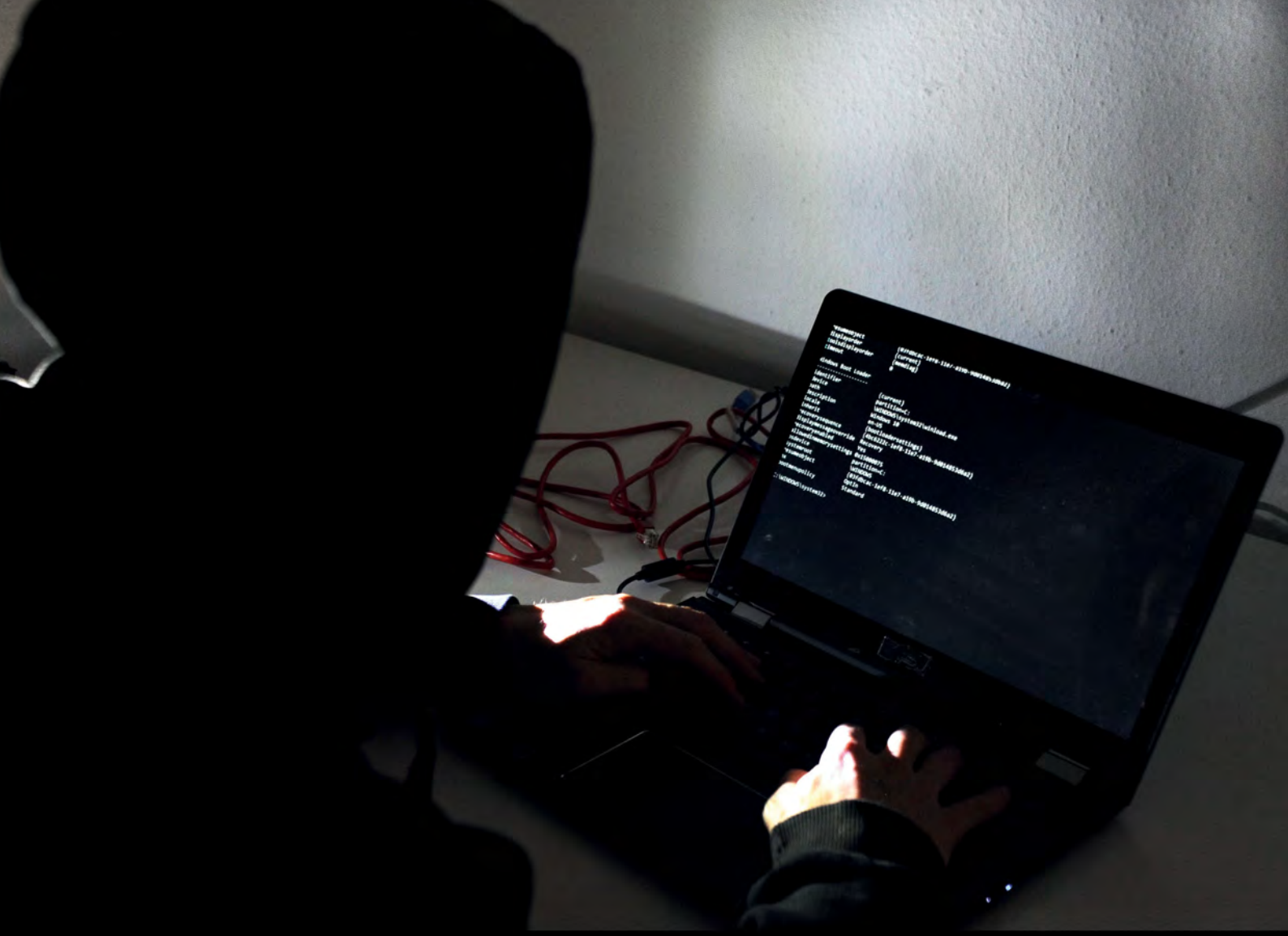


Strategien **gegen Spione**

Die Konkurrenz schläft nicht, sie spioniert. Gerade kleine und mittlere Unternehmen werden immer wieder Opfer krimineller Wettbewerber oder Zielscheibe ausländischer Geheimdienste. Doch die meisten Fälle bleiben im Dunkeln. **Michael Kilchling** und sein Team am **Max-Planck-Institut für ausländisches und internationales Strafrecht** in Freiburg möchten nun Licht in die Sache bringen. Gemeinsam mit Fraunhofer-Kollegen untersuchen sie das Ausmaß der Wirtschaftsspionage in Deutschland, wie sich Betriebe dagegen wehren und die Behörden Firmen besser unterstützen können.

Foto: dpa

TEXT **BENNO STIEBER**

Der chinesische Geschäftsführer kam als ein willkommener Partner zum Betonspezialisten Rieder ins bayrische Kolbermoor. Das Unternehmen für innovative Baustoffe, dessen Glasfaserbetonplatten das Stadion Soccer City in Johannesburg bei der Fußball-Weltmeisterschaft 2010 zu einem architektonischen Glanzstück machten, war froh, für einen millionenschweren Bauauftrag in China einen Partner vor Ort gefunden zu haben. Was in Kolbermoor niemand ahnte: dass es dem chinesischen Unternehmen in Wirklichkeit nur darum ging, Knowhow aus Deutschland abzuziehen, um den Auftrag allein zu übernehmen.

Beim Rundgang mit dem Geschäftsführer aus Fernost fiel Mitarbeitern von Rieder dann aber eine Minikamera am Gürtel ihres Gastes auf. Statt den Mann weiter in das Allerheiligste ihrer Firma blicken zu lassen, riefen sie die Polizei. Die Auswertung der Daten in der Gürtelkamera ergab später, dass das Material ausgereicht hätte, um die Hightech-Bauteile in China kopieren und nachbauen zu können. Der Schaden für das mittelständische Unternehmen wäre kaum zu beziffern gewesen.

Der Spionageversuch in der bayrischen Provinz ist im Vergleich zu anderen Fällen, die das Forschungsprojekt mit dem Akronym WiSKoS (Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa) untersucht, eher eine glückliche Ausnahme. Täter, Ziel und Motiv waren offensichtlich. Der Fall konnte schnell und erfolgreich abgeschlossen werden, ohne dass ein bleibender Schaden entstand. Der Spion wurde vom Münchner Landgericht zu einer Bewährungsstrafe verurteilt und musste Schadensersatz zahlen.

Attacke aus dem Netz: Die Täter sitzen oft weit weg in Russland, Indien oder der Karibik. Sie aufzuspüren, ist für deutsche Ermittler schwierig, oft scheitern sie an den Landesgrenzen.

Bei Wirtschaftsspionage fremder Geheimdienste und vor allem beim Ausspähen unter Konkurrenten ist so ein Ende eher die Ausnahme. Die Attacken kommen oft über das Glasfaserkabel. Die Opfer entdecken dann zu spät, dass wertvolle Daten von einem fernen Computer aus abgesaugt wurden. Nur selten lässt sich klären: Ging es um Sabotage oder tatsächlich darum, Knowhow zu stehlen? Sind die Hintermänner fremde Geheimdienste, oder war es doch der direkte Konkurrent, der Hacker beauftragt hat? In vielen Fällen kann noch nicht einmal der Schaden für das angegriffene Unternehmen genau beziffert werden. Vor allem bei Angriffen aus dem Cyberspace bleiben Hintermänner, Hintergründe und nicht selten sogar die eigentliche Absicht des Angriffs im Dunkeln.

So war es etwa bei einer Attacke gegen das Deutsche Zentrum für Luft- und Raumfahrt (DLR) im Jahr 2014, bei dem offenbar monatelang alle Betriebssysteme mit Trojanern infiltriert wurden. Zwar entdeckten die IT-Spezialisten vom Cyber-Abwehrzentrum des DLR im Code der Trojaner chinesische Schriftzeichen, doch das kann auch ein Ablenkungsmanöver eines anderen Geheimdienstes gewesen sein. Das Nachrichtenmagazin Der Spiegel berichtete damals, das DLR habe das Nationale Cyber-Abwehrzentrum in Bonn eingeschaltet, das auf solche Attacken spezialisiert ist. Doch die eigentlichen Drahtzieher wurden nie aufgespürt.

Spionage findet in Grauzonen statt, am erfolgreichsten ist sie, wenn sie unentdeckt bleibt. Das macht sie zum spannenden Stoff für Filme und Romane aus Zeiten des Kalten Krieges. Aber auch in der globalisierten und digitalen Welt von heute ist sie eine Erfolg versprechende Möglichkeit für konkurrierende Unternehmen oder für Regierungen von Industrie- und Schwellenländern, um sich mit Know-how aus fremden Forschungslabors im Wettbewerb zu halten. In Zeiten offener Märkte und internationaler Unternehmen haben sich die Bedingungen dafür allerdings enorm gewandelt – weitgehend unbeachtet von Politik und Wissenschaft.

FACHLITERATUR AUS ZEITEN DES KALTEN KRIEGES

Als sich das Forschungsteam des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg und des Fraunhofer-Instituts für System- und Innovationsforschung (ISI) in Karlsruhe unter der Leitung von Michael Kilchling und Esther Bollhöfer daranmachte, erst einmal das Ausmaß der heutigen Bedrohung für mittelständische Unternehmen abzuschätzen, waren die Forscher überrascht, wie wenige gesicherte aktuelle Erkenntnisse über Wirtschaftsspionage und Konkurrenzausspähung in Europa überhaupt vorliegen. „Wir haben festgestellt, dass es wirklich einen blinden Fleck gibt“, sagt Kilchling, wissenschaftlicher Referent am Max-Planck-Institut in Freiburg.

Und nicht nur die Agententhriller stammen aus den Zeiten des Kalten Krieges, sondern auch die meiste Fachliteratur über Wirtschaftsspionage. Die Erkenntnisse wurden also vor der Öffnung der Grenzen und dem Zusammenschluss im Europäischen Binnenmarkt gewonnen – einer Zeit, in der es noch eine nationale Wirtschaft gab, die vielfach als Schutzgut des Staates betrachtet wurde.

Diese Lücke soll das gemeinsame Forschungsprojekt WiSKoS schließen. Dabei lieferte das Max-Planck-Institut

Gefährliche Einblicke: Betriebsgeheimnisse sind oft Millionen wert. Besonders kleine und mittlere Unternehmen bräuchten mehr Unterstützung vom Staat, um sich zu schützen.

die juristische und kriminologische Fallanalyse und führte Expertengespräche im europäischen Ausland, während das Fraunhofer-Institut mit seinen guten Kontakten in die Wirtschaft die Befragung der Unternehmen beisteuerte. „Die Zusammenarbeit erwies sich als sehr glücklich“, sagt Michael Kilchling, „da wir einen guten Zugang zu den Behörden haben und das Fraunhofer-Institut bei Unternehmen einen hervorragenden Ruf genießt.“ Trotzdem war das Projekt für alle Beteiligten eine Herausforderung: Die Forscher verknüpften sehr unterschiedliche Herangehensweisen und Methoden, um den Status quo zu analysieren und daraus nicht nur grundlegende Erkenntnisse, sondern auch praktische Empfehlungen zu erarbeiten.

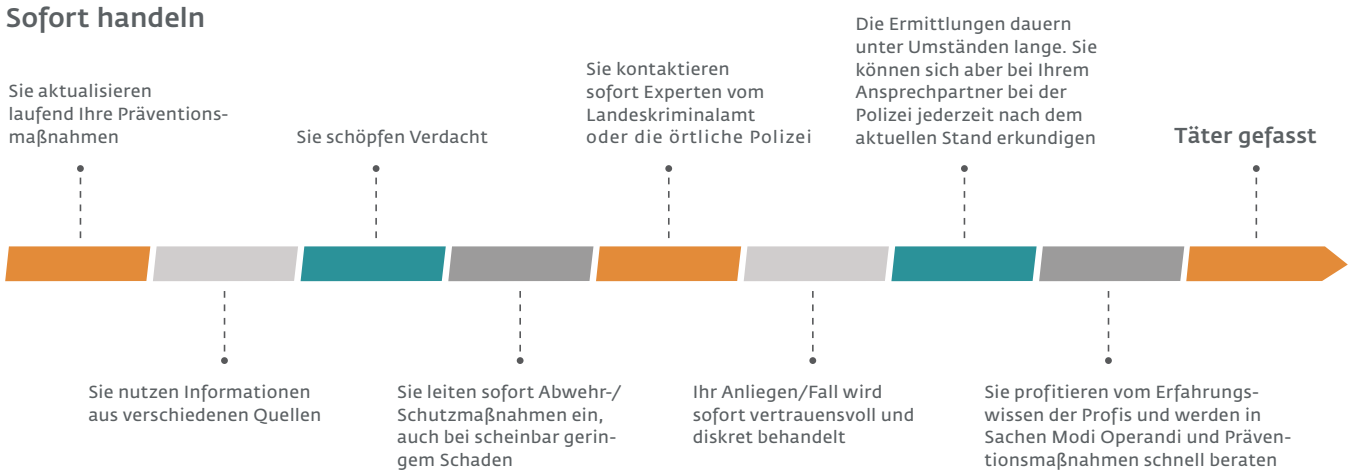
Das Team verschaffte sich zunächst mithilfe einer Umfrage einen möglichst umfassenden Überblick über die Bedrohungslage mittelständischer Unternehmen in Deutschland. Dann erfassten die Forscher die rechtliche Lage in Europa und den Umgang der Behörden mit der Thematik, um daraus Abwehrstrategien für Unternehmen und Behörden zu entwickeln.

Esther Bollhöfer betreut das Projekt als wissenschaftliche Mitarbeiterin am Fraunhofer ISI. Ihr Mitarbeiter, der sich um die Umfrage kümmerte, war überrascht, wie bereitwillig die Mittelständler über ihre Defizite in Sachen Sicherheit Auskunft gaben. Immerhin 612 von 8300 zufällig ausgewählten mittelständischen Unternehmen schickten den Fragebogen an die Forschergruppe zurück. Jedes fünfte Unternehmen gab zu, keine Strategie zur Abwehr von Spionage zu haben. Viele der Unternehmen würden sich mehr Hilfe vom Staat bei der Prävention wünschen. Nur zehn Firmen lehnten jede Hilfe vom Staat ab.

Obwohl die Befragten anonym blieben, waren nur wenige Unternehmen bereit zu berichten, wie sie mit Verdachtsfällen im eigenen Unternehmen umgehen. „Das kann bedeuten, dass sie darüber nicht sprechen möchten,

Freiburger Team: Am Max-Planck-Institut für ausländisches und internationales Strafrecht arbeiten Elisa Wallwaey, Michael Kilchling und Susanne Knickmeier (von links) am Projekt WiSKoS.

Fotos: CCO (oben), Markus Herb (unten)



Konkrete Ratschläge: Die Wissenschaftler empfehlen Unternehmen, rechtzeitig eine Strategie gegen Ausspähung zu entwickeln. Dazu gehören geeignete Vorkehrungen und ein Plan, wie Mitarbeiter und Leitung im Ernstfall reagieren sollten.

aber auch, dass sie keine Strategie dafür haben“, sagt Esther Bollhöfer. Von denen, die antworteten, greifen die meisten zu „eigenen Maßnahmen“, also privaten Ermittlungen. Deutlich abgeschlagen lag die Zusammenarbeit mit dem Verfassungsschutz, immerhin etwas besser wurde die Kooperation mit der Polizei eingestuft.

Diese Zurückhaltung gegenüber den Behörden erklärt sich das Forschungsteam auch damit, dass es in Deutschland nicht leicht zu durchschauen ist, wer für welchen Spionagefall der richtige Ansprechpartner ist. Die Zuständigkeit für Prävention und Strafverfolgung von Spionage in Wirtschaftsunternehmen splittet sich hierzulande je nach Delikt zwischen dem Bundesamt für Verfassungsschutz, 16 Landesverfassungsschutzämtern und ebenso vielen Landespolizeibehörden und sogenannten Schwerpunktstaatsanwaltschaften für Wirtschaftsdelikte auf. Behörden, die übrigens auch oft um die raren Fachleute konkurrieren.

Als großen Hemmschuh bei der Strafverfolgung haben die Wissenschaftler die rechtliche Trennung zwischen Wirtschaftsspionage und Konkurrenzausspähung im deutschen Strafrecht ausgemacht. Auch das ein Relikt aus der Zeit des Kalten Krieges, als der Staat die eigene Wirtschaft vor allem gegen Ausspähung aus dem Ostblock schützen musste. Bis heute gilt: Steckt hinter einem Ausspähversuch ein fremder Geheimdienst, kann neben der Polizei auch der Verfassungsschutz zuständig sein. Die strafrechtliche Verfolgung liegt dann grundsätzlich bei der Bundesanwaltschaft, die entweder das Bundes- oder ein Landeskriminalamt mit den Ermittlungen beauftragt.

Lässt sich die Beteiligung ausländischer Nachrichtendienste nicht beweisen, handelt es sich um Konkurrenzausspähung, wofür die örtliche Staatsanwaltschaft mit Unterstützung der lokalen Polizei zuständig ist. Oftmals sind die Täter bereits verschwunden und ihre Spuren verwischt, sodass die Ermittlungsverfahren eingestellt werden müssen.

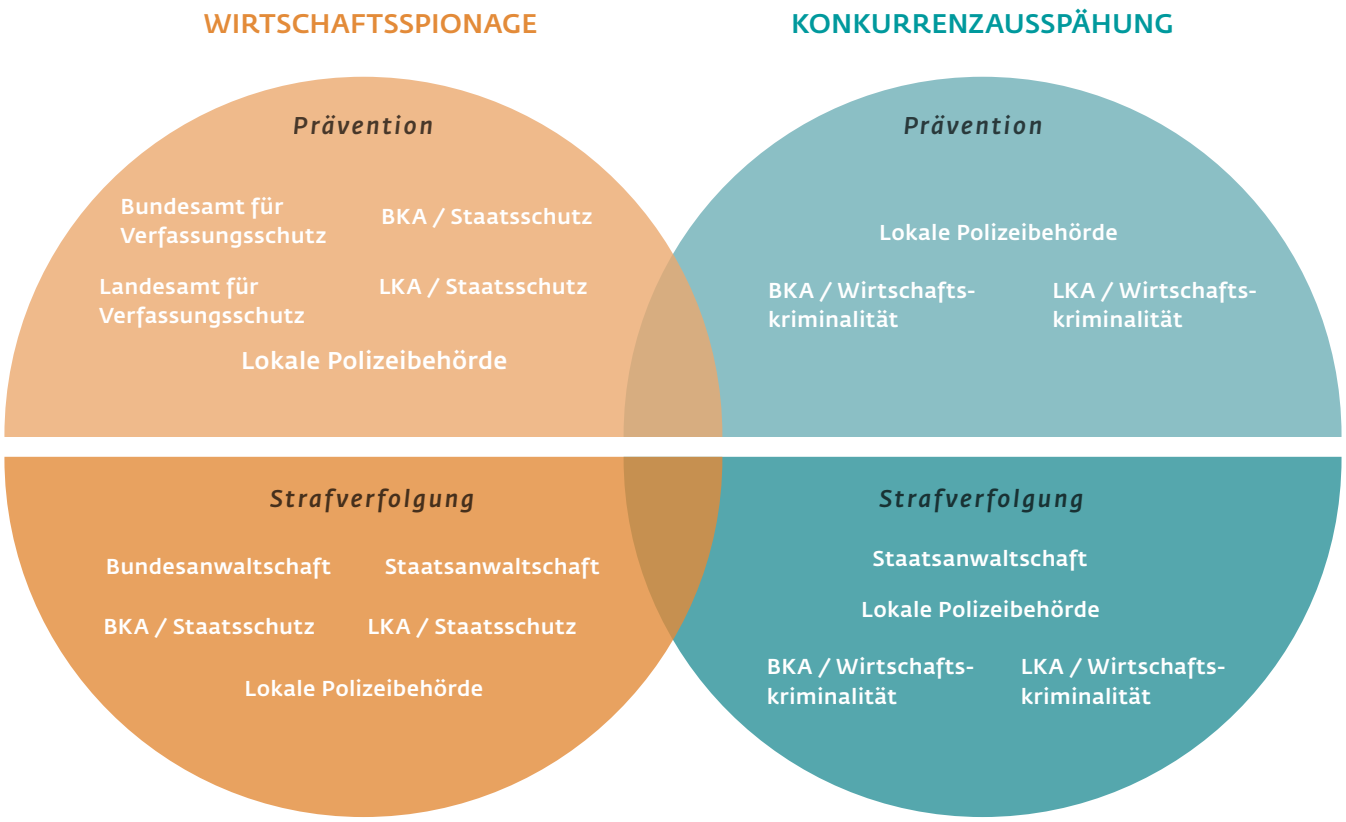
So geschehen in einem Fall, den Susanne Knickmeier vom Freiburger Max-Planck-Institut in Ermittlungsakten gefunden hat. Ein großes deutsches Unternehmen stellte fest, dass beachtliche Datenmengen aus seinem Rechenzentrum abgezogen wurden. Statt das Datenleck zu schließen, versuchten die zuständigen Mitarbeiter, den Cyberspionen eine Falle zu stellen. Sie ließen die Datenräuber weiter gewähren, bauten aber parallel ein neues System auf, in dem sie wichtige Daten in Sicherheit bringen konnten. So ließen sie die Spione in dem Glauben, weiter unentdeckt arbeiten zu können. Die Behörden hatten dadurch genügend Zeit, die Datenströme ins Ausland zu verfolgen.

DÜNNE AKTE TROTZ INTENSIVER ERMITTLUNGEN

Zugreifen konnten sie dort nicht. Das Landeskriminalamt machte in seiner Untersuchung die wahren Hintermänner des Angriffs nicht ausfindig, die Bundesanwaltschaft brach die Ermittlungen ab. Nun übernahm die örtliche Staatsanwaltschaft den Fall und versuchte, konkrete Personen hinter dem Angriff zu identifizieren – ebenfalls ohne Erfolg. Das Verfahren musste schließlich eingestellt werden.

„Das ist dann nur eine dünne Akte“, sagt Susanne Knickmeier, „doch durch die Interviews mit den Ermittlern wissen wir, wie aufwendig die Ermittlungen waren, auch wenn sie am Ende ins Nichts führten.“ Der Fall zeigt, dass die Möglichkeiten der Ermittler an Landesgrenzen scheitern, was nur durch internationale Kooperationsabkommen zu

Grafik: MPI für ausländisches und internationales Strafrecht



Schwierige Trennung: Je nachdem, ob ein Geheimdienst spioniert (Wirtschaftsspionage) oder ein konkurrierendes Unternehmen (Konkurrenzausspähung), sind unterschiedliche Behörden für Prävention und Strafverfolgung zuständig. Die Wissenschaftler empfehlen, die Kompetenzen zu bündeln.

lösen wäre. Er zeigt aber auch, dass durch die unterschiedlichen Zuständigkeiten der deutschen Behörden oft viel Zeit verloren geht, um Hintergründe zu ermitteln.

Die juristische Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung und die damit verbundenen unterschiedlichen Zuständigkeiten halten die Forscher vom Fraunhofer ISI und vom Freiburger Max-Planck-Institut nach ihren Gesprächen mit Unternehmen und Behörden für überholt. Konkret empfehlen sie eine Gesetzesreform, welche die geschädigten Unternehmen in den Mittelpunkt stellt. „Das Rechtsgut nationale Wirtschaft gibt es in Zeiten des europäischen Binnenmarkts nicht mehr“, sagt Michael Kilchling, und den angegriffenen Unternehmen seien die politischen Hintergründe egal.

Sie wünschen sich, dass das Leck schnell geschlossen wird, der Täter ermittelt und sie – wenn möglich – Schadensersatz geltend machen können. Das zeigt auch die Befragung: Die Unternehmen sind zur Zusammenarbeit mit Behörden bereit, wenn Aufwand und Ertrag in sinnvoller Relation stehen und sie selbst eine Chance zur Aufklärung sehen. Die Anonymität gegenüber Behörden bei der Anzeige ist dagegen nur einem geringen Teil der befragten Unternehmen wichtig.

FRÜHSTÜCKSRUNDEN ZUR SPIONAGEPRÄVENTION

Einen weiteren wesentlichen Ansatz, um Firmen wirkungsvoll zu schützen, sehen Kilchling und Bollhöfer in der Prävention. Da könne man sich auch an anderen europäischen Nationen orientieren. Wie unterschiedlich das Thema von Land zu Land behandelt wird, sage viel über das Verhältnis von Staat und Wirtschaft im jeweiligen Land aus, so Michael Kilchling. In Frankreich etwa mit seiner traditionell engen Verbindung zwischen beiden Bereichen gibt es seit 1997 eine „Ecole de Guerre Economique“. In der Hochschule für Graduierte lernen 50 Studenten in zehn Monaten die Regeln für den – wörtlich übersetzt – „Wirtschaftskrieg“, also wie man strategische Informationen über Konkurrenten gewinnt; aber auch, wie man Ausspähversuche abwehrt. Die Absolventen dieses Aufbaustudiengangs arbeiten später oft in Sicherheitsberatungsfirmen oder Strategieabteilungen großer Unternehmen.

Bei der Prävention könnte Deutschland sowohl von den Briten als auch von den Dänen einiges lernen. In Großbritannien findet Spionageprävention vor allem in informellen Kreisen und Frühstücksrunden statt, zu denen Unternehmer erst Zugang bekommen, wenn sie gewisse Fortbildungen absolviert haben, die staatlich gefördert werden. Dort lernen sich Unternehmer, Sicherheitsexperten und Strafverfolger persönlich kennen und knüpfen vertraute Kontakte. Denn Vertrauen ist eine wichtige Grundlage, um im Ernstfall gut zusammenzuarbeiten.

Grafik: MPI für ausländisches und internationales Strafrecht

Gute Erfahrung mit informellen Netzwerken hat auch Dänemark gemacht. Dort gibt es ebenfalls einen intensiven informellen Informationsaustausch zwischen Behörden und Wirtschaft, an dem auch Mittelständler beteiligt sind. Darüber hinaus verlangt der dänische Staat von allen börsennotierten Unternehmen ein Risiko-Assessment, also eine Bestandsaufnahme und die Bewertung von Risiken und Sicherheitsmaßnahmen zur Abwehr von Spionage.

Auf diese Weise haben sich in Dänemark nicht nur in börsennotierten Unternehmen allgemeine Sicherheitsstandards durchgesetzt. Diesen staatlichen Vorgaben würden sich auch viele deutsche Unternehmen gern unterwerfen. Mehr als die Hälfte der befragten Unternehmer fänden eine Art staatlichen Spionage-TÜV „sehr gut“ oder wenigstens „gut“. Außerdem würden sie sich mehr Informationsveranstaltungen von staatlicher Seite und persönliche Ansprechpartner bei den Behörden wünschen.

Der europäische Vergleich zeigt aber auch: Deutsche Unternehmen werden nicht häufiger ausspioniert als Unternehmen anderer Länder. Eine Erkenntnis, die einerseits beruhigend ist, aber angesichts des besonders innovativen Rufs deutscher Unternehmen in der Welt auch ein wenig kränkend sein könnte. Häufiger ausgespäht werden Firmen, die nicht nur eine Produktionsstätte, sondern auch Abteilungen für Forschung und Entwicklung im Ausland haben. Diese Außenstellen, meist kleiner und schlechter gesichert als Abteilungen im Mutterhaus, erweisen sich offensichtlich als besonders verwundbar. „Das heißt umgekehrt, dass die Stammsitze in Deutschland offenbar gewisse Hürden für die Spione bedeuten“, interpretiert Esther Bollhöfer.

Eine oft unterschätzte Gefahr, auch das zeigt die Analyse der Forschungsgruppe WiSKoS, ist Spionage an Hochschulen. Wissenschaftler und Studenten gerade an technischen Hochschulen arbeiten häufig mit vertraulichen Daten aus der Industrie, die oft durch die Hände Dutzender wissenschaftlicher Hilfskräfte gehen. Schutz ist da ziemlich schwierig. Und auch über das Internet versuchen Spione, wissenschaftliche Daten zu stehlen.

FORSCHUNGSINSTITUTE IM VISIER VON AGENTEN

Institute der Max-Planck-Gesellschaft sind selbst immer wieder das Ziel von Hackerangriffen. Rainer Gerling, IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, kann von vielen ausgefeilten Attacken berichten. Dabei hätten es Spitzel nicht nur auf biomedizinische Erkenntnisse oder neue Entwicklungen in der Materialforschung abgesehen. „Forscher, die politische und ökonomische Zusammenhänge untersuchen und womöglich in diesem Umfeld auch Beratungen machen, stehen genauso im Fokus“, berichtet Gerling. „Wenn sich Sozialwissenschaftler etwa mit gesellschaftlichen Strukturen von Minderheiten in bestimmten Ländern befassen, dann gibt es Interesse daran, diese Informationen zu bekommen.“

Bei den Bemühungen, Forschungsdaten zu schützen, kommt erschwerend hinzu, dass die Wissenschaft vom internationalen Austausch lebt. Gastwissenschaftler aus aller Welt kommen für einige Wochen oder Monate in Forschungsinstitute, arbeiten mit in den Labors, nehmen an Besprechungen teil und bekommen auf diese Weise Einblick in Technologien, Methoden und Ansätze, die noch nicht publiziert wurden. „Viele wissenschaftliche Institute sind sich dieser Gefahr gar nicht bewusst“, sagt Max-Planck-Forscherin Susanne Knickmeier. Selbstverständlich dürfen Gastdozenten und Studenten aus dem Ausland nicht unter Generalverdacht gestellt werden. Andererseits weist auch der Verfassungsschutz darauf hin, dass Länder wie China von ihren Auslandsstudenten erwarten, Kontakt zu den jeweiligen Botschaften zu halten, sodass der jeweilige Geheimdienst sie jederzeit anwerben kann.

Ein wenig Sensibilität an den Hochschulen wäre also zu erwarten. Doch als die WiSKoS-Forscher Universitäten anschrieben, um mit ihnen über die Gefahren der Ausspähung zu sprechen, bekamen sie, wie sich Elisa Wallwaey vom Max-Planck-Institut erinnert, von einem Institut als Antwort: „Wir sprechen gern mit Ihnen. Aber wie kommen Sie darauf, dass wir gefährdet sein könnten?“

Die Auswertung der Ergebnisse hat das WiSKoS-Team inzwischen fast beendet. Im Mai präsentieren die Forscher die Resultate auf einer Abschlusskonferenz in Brühl bei Bonn unter Schirmherrschaft des Bundeskriminalamts. Zum selben Zeitpunkt publizieren sie jeweils eigene Leitfäden mit praktischen Empfehlungen für Unternehmen, Polizeibehörden und Wissenschaftsorganisationen. Denn erklärtes Ziel des Projekts ist es, die Erkenntnisse möglichst direkt in die Anwendung zu bringen und so den Spionen die Arbeit zumindest ein wenig schwerer zu machen. ◀

AUF DEN PUNKT GEBRACHT

- **Das Ausspähen von Firmengeheimnissen, besonders auf elektronischem Wege, stellt eine zunehmende Gefahr für kleinere und mittlere Unternehmen in Deutschland dar; die wenigsten sind dagegen gewappnet.**
- **Die rechtliche Trennung zwischen Wirtschaftsspionage und Konkurrenzausspähung im deutschen Strafrecht erschwert die Verfolgung der Täter. Besser wäre es, wenn die Behörden ihre Kräfte bündelten.**
- **Zur besseren Prävention empfehlen Wissenschaftler staatlich festgelegte Sicherheitsstandards und eine bessere Vernetzung von Behörden und Unternehmen, schon bevor ein Spionagefall auftritt.**
- **Auch wissenschaftliche Einrichtungen sollten sich gegen Ausspähung schützen.**