

Angriff aus dem Reich der Mitte

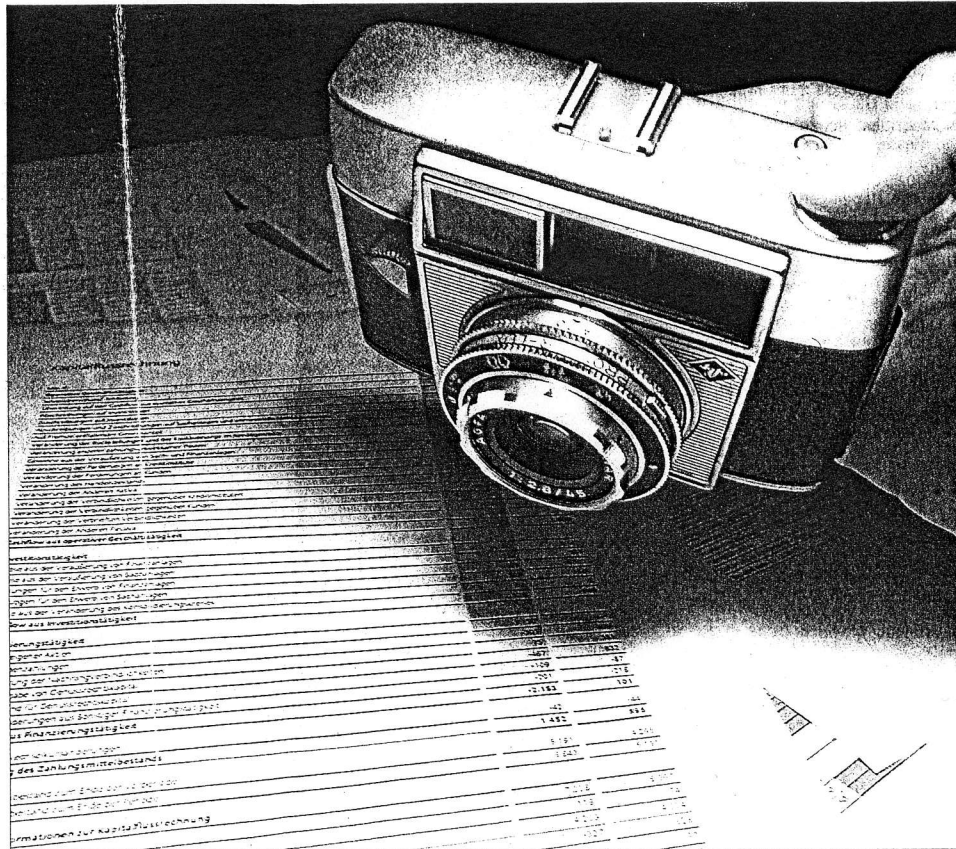
Spionage-Experte Udo Schauff vom Bundesverfassungsschutz gibt bei einem Vortrag Einblicke in seine Arbeit

Von Christoph Lüttgen

BAD NEUENAH. Innovation und Forschung auf Spitzenniveau haben Deutschland den Status einer Wirtschaftsmacht und den Ruf des Exportweltmeisters eingebracht. Während sich die wirtschaftliche Leistungskraft konkurrierender Länder oft auf ungeheure Rohstoffvorkommen gründet, kann die Bundesrepublik seit Generationen auf ihren Wissensvorsprung bauen. Doch das Know-how der deutschen Wirtschaft weckt international Begehrlichkeiten und macht Deutschland auch fast 20 Jahre nach Ende des „Kalten Krieges“ zum Tummelplatz für ausländische Geheimdienste.

„Die Wirtschaftsspionage ist eine der größten Gefahren, die Deutschland in Zukunft zu erwarten hat“, sagt Udo Schauff, Mitarbeiter der Abteilung Spionageabwehr beim Kölner Bundesamt für Verfassungsschutz, das für die Beobachtung und Analyse von Operationen fremder Nachrichtendienste zuständig ist. „Staaten mit Technologierückstand haben es eher auf Produkte abgesehen, während hoch industrialisierte Länder in erster Linie an wirtschaftlichen oder wirtschaftspolitischen Strategien interessiert sind“, erklärt Schauff in einem Vortrag, zu dem ihn die Gesellschaft für Wehr- und Sicherheitstechnik nach Bad Neuenahr eingeladen hatte, und zu dem 100 interessierte Bürger gekommen waren. Durch den Datenklau entstehen der deutschen Wirtschaft jährlich Schäden in Milliardenhöhe. Längst bedrohe Wirtschaftsspionage den Wissensvorsprung deutscher Unternehmen.

Während das Bundesamt keine Erkenntnisse darüber haben will, dass etwa westliche Nachrichtendienste systematische Wirtschaftsspionage gegen die Bundesrepublik betreiben, hat es China



Die Zeiten sind vorbei: Früher mussten die Agenten die geheimen Dokumente noch abfotografieren, heute erlangt das Ausspähen auf dem elektronischen Sektor enorme Bedeutung. FOTO: MARTIN GAUSMANN

und Russland als „Hauptgegner“ ausgemacht. „Mit etwa 800 000 hauptamtlichen Mitarbeitern im MSS, dem für die zivile Aufklärung zuständigen Staatssicherheitsdienst, unterhält China das größte informelle Spionagenetz der Welt“, so Schauff, dessen Vorträge der Sensibilisierung deutscher Unternehmen und Forschungseinrichtungen dienen sollen.

Immerhin 500 000 Spitzel umfasse das Kontingent der drei russischen Nachrichtendienste. Alleine

15 000 hauptamtliche Mitarbeiter stünden im Dienst der aus dem KGB hervorgegangenen Auslandsaufklärung SWR. Dabei habe der russische Geheimdienst insbesondere Deutschland fest ins Visier genommen. „Während die russischen Dienste noch primär mit klassischen Agenten arbeiten, sind die Chinesen hauptsächlich auf dem elektronischen Sektor aktiv“, erklärte Schauff. So schätzen die Verfassungsschützer, dass deutsche Firmen und Behörden im

Schnitt etwa alle ein bis zwei Tage das Ziel von Hacker-Angriffen aus dem Reich der Mitte sind. Als Stützpunkte ihrer Agenten nutzen beide Länder ihre jeweiligen Botschaften. Von dort aus seien die als Diplomaten getarnten Spione bemüht, Kontakte zu Bundesbürgern, die wichtige Funktionen in Staat, Wirtschaft und Gesellschaft innehaben, zu knüpfen, mit dem Ziel sie als Informanten, Tipgeber oder gar Agenten zu gewinnen. In dem Zusammenhang verwies

Schauff auf den Fall eines ehemaligen Ingenieurs des Hubschrauber-Herstellers Eurocopter, zu dem ein russischer Geheimdienstoffizier ein fast freundschaftliches Verhältnis aufgebaut hatte, bevor er ihn zur Herausgabe geheimer Informationen über einen von Eurocopter hergestellten Kampfhubschrauber hatte bewegen können. Erst im Juni ist der 44-Jährige vom Oberlandesgericht München wegen Spionage zu einer Bewährungsstrafe verurteilt worden.

Im Gegensatz zu den russischen Diensten sei das Anwerben von Ausländern bei den Chinesen eher die Ausnahme. „In der Regel wendet man sich an im Ausland lebende Landsleute. Nach unseren Erkenntnissen werden zahlreiche Studenten, Praktikanten und Wissenschaftler regelmäßig eingelenkt und abgeschöpft“, berichtet Udo Schauff.

Statt „traditioneller Ausspähungsversuche“ stellten mittlerweile jedoch die Möglichkeiten der modernen Informations- und Kommunikationstechnik die größere Gefahr dar. Über sie ließen sich in Bruchteilen von Sekunden riesige Datenmengen transportieren – und das bei sehr geringem Risiko, entdeckt zu werden. Neben E-Mails, in deren Anhängen Spähprogramme lauerten, seien drahtlose W-Lan-Verbindungen beliebt, um sich in die Netzwerke von Unternehmen einzuschleichen.

Kurios: Agenten greifen dabei nicht selten auf handelsübliche W-Lan-Finder zurück, die äußerlich einer harmlosen Armbanduhr ähnelten und für knapp 15 Euro in zahlreichen Internetshops zu erwerben sind. Eine fast schon unterschämte simple Methode bestünde im Anbringen so genannter Keylogger. Sie werden unbemerkt an der Rückseite von Computern eingesteckt und zeichnen sämtliche relevanten Daten auf. Sind die Angreifer erst einmal in ihrem Besitz, haben sie leichtes Spiel.