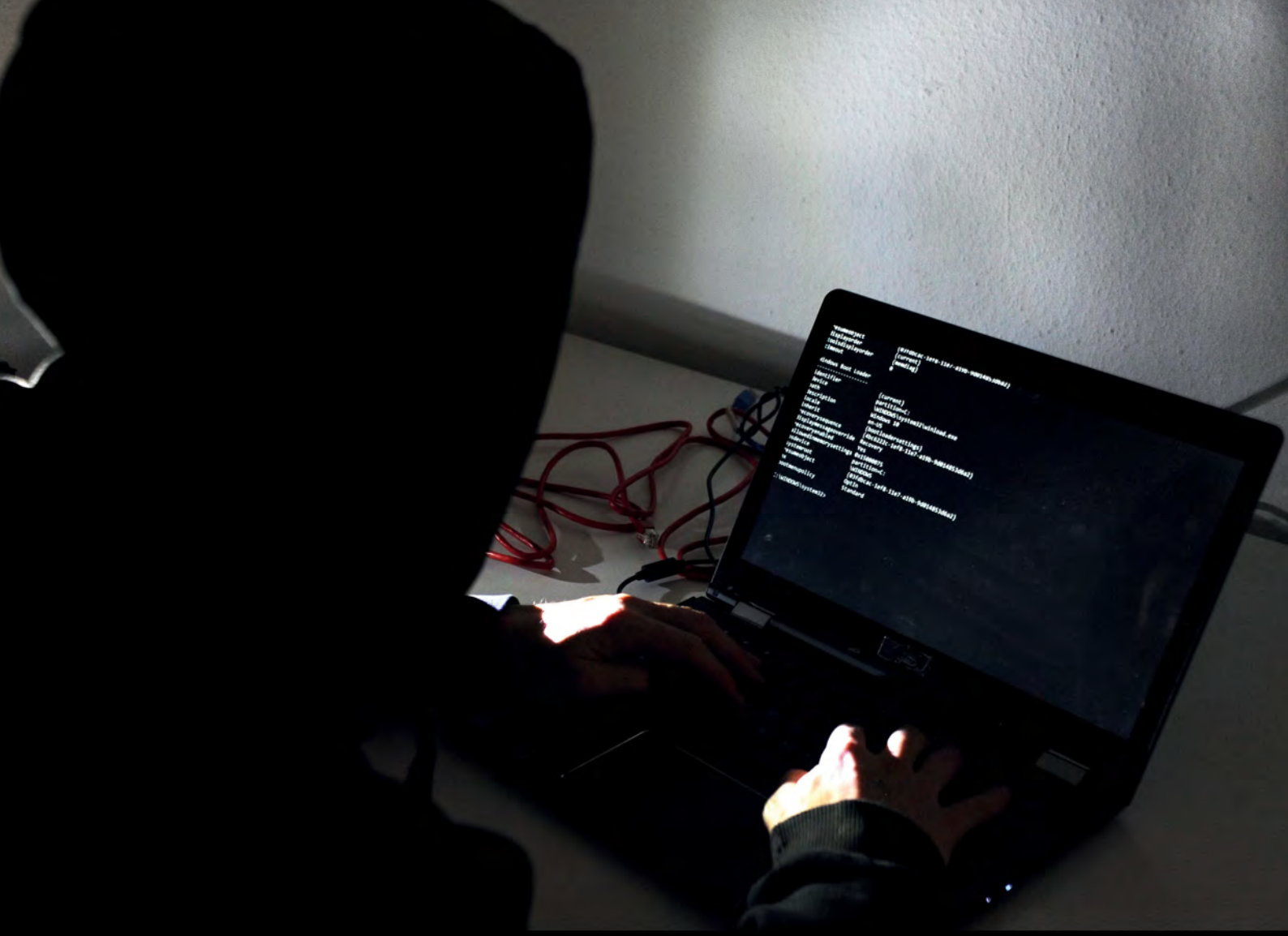


Anti-Espionage Strategies

The competition isn't sleeping, it's spying. And especially small and medium-sized businesses are increasingly falling victim to criminal competitors or being targeted by foreign intelligence services. Nevertheless, most cases remain shrouded in mystery. **Michael Kilchling** and his team at the **Max Planck Institute for Foreign and International Criminal Law** in Freiburg are now attempting to shed some light on the phenomenon. Together with colleagues at the Fraunhofer-Gesellschaft, they are conducting research into the scale of industrial espionage in Germany, how companies are combating it and how the authorities could better support them in their efforts.

Photo: dpa

TEXT **BENNO STIEBER**

Rieder, a company specializing in concrete and headquartered in Kolbermoor, Bavaria, greeted the visiting Chinese CEO as a welcome partner. The firm is renowned for its innovative building materials – its fiberglass concrete slabs turned the Soccer City stadium in Johannesburg into an architectural showpiece at the soccer World Cup in 2010 – and it was delighted to have found a local partner for a Chinese construction contract worth millions. No one in Kolbermoor suspected that the Chinese company was really only interested in stealing cutting-edge know-how from Germany in order to take over the contract on its own.

While the CEO from the Far East was touring the plant, Rieder employees spotted a mini-camera attached to their guest's belt. Instead of allowing their visitor to continue exploring the company's inner sanctums, they called the police. Analysis of the belt camera's data later revealed that the material would have been sufficient to copy and reproduce the high-tech components in China. The damage to the medium-sized company would have been immeasurable.

The attempted espionage in the Bavarian province is a fortunate exception compared with other cases examined by the "WiSKoS – Economic and industrial espionage in Germany and Europe" research project. The perpetrator, objective and motive were all apparent. The case was quickly and successfully dealt with and no long-term damage was done. The Munich District Court handed down a suspended sentence to the spy and ordered him to pay damages.

Such outcomes tend to be the exception in cases of economic espionage by foreign intelligence services and, above all, spying by competitors. These kinds of attacks are often launched via fiberoptic cables, and victims don't notice that a remote computer has stolen valuable data until it's too late. Rarely is it established whether the aim was sabotage or actually to steal know-how. Was the attack sponsored by foreign intelligence services, or were the hackers hired by direct competitors? In many cases, it isn't even possible to quantify the damage caused to the company attacked. Particularly when attacks are carried out from cyberspace, the perpetrators, background details and frequently even the actual purpose of the strike remain shrouded in mystery.

This was the case in an attack on the German Aerospace Center (DLR) in 2014, when all of its operating systems were infiltrated by trojans over the course of several months. The IT experts from the organization's cyber defense unit discovered Chinese characters in the trojans' code, but this may have been a diversion tactic by another intelligence agency. At the time, the German news magazine Der Spiegel reported that the DLR had called in the National Cyberdefence Centre in Bonn, which specializes in this kind of attack. Still, it was never determined who was actually behind it.

Espionage takes place in gray areas, and it is most successful when it remains undetected. This makes it exciting material for films and novels set in the Cold War era. But also in today's globalized and digital world, it offers a highly promising opportunity for business competitors or governments in both industrialized and emerging countries to keep pace with leading-edge developments from rival research labs abroad. However, in times of open markets and international corporations, the conditions for such espionage have changed tremendously – largely unnoticed by politicians and scientists.

SPECIALIST LITERATURE FROM THE COLD WAR ERA

When the research team at the Max Planck Institute for Foreign and International Criminal Law in Freiburg and the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe, headed by Michael Kilchling and Esther Bollhöfer, started work on assessing the scale of the current threat to medium-sized businesses, the researchers were surprised by how little substantiated empirical knowledge there was on economic and industrial espionage in Europe. "We realized that it's a real blind spot," says Kilchling, a Senior Researcher at the Max Planck Institute in Freiburg.

And it's not just spy thrillers that are set in the Cold War period; most of the specialist literature on economic espionage is from that era, too. The insights

Attacks from the web: The perpetrators are often in far-away places such as Russia, India or the Caribbean. It is difficult for German investigators to track them down; they are often defeated by national borders.

Dangerous insights: Trade secrets are often worth millions. Small and medium-sized businesses in particular need more support from the government to protect themselves.

were obtained before borders were opened and the European single market created, during a time when national economies still existed and were widely regarded as an asset worthy of state protection.

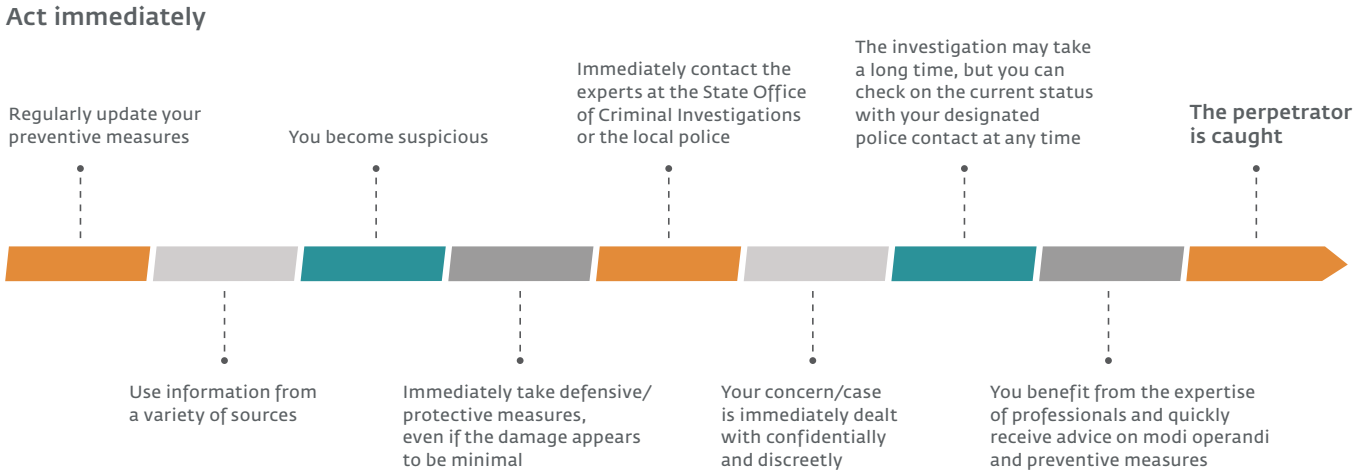
The joint WiSKoS research project aims to close this gap. The Max Planck Institute carried out the legal and criminological analysis of the cases and conducted expert interviews in other European countries, while the Fraunhofer Institute used its extensive connections with industry to conduct the survey of companies. "The collaboration proved extremely fruitful, as we have good access to public authorities and the Fraunhofer Institute enjoys an excellent reputation in industry," says Michael Kilchling. Nevertheless, the project was a challenge for everyone involved. The researchers used very different approaches and methods to analyze the status quo and, on the basis of their findings, to establish not only a core body of knowledge, but also a set of practical recommendations.

The team initially conducted a survey to obtain as comprehensive an overview as possible of the threats facing medium-sized companies in Germany. The researchers then examined the legal situation in Europe and how the authorities deal with the issue, so as to develop defensive strategies for companies and public authorities.

Esther Bollhöfer, an academic staff member at the Fraunhofer ISI, is managing the project modules that are under the responsibility of her institute. Her colleague who carried out the survey was surprised by the willingness of medium-sized companies to provide information about their shortcomings with respect to security: no fewer than 612 out of 8,300 randomly selected SMEs returned the questionnaire to the research group. One in five companies admitted they didn't have an anti-espionage strategy in place. Many of the companies would like to see the government provide more support with preven-

The team in Freiburg: Elisa Wallwaey, Michael Kilchling and Susanne Knickmeier (from left) are working on the WiSKoS project at the Max Planck Institute for Foreign and International Criminal Law.

Photo: CCO (top), Markus Herb (bottom)



Specific recommendations: The scientists advise companies to develop an anti-espionage strategy before it's too late. This includes suitable preventive measures and a plan governing how employees and management should respond in the event of an attack.

tion. Only ten companies rejected the idea of state intervention.

Despite the anonymity of the survey, few companies were willing to disclose how they deal with suspected cases internally. "This may mean that they don't wish to discuss it, but it could also indicate that they have no strategy in place," says Esther Bollhöfer. Of those who responded, the majority undertake their "own measures" – in other words, they conduct private investigations. Only a very few indicated that they would cooperate with the Office for the Protection of the Constitution, while cooperation with the police scored slightly higher.

The research team believes this reluctance to turn to the authorities is explained by the fact that it isn't easy in Germany to determine which authority to contact for which type of espionage. Responsibility for the prevention and criminal prosecution of espionage in industry is divided between the federal intelligence service and their 16 counterparts at the state level (intelligence services of the federal states), the Federal Police Office (Bundeskriminalamt), the Federal Attorney General (Generalbundesanwalt) and the local public prosecutor's offices for economic crimes, depending on the offense. These authorities incidentally also often compete for the scarce number of specialists available in the field.

The researchers identified the legal distinction between economic and industrial espionage under German criminal law as the biggest stumbling block to criminal prosecution. This is also a relic from the Cold War period, when the state had to focus primarily on protecting its own economy against espionage from the Eastern Bloc. Currently, if a foreign intelligence service is behind an attempt at espionage, the secret service may be responsible in addition to the police. The Federal Attorney General is then generally responsible for criminal prosecution, assigning the case to either the federal or state police authorities for criminal investigations.

If there is no evidence of the involvement of foreign intelligence services, it is a case of industrial espionage, for which the local public prosecutor's office is responsible with the support of the local police force. Often, the perpetrators have vanished or covered their tracks, and the investigation must be terminated.

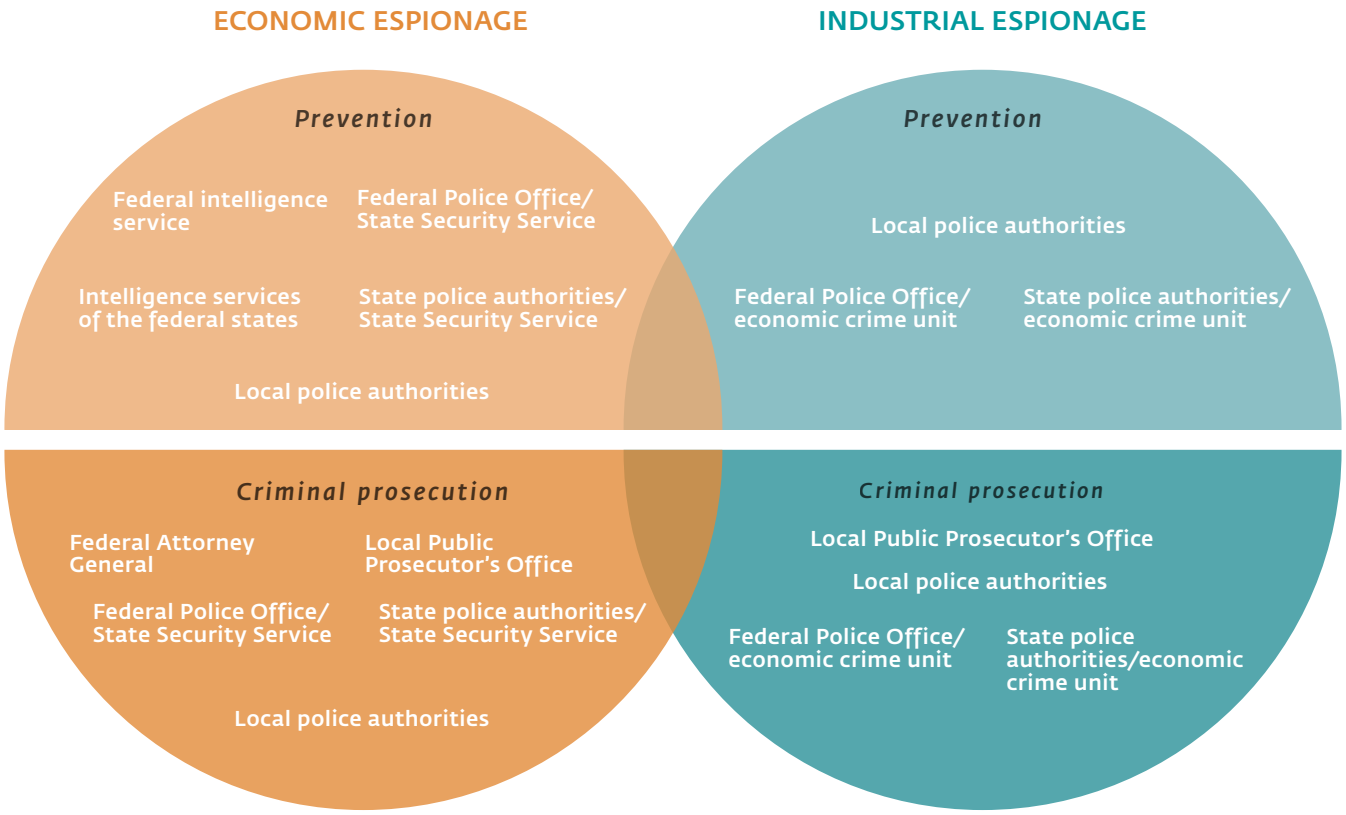
This is precisely what happened in a case that Susanne Knickmeier at the Max Planck Institute in Freiburg discovered in the investigation files. A large German company discovered that considerable amounts of data were being pulled from its datacenter. Instead of plugging the data leak, the employees responsible for the matter tried to set a trap for the cybercriminals. They allowed the data thieves to carry on with what they were doing while at the same time setting up a new system where they could secure important data. This led the spies to believe they could continue their activities undetected, and gave the authorities enough time to trace the data flows to another country.

THIN FILE DESPITE INTENSIVE INVESTIGATION

There, however, they were unable to intervene. The Federal Police Office was unable to identify the real culprits behind the attack, and the Federal Attorney General dropped the investigation. The local public prosecutor's office then took over the case and tried to determine exactly who was behind the attack – also in vain. The proceedings were eventually terminated.

"There is only a thin file," says Susanne Knickmeier, "but we know from the interviews with the investigators

Graphic: MPI for Foreign and International Criminal Law



Complex distinction: Depending on whether an intelligence service (economic espionage) or a competitor (industrial espionage) is spying, different authorities are responsible for prevention and criminal prosecution. The scientists recommend bundling these areas.

the great lengths they went to, despite ultimately failing to achieve a positive outcome." The case shows that the investigators' remit is restricted by national borders, which can only be resolved by international cooperation agreements. However, it also indicates that much time is often lost during investigations due to the different scopes of responsibility of the German authorities.

Following their interviews with companies and authorities, the research team from the Fraunhofer ISI and the Max Planck Institute in Freiburg believe that the legal distinction between economic and industrial espionage and the various areas of competence associated with it are outdated. In particular, they recommend a legislative reform that puts the focus on the companies that suffer damages. "In the era of the European single market, the national economy as a legal asset no longer exists," says Michael Kilchling, and the companies attacked aren't concerned about the political motives.

They want the leak to be plugged as quickly as possible, the perpetrator to be prosecuted, and to claim compensation, if possible. This is also reflected in the survey: the companies are willing to cooperate with the authorities if the cost-benefit ratio is reasonable and if they themselves believe there is a genuine chance of resolving the matter. Anonymity when notifying the authorities, on the other hand, was important to only a small number of the companies surveyed.

BREAKFAST MEETINGS ON ESPIONAGE PREVENTION

Kilchling and Bollhöfer see prevention as another key factor in protecting companies effectively, and suggest adopting approaches used in other European countries. Just how differently the issue is dealt with from one country to the next reveals a great deal about the relationship between government and business in the country concerned, says Michael Kilchling. In France, where the two sectors traditionally have close ties, the "Economic Warfare School of Paris" was established in 1997. At this postgraduate institution, 50 students spend ten months learning about the principles of economic warfare – that is, how to obtain strategic information about competitors – as well as about how to protect against espionage. Those who complete this postgraduate program often go on to work for security consulting firms or in the strategy departments of major corporations.

With regard to prevention, Germany could learn a great deal from the UK and Denmark. In the UK, espionage prevention is conducted primarily in informal groups and breakfast meetings to which companies gain access only once they have completed advanced training courses funded by the government. Business leaders, security experts and public prosecutors get to know one another here and establish

Graphic: MPI for Foreign and International Criminal Law

networks of trust. Trust is vitally important to successful cooperation in the event of an actual attack.

Denmark has also been successful with informal networks. Here, there is also an extensive informal flow of information between authorities and the business community, with SMEs also participating. The Danish government also requires all listed companies to document and assess their espionage risks and anti-espionage security measures.

As a result, general security standards have become prevalent in Denmark – and not just in listed companies. Numerous German companies would also voluntarily comply with these government requirements. More than half of the companies surveyed deemed a kind of state espionage certification to be "very good" or at least "good." They would also like to see more information events organized by the government and have personal designated contacts at government agencies.

But a comparison with other European countries also shows that German companies aren't spied on more often than firms in other countries. This is reassuring, in one respect, but also something of an affront in view of German industry's reputation for innovation worldwide. Companies that have not only a production facility abroad, but also research and development departments, are spied on more often. These branches, which are usually smaller and less secure than departments at the head office, are particularly vulnerable. "Conversely," as Esther Bollhöfer interprets it, "this also suggests that spies find it hard to penetrate headquarters in Germany."

An often-underestimated risk, as also revealed by the WiSKoS Research Group, is espionage at universities. Researchers and students, particularly at technical universities, often work with confidential data from industry, which frequently passes through the hands of dozens of research assistants. This makes protection quite difficult. Spies also try to steal research data via the internet.

RESEARCH INSTITUTES TARGETED BY SPIES

The Max Planck Institutes themselves are constantly being targeted by hackers. Rainer Gerling, an IT Security Officer at the Max Planck Society, can recall many ingenious attacks. The spies weren't only interested in discoveries in biomedicine or new developments in materials research. "Researchers who examine political and economic relationships and who possibly offer consulting in these fields are targets, too," reports Gerling. "When social scientists delve into the social structures of minorities in certain countries, there is always interest in obtaining this information."

The fact that science depends on international exchange complicates efforts to protect research data. Visiting scientists from all over the world spend several weeks or months at research institutes, work in their laboratories and take part in meetings, obtaining insight into technologies, methods and approaches that have not yet been published. "Many research institutes aren't even aware of the danger," points out Max Planck researcher Susanne Knickmeier. Visiting professors and students from abroad obviously can't be placed under general suspicion. On the other hand, the intelligence service also warns that countries such as China expect their students abroad to maintain contact with their embassies, enabling the intelligence service to enlist them at any time.

Universities could therefore be expected to show some degree of awareness. However, when the WiSKoS researchers were looking for universities willing to discuss the dangers of espionage, Elisa Wallwaey from the Max Planck Institute recalls this reply from one institution: "We would be pleased to discuss this matter with you. But what makes you think that we could be at risk?"

The WiSKoS team has since finished evaluating the results. In May, the researchers presented their findings at a closing conference in Brühl, near Bonn, under the aegis of the Federal Police Office. At the same time, they also published their own guidelines with practical recommendations for companies, police authorities and scientific organizations. After all, the project's stated goal is to apply the findings as directly as possible so as to make the work of the spies at least a bit more difficult. ◀

TO THE POINT

- **Industrial espionage, especially via electronic means, poses an increasing risk to small and medium-sized businesses in Germany; very few are equipped to deal with this.**
- **The legal distinction between economic and industrial espionage under German criminal law makes it more difficult to prosecute the perpetrators. It would be better if the authorities joined forces.**
- **To improve prevention, the researchers recommend government-defined security standards and better networking between authorities and industry before espionage occurs.**
- **Academic and research institutions should also protect themselves against espionage.**