

Ladenburger Thesen zum Wirtschaftsschutz

Die folgenden Thesen beschreiben eine Forschungsagenda, die mit Unterstützung der Daimler und Benz Stiftung im Format der Ladenburger Diskurse vom 26.-27. Juni 2025 entwickelt wurde. Vertreterinnen und Vertreter aus Wirtschaft, Sicherheitsverwaltung (Bundes- und Landesebene), Justiz und Wissenschaft erhielten Gelegenheit, ihre Perspektiven zur Bedrohung durch „Wirtschaftsspionage und Konkurrenzausspähung“ einzubringen. Die Ladenburger Thesen dokumentieren die Ergebnisse aus Impulsreferaten, Diskussionen und verschiedenen Arbeitsgruppen. Dabei schließen sie Widersprüche nicht aus und nehmen auch keine Antworten vorweg. Vielmehr bezeichnen sie dringende Forschungsdesiderata. Allein gesicherte Ergebnisse zu den aufgeworfenen Fragen und Problemen können eine belastbare Grundlage für evidenzbasierte Wirtschaftsschutzpolitik bilden.

I. Problemdimension

Phänomenbezogen:

1. Wirtschaftsspionage und Konkurrenzausspähung stellen lediglich Teilaspekte einer umfassenden Bedrohungslage für die deutsche Wirtschaft und Wissenschaft dar, die sich nur schwer von verwandten Bedrohungen, beispielsweise durch Desinformation und Sabotage, abgrenzen lassen.
2. Auf Opferseite besteht eine hohe Sensibilität mit Blick auf mögliche Reputations- und Kontrollverluste im Falle eines staatlichen Eingreifens bzw. des öffentliche Bekanntwerdens von Angriffen. Insofern fehlt es teilweise an dem nötigen Vertrauen in behördliche Problemlösungskompetenzen. Dies gilt weniger gegenüber den Nachrichtendiensten, sondern eher im Zusammenhang mit Kontakten gegenüber den Strafverfolgungsbehörden, die in Deutschland grundsätzlich an das Legalitätsprinzip gebunden, also bei Bestehen eines Anfangsverdachts zur Einleitung und Durchführung eines Strafverfahrens verpflichtet sind. Infolgedessen fehlt es gerade bei den Strafverfolgungsbehörden mangels Fallaufkommens gelegentlich an einschlägiger Expertise, die an weitere Opfer präventiv oder im Rahmen der repressiven Fallbearbeitung weitergegeben werden könnte.
3. Speziell auf Unternehmensseite führt dies zu einem zurückhaltenden Anzeigeverhalten gegenüber staatlichen Stellen und einem vorrangigen Rückgriff auf Dienstleistungen privater Sicherheitsanbieter. Folgen sind insbesondere ein hohes Dunkelfeld in Bezug auf das tatsächliche Fallaufkommen sowie Schwierigkeiten bei der Bezifferung des tatsächlichen wirtschaftlichen Schadens.

Administrativ:

4. Angesichts der zahlreichen, sich häufig überlappenden Zuständigkeiten der deutschen Sicherheitsbehörden im Bereich des Wirtschaftsschutzes besitzt eine ausreichende Koordinierung besondere Bedeutung. Infolgedessen ist für die potenziellen Opfer angesichts der unübersichtlichen Rechtslage ein einheitlicher Ansprechpartner unabdingbar, der zeitnah Expertise zur Bewältigung von Krisensituationen vermittelt.
5. Mit Blick auf das Fehlen einer die behördlichen Zuständigkeitsgrenzen überwindenden Expertise sollte ein gemeinsamer Wissensbestand zu Bedrohungsarten und Vorgehen der Akteure in Gestalt eines bundesweiten, nach Möglichkeit automatisierten „Lagebildes Wirtschaftsschutz“ geschaffen werden, damit sich die Unternehmen zumindest auf erwartbare Szenarien vorbereiten können.
6. Erforderlich ist mit Blick auf das hohe Dunkelfeld, durch das die tatsächlichen Fallzahlen nicht einmal ansatzweise wiedergegeben werden, eine deutlichere inhaltliche Schwerpunktsetzung der deutschen Sicherheitsbehörden im Bereich von Wirtschaftsspionage und Konkurrenzausspähung, die sich auch in einer besseren Personal- und Sachmittelausstattung niederschlagen sollte.

Wirtschaftlich:

7. Die zahlreichen bereits vorhandenen Austausch- und Kooperationsformate zwischen Wirtschaft und Verwaltung für den Wirtschaftsschutz bleiben regelmäßig zu unverbindlich und führen nicht zu konkreten Reformvorschlägen. Zudem fehlt es an einer ausreichenden Einbeziehung der Wissenschaft und einer Entwicklung einheitlicher wirtschaftspolitischer Strategien mit klaren Verantwortlichkeiten, Umsetzungszeitlinien und hinterlegten Ressourcen zur Umsetzung.
8. Auf operativer Ebene existieren keine ausreichenden, gesetzlich abgesicherten Kooperationsmodi, um bei Verdachtsfällen der Gefahr eines Kontrollverlustes für die Unternehmen wirksam zu begegnen.
9. Zumindest jenseits des Bereichs von Cybersicherheit mangelt es an einer ausreichenden behördlichen Standardsetzung für den Unternehmensschutz („Security by Design“). Ob dies durch freiwillige Standards von Unternehmen für Unternehmen („DIN SPEC Corporate Security“) kompensiert werden kann, erscheint fraglich.
10. Zum Schutz vor Ausspähung bedürfen deutsche Wirtschaftsunternehmen einer stärkeren staatlichen Unterstützung im Bereich des personellen Geheimschutzes, speziell im Zusammenhang von Sicherheits- und Zuverlässigkeitsüberprüfungen von Mitarbeitenden in besonders sensiblen Bereichen.

Rechtlich:

11. Der „Wirtschaftsschutz“ stellt sich bislang nicht als klares juristisches Konzept dar. Er muss daher als schutzwürdiges Rechtsgut näher ausdifferenziert und verfassungsrechtlich hinterlegt werden.
12. Das unklare Verhältnis zwischen privater (z.B. DIN oder ISO) und staatlicher Rechtssetzung bedarf dringend einer näheren Präzisierung.
13. Die bestehenden Regelungen zur Datenübermittlung in den deutschen Sicherheitsgesetzen sind unter Einbeziehung der zwingenden Vorgaben des Bundesverfassungsgerichts dringend reformbedürftig. Dies betrifft sowohl den Austausch von personenbezogenen Daten zwischen den verschiedenen Sicherheitsbehörden als auch die Datenübermittlungen von den Behörden an die Unternehmen als Private.
14. Es fehlt an einem zeitgemäßen Wirtschaftsschutzstrafrecht. Insbesondere die deutschen Geheimchutz- und Spionagedelikte sind deshalb an die Herausforderungen durch Wirtschaftsspionage und Konkurrenzausspähung anzupassen. Entsprechendes gilt für die zur Durchführung effektiver Ermittlungen erforderlichen Befugnisse nach der Strafprozessordnung.
15. Der gesetzliche Auftrag der Verfassungsschutzbehörden und die nachrichtendienstlichen Befugnisse müssen an die Herausforderungen von Wirtschaftsspionage und Konkurrenzausspähung angepasst werden.
16. Das in sich stark zerfaserte Sicherheits- bzw. Zuverlässigkeitsüberprüfungsrecht muss in Bezug auf Beschäftigte in der Privatwirtschaft flexibilisiert werden.

Wissenschaftlich:

17. Wissenschaftliche Expertise im Bereich des Wirtschaftsschutzes wird kaum angeboten und wenig nachgefragt. Insofern fehlen hier Strukturelemente eines nachhaltigen Diskurses, beispielsweise in Gestalt von Fachtagungen und Publikationen.
18. Phänomenologische Forschung zur tatsächlichen Bedrohungslage durch Wirtschaftsspionage und Konkurrenzausspähung ist praktisch nicht existent.
19. Einschlägige Forschungsförderungsangebote sind bislang nicht vorhanden und/oder werden nicht eingefordert oder koordiniert (z.B. BMBF- oder DFG-Förderlinien).
20. Insgesamt ist der Bereich des Wirtschaftsschutzes sowohl in empirischer Hinsicht als auch mit Blick auf die erforderlichen rechtlichen Rahmenbedingungen nicht ausreichend erforscht, so dass es aktuell an einer fundierten wissenschaftlichen Grundlage für eine nationale Wirtschaftsschutzstrategie fehlt.

II. Strategiedimension

21. Es besteht ein dringendes Bedürfnis nach einer Wirtschaftsschutzstrategie „aus einem Guss“, die an anderen nationale Sicherheitsstrategien, -pläne und -programme anschließt und mit ausreichenden Ressourcen (Personal- und Sachmitteln) hinterlegt ist.
22. In diesem Kontext verspricht allein eine evidenzbasierte Strategie nachhaltigen Erfolg. Insoweit fehlt es aber an einem zentralen Akteur, der den erforderlichen interdisziplinären fachlichen Diskurs initiieren kann.
23. Eine solche Strategie muss Informationen und Impulse aus dem Ausland aufnehmen und sich in das Mehrebenensystem europäischer Wirtschafts- und Sicherheitspolitik einordnen lassen.
24. Thematisch einschlägige Forschungsförderungsprogramme sind in Abstimmung von Wirtschaft, Wissenschaft und Politik zu entwickeln.
25. Angesichts der immanenten Bedrohung für die deutsche Wirtschaft und Wissenschaft sind Zeitlinien für die kurz-, mittel- und langfristige Umsetzung zu identifizieren.

III. Umsetzungsdimension

26. Technisch-organisatorischen Maßnahmen der Wirtschaftsunternehmen im Bereich der Prävention entscheidende Bedeutung zu. Sie sind durch Erfahrungsaustausch und weitere Maßnahmen zu optimieren.
27. Es sind rechtliche Formate für eine effektive und verfassungskonforme Kooperation von betroffenen Wirtschaftsunternehmen und Sicherheitsbehörden im Verdachtsfall zu entwickeln. Vergleichbar dem Gemeinsamen Terrorismus-Abwehrzentrum (GTAZ) oder anderen Fusion Centern könnte etwa ein Gemeinsames Zentrum Wirtschaftsschutz (GZW) eingerichtet werden. Dieses sollte für Wirtschaft und Wissenschaft im Idealfall rund um die Uhr digitale und analoge Meldewege sowie Erste Hilfe im Verdachtsfall i.S. eines „First Response Systems“ anbieten, konkrete Lageerkennnisse und Warnmeldungen steuern sowie allgemeine Handlungsempfehlungen für den Umgang mit Verdachtsfällen erstellen.
28. Im Bereich des Wirtschaftsschutzes sollten im Rahmen des rechtlich Zulässigen gemeinsame behördenübergreifende Ermittlungsgruppen eingerichtet werden.
29. Die gesetzlichen Aufgaben und Befugnisse der Sicherheitsbehörden sind mit Blick auf die aktuellen Herausforderungen durch Spionage, Sabotage und Destabilisierungsbestrebungen ausländischer Akteure zu überprüfen und anzupassen. Dabei sind insbesondere auch die Zusammenarbeit und der Informationsaustausch der Behörden mit Privaten in den Blick zu nehmen.

30. Es ist ein modernes Wirtschaftsschutzstrafrecht mit einer klaren Ordnungsidee zu schaffen.
31. Sinnvoll erscheint die gesetzliche Einführung eines/einer sicherheitsüberprüften „Wirtschaftsschutzbeauftragten“ als auch bei den Behörden hinterlegte Kontaktperson bei Unternehmen einer gewissen Größenordnung.
32. Wirtschaftsschutzinitiativen sind wissenschaftlich zu begleiten und hierzu mit strategischen Forschungsinitiativen und Fördermitteln aus öffentlicher wie privater Hand auszustatten.