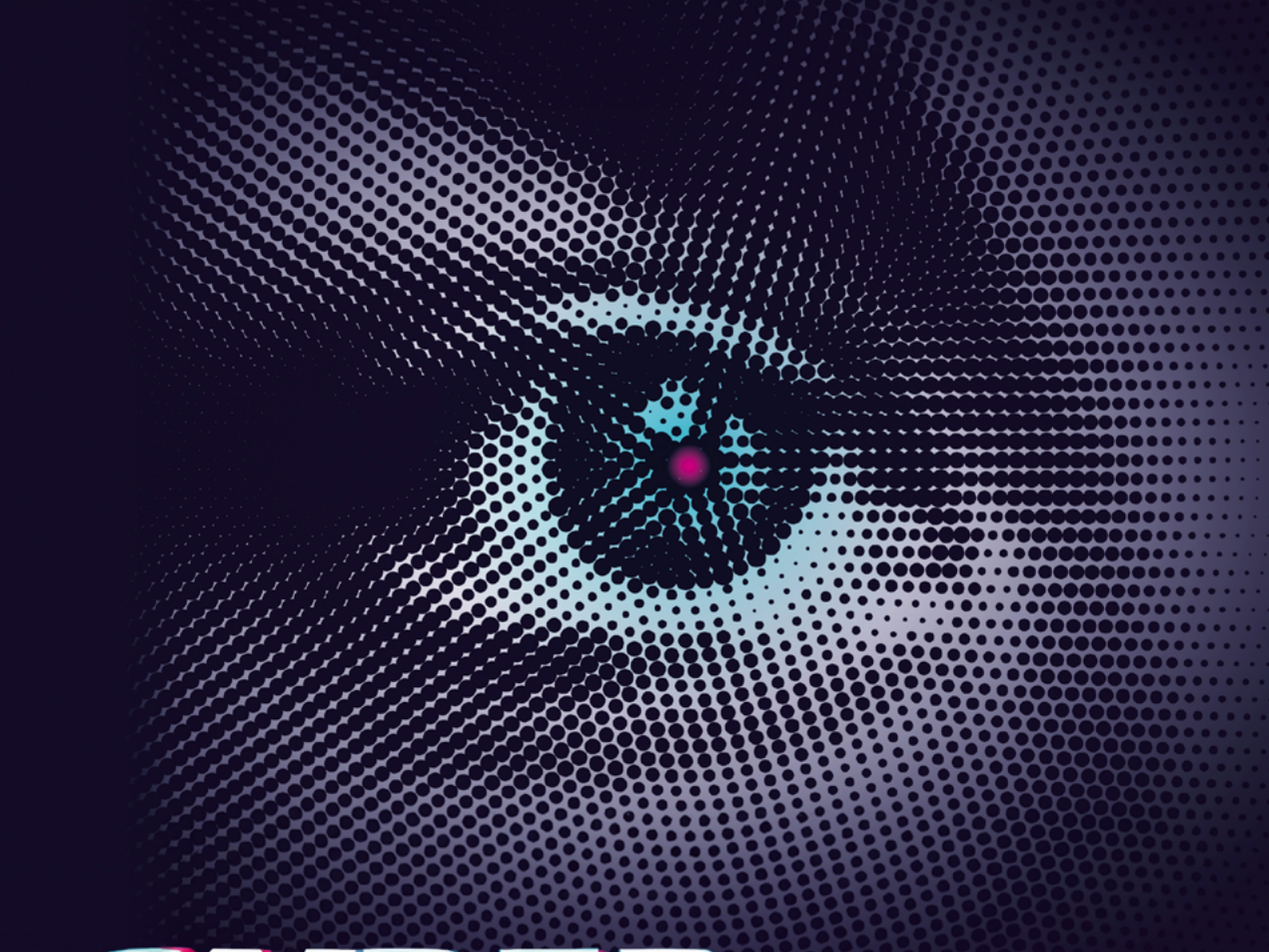


CYBER SPIONAGE

Wie Nachrichtendienste um Informationen und Kontrolle kämpfen

Florian Dalwigk

Rheinwerk Computing

Liebe Leserin, lieber Leser,

kann man aus Büchern etwas über die geheime Arbeit von Nachrichtendiensten lernen? Sind das nicht streng geheime Vorgänge, über die niemand schreiben darf? Die Antwort: *Ja – und nein*.

Operative Details bleiben natürlich Verschlusssache. Die Identität von Agenten oder der Ablauf von Geheimoperationen müssen geschützt werden. Doch für das Verständnis der Hintergründe und Folgen sind sie unerheblich. Schon Arthur Schlesinger, »Hofhistoriker« des Weißen Hauses und enger Vertrauter mehrerer US-Präsidenten, betonte:

> *There have been few greater frauds, [than the idea] that only those with access to classified information know enough to have a judgment on questions of foreign policy. Actually, 99 per cent of the information necessary for intelligent political judgment is available to any careful reader [...].*[1]

Auch der ehemalige US-Außenminister Dean Rusk war überzeugt: Bürgerinnen und Bürger können sich eine fundierte Meinung bilden – ganz ohne Geheimwissen.

> *I don't know of many subjects on which a private citizen could not make a reasonable judgment by reading information readily available on that subject. I don't believe that secrets impair the judgment of citizens about major policy issues.*[2]

Florian Dalwigk hat in diesem Buch genau das getan: Offene Quellen so zusammengeführt, dass Sie sich selbst ein Bild machen können. Bevor Sie anfangen zu lesen, habe ich aber noch einen Hinweis: Das Buch wurde mit großer Sorgfalt geschrieben, lektoriert und produziert. Aber wo Menschen arbeiten, passieren Fehler. Haben Sie Korrekturen oder Anregungen? Melden Sie sich gern!

Ihr Dr. Christoph Meister
Lektorat Computing

christoph.meister@rheinwerk-verlag.de
www.rheinwerk-verlag.de
Rheinwerk Verlag • Rheinwerkallee 4 • 53227 Bonn

1 Schlesinger, A. (1972): The Secrecy Dilemma, in: The New York Times. 6. Feb. 1972. S. 12
2 Rusk, D. (1990). As I Saw It. S. 578.

Auf einen Blick

Impressum

Dieses E-Book ist ein Verlagsprodukt, an dem viele mitgewirkt haben, insbesondere:

Autor Florian Dalwigk
Lektorat Christoph Meister
Copy-Editing Friederike Daenecke, Zülpich
Typografie & Layout Vera Brauner
Satz E-Book SatzPro, Krefeld
Herstellung E-Book Maxi Beithe
Covergestaltung Bastian Illerhaus
Coverbild Shutterstock: 2244549565 © Kundra, 1891545190 © DaryaKoM

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

ISBN 978-3-367-11181-7 (E-PDF)

1. Auflage 2026
© Rheinwerk Verlag, Bonn 2026

Rheinwerk Verlag GmbH • Rheinwerkallee 4 • 53227 Bonn
service@rheinwerk-verlag.de

Informationen zu unserem Verlag und Kontaktmöglichkeiten finden Sie auf unserer Verlagswebsite *www.rheinwerk-verlag.de*. Dort können Sie sich auch umfassend über unser aktuelles Programm informieren und unsere Bücher und E-Books bestellen.

Inhalt

Geleitwort

Als ich vor einigen Jahren meinen Dienst antrat, glaubte ich noch, Spionage würde so aussehen wie in den alten James-Bond-Filmen: geheime Treffen in Tiefgaragen, Nachrichten in toten Briefkästen und finstere Typen in Trenchcoats. Doch die Welt, in der Nachrichtendienste heute operieren, ist eine vollkommen andere. Die gefährlichsten Operationen unserer Zeit finden nicht mehr in dunklen Gassen statt: Sie laufen in Rechenzentren, über Glasfaserleitungen und auf mobilen Endgeräten. Ich habe in meiner bisherigen Laufbahn schon erlebt, wie Staaten durch Einfluss in Social-Media versucht habe, Gesellschaften zu destabilisieren, ohne dass ein einziger Schuss fällt. Ich habe gesehen, wie Hackergruppen kritische Infrastrukturen attackieren und Informationen ausspähen.

Cyberspionage ist ein fester Bestandteil geopolitischer Machtpolitik geworden. Staaten kämpfen längst nicht mehr nur um Territorien oder Rohstoffe, sondern um Daten, Zugänge und die Kontrolle über digitale Systeme. Wer Informationen besitzt, besitzt Macht. Dabei ist die Grenze zwischen Krieg, Spionage und Cyberkriminalität kaum noch klar erkennbar. Hackergruppen agieren im Auftrag von Staaten, Staaten bedienen sich wiederum teilweise krimineller Organisationen und künstliche Intelligenz beginnt zunehmend, die Spielregeln dieser Konflikte grundlegend zu verändern. Besonders gefährlich ist, dass Cyberspionage häufig monate- oder sogar jahrelang unentdeckt bleibt. Systeme funktionieren dem Anschein nach normal weiter, während im Hintergrund Informationen ausgeleitet und analysiert werden.

Viele Menschen gehen noch immer davon aus, sie seien für ausländische Dienste uninteressant. Doch genau diese Annahme ist längst überholt. In einer digitalisierten Welt ist nahezu jede Information potenziell wertvoll. Bewegungsprofile, Kontakte, persönliche Interessen oder Metadaten ergeben zusammengenommen ein äußerst präzises Bild eines Menschen.

Dieses Buch zeigt eine Welt, über die öffentlich nur selten gesprochen wird. Eine Welt zwischen Machtpolitik, Kontrolle von Informationen und psychologischer Einflussnahme. Florian Dalwigk gelingt dabei etwas, das in diesem Themenfeld selten geworden ist. Er verbindet technische Hintergründe mit strategischem Verständnis und macht komplexe Zusammenhänge nachvollziehbar, ohne sie unnötig zu sensationalisieren.

Das Buch führt nicht nur oberflächlich in Welt der Nachrichtendienste und Cyberspionage ein, sondern beleuchtet unter anderem staatliche Akteure, Malware als geopolitische Waffe, Einflussoperationen und die oft unterschätzte Rolle künstlicher Intelligenz in zukünftigen Konflikten. Dabei wird eines schnell deutlich: Cyberspionage betrifft nicht nur Regierungen oder Geheimdienste. Sie betrifft Unternehmen, Wissenschaftseinrichtungen, kritische Infrastruktur und letztlich jeden einzelnen Bürger. Denn wer heute digitale

Systeme nutzt, bewegt sich automatisch in einem Raum, der von Interessen, Überwachung, Manipulation und Informationsgewinnung geprägt ist.

Dieses Buch romantisiert Nachrichtendienste nicht. Es verklärt weder Spionage noch Überwachung. Stattdessen vermittelt es ein realistisches Bild einer Welt, die häufig von Grauzonen geprägt ist. Genau das macht seine besondere Stärke aus. Es zeigt, dass Sicherheitsbehörden einerseits notwendig sein können, um Staaten und Gesellschaften zu schützen, gleichzeitig aber immer auch Fragen nach Kontrolle, Transparenz und Freiheit aufwerfen. Vielleicht werden Sie einige Kapitel mit einem Gefühl der Faszination lesen. Andere hingegen könnten Sie verunsichern. Das ist normal. Wer beginnt, die Mechanismen moderner Informationskriege zu verstehen, erkennt schnell, wie verletzlich digitalisierte Gesellschaften tatsächlich sind. Und dennoch halte ich Bücher wie dieses für wichtig. Die Öffentlichkeit bekommt von diesen Entwicklungen meist nur dann etwas mit, wenn große Vorfälle bekannt werden. Edward Snowden lässt grüßen.

Demokratische Gesellschaften dürfen Themen wie Cyberspionage, Einflussoperationen und digitale Machtstrukturen nicht ausschließlich Geheimdiensten oder Militärs überlassen. Wissenschaft und Öffentlichkeitsarbeit in diesem Bereich sind essenziell, damit Menschen verstehen können, wie moderne Konflikte funktionieren und welche Risiken mit neuen Technologien verbunden sind. Die größte Gefahr geht oft nicht von dem aus, was geheim ist. Sondern von dem, was offen geschieht und trotzdem kaum jemand bemerkt. Vielleicht werden Sie nach diesem Buch manche Dinge anders betrachten. Ihr Smartphone. Ihre digitalen Spuren. Profile in sozialen Netzwerken. Nachrichtenmeldungen. Die scheinbar harmlose App auf Ihrem Gerät. Vielleicht erkennen Sie, dass Informationen niemals neutral sind und dass Kontrolle über Informationen zu den mächtigsten Werkzeugen unserer Zeit gehört.

Cyberspionage ist längst Teil unserer Gegenwart geworden. Dieses Buch hilft Ihnen dabei, sie zu verstehen.

Franz K.
Mitarbeiter im Umfeld eines Nachrichtendiensts

Kapitel 1
Von Spionen und Hackern

Seit Staaten existieren, versuchen sie, einander auszuhorchen, Schwächen des Gegners zu identifizieren und strategische Vorteile zu erlangen. Jahrhundertelang geschah das aufgrund des damaligen Standes der Technik vor allem durch menschliche Quellen, geheime Treffen, chiffrierte Nachrichten und riskante Operationen. Während die Motivation für Spionage auch heute noch die gleiche ist, hat sich das Schlachtfeld grundlegend verschoben, denn mittlerweile findet ein Großteil geheimer staatlicher Konflikte nicht mehr in dunklen Gassen statt, sondern in Rechenzentren und auf Servern. Informationen, die einst nur in verstaubten Aktenschränken verwahrt wurden, zirkulieren nun in globalen Netzwerken. Geheime Regierungsdokumente, Militärpläne und zutiefst persönliche Kommunikationen liegen digital vor – oft nur durch wenige technische Barrieren geschützt. Das ist das Feld, auf dem die moderne Cyberspionage agiert.

Sie hinterlässt keine aufgebrochenen Türen und keine direkt sichtbaren Spuren am Tatort. Häufig bleibt sie monatelang, manchmal sogar jahrelang unentdeckt. Während Systeme scheinbar normal funktionieren, werden im Hintergrund Daten kopiert, analysiert und ins Ausland weitergeleitet. Betroffen sind nicht nur Geheimdienste und Militärs, sondern auch Unternehmen, Forschungseinrichtungen, kritische Infrastrukturen und letztlich auch unsere Gesellschaft. Die Täter sind nicht nur vereinzelte Hacker mit kriminellen Motiven, sondern hochprofessionelle Akteure, die staatlich unterstützt werden und mit erheblichen Ressourcen ausgestattet sind.

In diesem Kapitel lege ich das Fundament, das es Ihnen ermöglicht, hinter die Kulissen dieser unsichtbaren Konflikte zu blicken. Bevor wir konkrete Akteure, Methoden oder Fallbeispiele betrachten, ist es notwendig, ein gemeinsames Verständnis von den Begriffen zu schaffen: Was genau versteht man unter Spionage, Nachrichtendiensten, Geheimdiensten oder Cyberspionage? Darauf aufbauend stelle ich Ihnen den sogenannten *Geheimdienstzyklus* vor. Dieses Modell beschreibt, wie Informationen systematisch gewonnen, ausgewertet und in politische Entscheidungsprozesse eingebracht werden.

Ein wichtiger Schwerpunkt ist die Abgrenzung zwischen *Cyberspionage* und *Cyberkriminalität*. Beide Phänomene nutzen ähnliche technische Werkzeuge, verfolgen jedoch grundlegend unterschiedliche Ziele und unterliegen anderen rechtlichen und politischen Rahmenbedingungen. Diese Unterscheidung ist wichtig, um staatliches Handeln, strafrechtliche Verfolgung und internationale Reaktionen korrekt bewerten zu können.

Disclaimer

Dieses Buch basiert ausschließlich auf öffentlich zugänglichen, frei verfügbaren und allgemein bekannten Informationen. Alle dargestellten Sachverhalte, Methoden und Fallbeispiele stammen aus offenen Quellen wie wissenschaftlicher Literatur, Gerichtsentscheidungen, parlamentarischen Dokumenten, Medienberichten sowie offiziellen Veröffentlichungen staatlicher Stellen und internationaler Organisationen.

Es werden keine Verschlusssachen oder geheimhaltungsbedürftigen Informationen beschrieben oder offengelegt.

Die Darstellung verfolgt keine politische Agenda und erhebt nicht den Anspruch, reale nachrichtendienstliche Verfahren in Teilen oder gar vollständig abzubilden. Etwaige Fallbeispiele, Szenarien oder Personen, die im Buch beschrieben werden, sind, sofern sie nicht ausdrücklich als real gekennzeichnet werden, fiktiv oder abstrahiert. Sie dienen ausschließlich der Veranschaulichung komplexer Zusammenhänge und stellen keinen Bezug zu laufenden oder realen nachrichtendienstlichen Operationen her.

Dieses Buch ist kein Insiderbericht, keine Anleitung und kein Beitrag zum Geheimnisverrat, sondern eine Aufarbeitung dessen, was in demokratischen Gesellschaften öffentlich diskutierbar und überprüfbar ist.

1.1 Das Geheimnis dieses Buchs

Cyberspionage ist kein Themenfeld, das man sich allein über Definitionen, Schaubilder und Merksätze erschließen sollte. Deshalb ist dieses Buch bewusst als spannende Entdeckungsreise konzipiert, die Theorie, Praxis und eigene Spionageaktivitäten miteinander verbindet.

In mehreren Kapiteln werden aktuell für die Cyberspionage relevante Themen behandelt. Wir beginnen mit technischen Grundlagen und tasten uns über operative Methoden bis hin zu rechtlichen, politischen und gesellschaftlichen Fragen vor. Die theoretischen Abschnitte liefern Ihnen das notwendige Fundament, um spätere Beispiele und Diskussionen einordnen zu können. Mein Ziel ist, dass Sie ein echtes Verständnis und Gefühl dafür bekommen, wie Cyberspionage heutzutage praktiziert wird und warum Sie davon betroffen sind.

Begleitet werden diese Grundlagen durch Videos aus meiner Vorlesung »Cyberspionage«, die ich seit 2024 an verschiedenen Hochschulen in Deutschland und im Ausland anbiete. In diesen Videos werden ausgewählte Inhalte vertieft, visualisiert oder aus einer anderen Perspektive beleuchtet.

In Kapitel 7, »OSINT – Die Macht der frei zugänglichen Informationen«, begleitet Sie zudem ein fiktiver Spionagefall, an dem Sie aktiv teilnehmen können. Dreh- und Angel-

punkt ist der russische Agent Florin Dalvikov, der bereits von vielen Nachrichten- und Geheimdiensten weltweit beobachtet wird. Wenn Sie sich länger mit ihm und seinem Wirken beschäftigen, werden Sie feststellen, dass er es mit der operativen Sicherheit nicht so genau nimmt, was Ihnen die Möglichkeit bietet, über ihn zu recherchieren und seinen digitalen Spuren bis in den Kreml zu folgen.

Ergänzt wird jedes Kapitel durch Nachdenkfragen. Sie dienen nicht der Wissensabfrage, sondern sollen Sie dazu anregen, Position zu beziehen, Annahmen zu hinterfragen und Parallelen zur realen Welt zu ziehen. Die meisten dieser Fragen haben keine eindeutige Antwort, und genau das ist auch beabsichtigt. Wenn Sie über ein bestimmtes Thema diskutieren möchten, dann kontaktieren Sie mich gern per LinkedIn (*https://www.linkedin.com/in/florian-dalwigk/*) oder senden Sie mir eine E-Mail an *info@florian-dalwigk.de*.

Das Geheimnis dieses Buchs besteht somit nicht in der reinen Wissensvermittlung, sondern im Zusammenspiel aus praxisnahen Berichten, der Anwendung echter Spionagetechniken und Reflexion. Ich lade Sie ein, Cyberspionage nicht, wie in vielen anderen Büchern, nur passiv durch Lesen nachzuvollziehen, sondern sie zu erleben.

Ich wünsche Ihnen viel Spaß beim Spionieren!

1.2 Worüber reden wir eigentlich?

Bevor man sich näher mit einem neuen Thema beschäftigt, sollte man sich zunächst den Begriffsapparat anschauen. Das gilt umso mehr, wenn es viele unterschiedliche Definitionen und Ideen gibt, die eine gute Kommunikation schwer machen.

1.2.1 Begriffe und Definitionen

Was versteht man eigentlich unter *Spionage*? Darüber gibt die folgende Definition des Bundesamtes für Verfassungsschutz Auskunft:

> *»Unter Spionage versteht man die Erkundung der politischen Faktoren sowie der wirtschaftlichen, wissenschaftlichen und militärischen Potenziale eines anderen Staates durch ausländische Nachrichtendienste oder in deren Auftrag - zumeist mit verdeckten Mitteln und Methoden. Soweit Spionage gegen die Bundesrepublik Deutschland gerichtet ist, kommt eine Strafbarkeit gemäß § 93 ff. StGB in Betracht.«*[1]

Schauen wir uns diese Definition etwas genauer an:

- Die *Erkundung der politischen Faktoren* bezieht sich auf das Sammeln von Informationen über die politische Landschaft, Entscheidungsträger, politische Pläne und Strategien eines Staates. Die Informationen können z. B. beinhalten, wie ein Staat auf in-

1 Bundesamt für Verfassungsschutz. Begriffe und Hintergründe. *https://www.verfassungsschutz.de/DE/themen/spionage-und-proliferationsabwehr/begriff-und-hintergruende/begriff-und-hintergruende_node.html* [Stand: 19.03.2025].

terne oder externe Ereignisse reagiert oder welche langfristigen politischen Ziele er verfolgt.

- Mit *wirtschaftlichen Potenzialen* sind Informationen über die Wirtschaftskraft eines Staates gemeint. Diese umfassen Daten zu wichtigen Industrien, Handelsbeziehungen, wirtschaftlichen Ressourcen und Innovationen sowie ökonomischen Strategien und Plänen.
- Mit *militärischen Potenzialen* sind Informationen über die Streitkräfte eines Staates, deren Fähigkeiten, Ausrüstung, Strategien, Pläne und Manöver gemeint. Das schließt auch geheime Informationen über Militärtechnologie und Verteidigungsinfrastruktur ein.
- Spionage wird typischerweise mit *verdeckten Mitteln und Methoden* durchgeführt, die darauf abzielen, ohne Wissen oder Genehmigung des Beobachtungsobjekts Informationen zu sammeln. In Deutschland sind dafür sogenannte *nachrichtendienstliche Mittel* vorgesehen.
- Spionage, die gegen die Bundesrepublik Deutschland gerichtet ist, ist hierzulande strafrechtlich relevant. Die *Paragrafen 93 ff. des Strafgesetzbuches (StGB)* befassen sich mit *Landesverrat* und *geheimdienstlicher Agententätigkeit*. Diese Gesetze definieren die rechtlichen Grenzen und die Strafen für Aktivitäten, die als Spionage eingestuft werden können.

Nachdem wir soeben geklärt haben, was man unter dem Begriff Spionage versteht und dass sie sich (in Deutschland) sogenannter nachrichtendienstlicher Mittel bedient, schauen wir uns nun an, was sich dahinter verbirgt:

> *Nachrichtendienstliche Mittel* sind Werkzeuge, Methoden und Techniken, die von Nachrichtendiensten verwendet werden, um Informationen zu sammeln, zu analysieren und zu verarbeiten.

Beispiele für solche nachrichtendienstliche Mittel sind Abhörwanzen, Observation sowie die Überwachung des Brief-, Post- und Fernmeldeverkehrs.[2]

Spione und Agenten

Spionage wird in der Regel von Spionen durchgeführt. Oder doch von Agenten? Was ist der Unterschied?

> Ein *Agent* ist jede Person, die offiziell oder inoffiziell für einen Nachrichten- oder Geheimdienst arbeitet.

2 Die rechtliche Grundlage dafür bildet das Artikel-10-Gesetz (siehe Abschnitt 2.5).

Diese Definition eines Agenten umfasst jede Person, die für einen Nachrichten- oder Geheimdienst tätig ist, und zwar von den Reinigungskräften bis hin zu seinem Präsidenten. Die Rolle von Reinigungskräften darf in diesem Zusammenhang nicht unterschätzt werden, da diese weitreichenden Zugriff auf die Büros der anderen Agenten haben und dadurch prädestiniert für Anwerbungsversuche von fremden Diensten sind. Nicht umsonst wird in Deutschland auch für diese Personen, wenn sie das Gelände eines Nachrichten- oder Geheimdienstes betreten sollen, eine Sicherheitsüberprüfung mit besonderen Sicherheitsermittlungen (SÜ3, siehe Abschnitt 2.2.3) durchgeführt.

Auch wenn man intuitiv davon ausgeht, dass ein Spion dasselbe wie ein Agent ist, so gibt es doch einen entscheidenden Unterschied:

> Ein *Spion* ist eine Person, die heimlich und unter falscher Identität Informationen sammelt, die für eine fremde Regierung, Organisation oder Gruppe von strategischem Interesse sind.

Der Hauptunterschied zwischen einem Agenten und einem Spion besteht darin, dass Spione speziell für das verdeckte Sammeln von Informationen ausgebildet sind und ihre Identität sowie ihre Missionen geheim halten. Aus diesen beiden Definitionen können wir schlussfolgern, dass jeder Spion ein Agent, aber nicht jeder Agent ein Spion ist.

Sie haben im Zusammenhang mit Agenten bestimmt auch schon einmal von Doppelagenten gehört, oder?

> Ein *Doppelagent* ist eine Person, die offiziell für einen Nachrichten- oder Geheimdienst arbeitet, jedoch insgeheim Informationen an einen konkurrierenden oder feindlichen Dienst weitergibt.

Ein Doppelagent nutzt seine offizielle Position und seinen Zugang zu Geheimnissen, um diese Informationen heimlich an den Gegner zu übermitteln. Das kann zwecks persönlicher Bereicherung, aus ideologischen Gründen oder durch Zwang erfolgen. Doch was unterscheidet einen Doppelagenten von einem Spion?

Neben der Informationsbeschaffung spielt ein Doppelagent auch eine wichtige Rolle im strategischen Spiel zwischen zwei konkurrierenden Geheimdiensten, indem er Informationen manipuliert, um die Aktionen und Reaktionen der involvierten Parteien zu beeinflussen. Das primäre Ziel eines Spions ist es, Informationen zu sammeln, die dem Auftraggeber nützen.

Beide operieren im Geheimen: Sowohl Spione als auch Doppelagenten müssen ihre wahren Absichten und Tätigkeiten vor anderen verbergen, um effektiv zu sein und nicht enttarnt zu werden. Sowohl Spione als auch Doppelagenten sind damit beschäftigt, sensible Informationen zu sammeln. Diese Informationen sind in der Regel von strategischer Bedeutung für die Regierung oder die Organisation, die sie repräsentieren oder der sie Infor-

mationen liefern. Beide setzen sich erheblichen persönlichen Risiken aus. Die Entdeckung könnte zu schwerwiegenden Konsequenzen wie Strafverfolgung, Folter bis hin zu einem Todesurteil durch die betroffenen Parteien führen.

Ein Doppelagent ist also offiziell ein Mitglied oder Mitarbeiter eines Nachrichten- oder Geheimdienstes, arbeitet aber heimlich auch für einen konkurrierenden oder feindlichen Dienst. Seine Tätigkeit umfasst den Verrat an seinem eigenen Dienst. Ein Spion arbeitet in der Regel ausschließlich für eine fremde Regierung oder Organisation, oft unter einer falschen Identität bzw. *Legende* und ist nicht offiziell mit dem Ziel seiner Spionage verbunden.

Ein bekanntes Beispiel für einen Doppelagenten war Oleg Antonowitsch Gordijewski. Gordievsky war KGB-Offizier und diente in westlichen Posten, arbeitete aber über Jahre hinweg heimlich als Doppelagent für den britischen Geheimdienst MI6.[3] Als sowjetischer Insider lieferte er Informationen an Großbritannien, während er nach außen weiterhin als KGB-Mann auftrat.

Spione, Agenten und Doppelagenten haben gemeinsam, dass sie sich für Geheimnisse interessieren. Eine wichtige Art von Geheimnis ist das *Staatsgeheimnis*. Dieses ist im Strafgesetzbuch (StGB) folgendermaßen definiert:[4]

> *»§ 93 Begriff des Staatsgeheimnisses*
>
> *(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.*
>
> *(2) Tatsachen, die gegen die freiheitliche demokratische Grundordnung oder unter Geheimhaltung gegenüber den Vertragspartnern der Bundesrepublik Deutschland gegen zwischenstaatlich vereinbarte Rüstungsbeschränkungen verstoßen, sind keine Staatsgeheimnisse.«*

Beispiele für Staatsgeheimnisse nach § 93 StGB sind unter anderem *militärische Informationen*, d. h. Details über Verteidigungsstrategien, Waffensysteme, Stationierungsorte von Truppen oder geheime Militäroperationen. Auch *diplomatische Korrespondenzen*, also die vertrauliche Kommunikation zwischen Botschaften, oder geheime Verhandlungsdetails zählen dazu, ebenso wie Informationen aus der Arbeit von Nachrichtendiensten, die zur Abwehr von Gefahren für die nationale Sicherheit beitragen.

3 The Guardian. (21.03.2025). Former KGB double agent Oleg Gordievsky dies in Surrey aged 86. *https://www.theguardian.com/uk-news/2025/mar/21/former-kgb-double-agent-oleg-gordievsky-dies-in-surrey-aged-86* [Stand: 27.12.2025].

4 Strafgesetzbuch (StGB). § 93 Begriff des Staatsgeheimnisses. *https://www.gesetze-im-internet.de/stgb/__93.html* [Stand: 31.03.2025].

Agenten und Spione verwenden sogenannte Legenden:

> Eine *Legende* ist eine sorgfältig konstruierte Identität oder Hintergrundgeschichte, die ein Agent oder Spion verwendet, um seine wahre Identität zu verbergen und seine Spionageaktivitäten zu ermöglichen.

Eine Legende kann aus detaillierten Lebensgeschichten, gefälschten Dokumenten, Berufserfahrungen, sozialen Verbindungen und anderen Elementen bestehen, die alle darauf abzielen, den Agenten in seiner Rolle glaubwürdig zu machen. Diese falsche Identität muss konsistent, überzeugend und robust genug sein, um Überprüfungen durch einen Geheimdienst oder neugierige Personen standzuhalten, die Zweifel an der Echtheit des Agenten hegen könnten. Die Erstellung und Aufrechterhaltung einer Legende ist eine grundlegende Fähigkeit im Spionagehandwerk, da sie für den Erfolg von verdeckten Operationen entscheidend ist.

Frage #001: Überlegen Sie sich eine glaubwürdige Legende, mit der Sie Zugang zur Münchner Sicherheitskonferenz (MSC) bekommen könnten.

Operationen

Spionageakte finden in der Regel in sogenannten Operationen statt:

> Eine *Operation* ist eine systematische und geplante Aktion oder Serie von Aktionen, die von Nachrichten- oder Geheimdiensten durchgeführt wird, um Informationen zu sammeln, zu analysieren oder zu beeinflussen. Dabei werden verschiedene Spionagetechniken wie HUMINT oder SIGINT eingesetzt. Eine Operation wird von *Operateuren* durchgeführt.

Operateure sind in diesem Zusammenhang z. B. Spione. Im Spionagekontext meint man jedoch meistens verdeckte Operationen:

> Eine *verdeckte Operation*, auch *Geheimoperation* genannt, ist eine Operation, bei der die Beteiligung des auftraggebenden Akteurs nicht offengelegt werden soll.

Verdeckte Operationen können verschiedene Formen annehmen. Bei der klassischen Spionage werden die politischen Faktoren sowie die wirtschaftlichen, wissenschaftlichen und militärischen Potenziale eines anderen Staates durch ausländische Dienste erkundet.

Sabotage bezeichnet Aktivitäten, die darauf abzielen, feindliche Ressourcen oder Operationen zu stören oder zu zerstören, wie das Sprengen von Brücken oder das Stören der Kommunikationsinfrastruktur. Berichten zufolge haben russische Hackergruppen z. B. Sabotageversuche gegen niederländische kritische Infrastrukturen durchgeführt, indem

sie digitale Zugangspunkte infiltrierten, um spätere Störungen herbeizuführen.[5] Obwohl größere Schäden bislang verhindert wurden, markiert dies eine weitere Eskalation hybrider Bedrohungen, bei denen Sabotageabsichten digital initiiert werden.

Unter *Einflussoperationen (Influence Operations)* versteht man Maßnahmen, die darauf abzielen, politische Entscheidungen oder öffentliche Meinungen in einem anderen Land zu beeinflussen. Das wird oft durch die Verbreitung von Propaganda oder Desinformation zu erreichen versucht. US-Behörden beschrieben 2024 eine verdeckte, staatlich unterstützte Kampagne, die unter anderem Influencer, bezahlte Social-Media-Werbung, KI-generierte Inhalte und ein Netz aus Domains bzw. Accounts nutzte, um russische Narrative zu pushen und Reichweite zu erzeugen.[6]

Die Geheimhaltung steht bei verdeckten Operationen an oberster Stelle. Die Operateure müssen darauf achten, die Verbindungen zum auftraggebenden Staat oder Dienst zu verschleiern, um diplomatische Verwicklungen, öffentliche Skandale oder militärische Vergeltungsschläge zu vermeiden. Bei solchen Operationen werden häufig sogenannte Schläferzellen eingesetzt.

> Eine *Schläferzelle* bezeichnet eine Gruppe von Agenten, die von einer Organisation oder einem Staat aktiviert werden können, aber bis zu diesem Zeitpunkt inaktiv bleiben und ein normales Leben führen.

Im Film *Salt* (2010) mit Angelina Jolie wird dieses Konzept sehr anschaulich dargestellt: Die Hauptfigur Evelyn Salt ist eine CIA-Agentin, von der behauptet wird, sie sei eine russische Schläferagentin. Im Laufe des Films wird klar, dass sie Teil eines sowjetischen Programms war, bei dem Kinder in den USA aufgezogen und trainiert wurden, um später als getarnte Agenten zu agieren – also klassische Schläferzellen. Sie lebten ein normales Leben, bis der Zeitpunkt kam, an dem sie ihren geheimen Auftrag erfüllen sollten.

Solche Spionagefilme bilden aber natürlich nur einen Teil der Realität ab. Genauso, wie beim Hacking nicht fortwährend Tausende Codezeilen in atemberaubender 3D-Grafik vor dem inneren Auge eines Hackers vorbeifliegen, so sind auch reale nachrichtendienstliche Operationen meist unspektakulär, geprägt von langwieriger Vorbereitung, Tarnung und psychologischer Einflussnahme. Ein historisches Beispiel für derartige verdeckte Strukturen ist das NATO-Programm *Gladio*, bei dem Schläferzellen in Westeuropa während des Kalten Krieges im Geheimen aufgebaut wurden, um im Falle einer sowjetischen Invasion sofort aktiviert werden zu können.

5 Martin, A. (22.04.2025). Russia attempting cyber sabotage attacks against Dutch critical infrastructure. The Record. *https://therecord.media/dutch-mivd-report-russian-cyber-sabotage* [Stand: 27.12.2025].

6 U.S. Department of Justice. (04.09.2024). Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere (Press release). *https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence* [Stand: 27.12.2025].

Neben *Operationen* und *verdeckten Operationen* gibt es noch *Black Ops*:

> *Black Ops* sind spezielle, streng geheime verdeckte Operationen, die von Geheimdiensten durchgeführt werden, um heikle und oft rechtlich oder moralisch fragwürdige Ziele zu erreichen, ohne dass eine offizielle Verbindung oder Verantwortlichkeit nachweisbar ist. Diese Operationen sind so konzipiert, dass sie eine maximal plausible Abstreitbarkeit bieten, falls ihre Aktivitäten aufgedeckt werden sollten.

Black Ops sind also von einem hohen Grad an Geheimhaltung geprägt. Die beteiligten Operateure, ihre Aktionen, Ziele und selbst die Existenz der Operationen selbst werden streng vertraulich behandelt.

Ein zentrales Merkmal dieser Art von Operationen ist die Fähigkeit der auftraggebenden Regierung oder Organisation, jegliche Beteiligung abzustreiten. Das wird oft durch die Verwendung von nicht registrierten Operationseinheiten erreicht. Zudem bleibt in der Regel eine offizielle Dokumentation aus. Black Ops können den Einsatz von unter normalen Umständen als illegal oder unethisch geltenden Methoden umfassen, wie z. B. Sabotage, Entführungen, gezielte Tötungen, die Förderung von Unruhen oder andere Formen der verdeckten Kriegsführung.

Ein Beispiel für eine Black Op ist *Operation Ajax* aus dem Jahr 1953. Hierbei handelte es sich um eine Operation von der CIA zum Sturz des iranischen Premierministers Mohammad Mossadegh, um pro-westliche Mächte in Iran zu stärken und den Zugang zu Ölressourcen zu sichern.

Malware

Im Kontext von Malware bezeichnet *Dormant Malware* Schadsoftware, die sich zunächst unauffällig verhält, nachdem sie ein System infiziert hat. Sie bleibt inaktiv, bis sie durch einen bestimmten *Trigger*, z. B. ein Datum, ein bestimmtes Ereignis oder einen Befehl vom Angreifer, aktiviert wird. Ein Beispiel für eine solche Dormant Malware ist der Android-Trojaner *Andr/KongFu-L*. Diese Schadsoftware tarnte sich als voll funktionsfähige Version des Spiels *Angry Birds Space* und wurde über inoffizielle Android-App-Stores verbreitet.

Nach der Installation blieb die Malware zunächst inaktiv und unauffällig. Erst nach Erreichen eines bestimmten Spielfortschritts, z. B. beim Abschluss eines bestimmten Levels, wurde sie aktiviert. Dann nutzte sie die *GingerBreak-Sicherheitslücke*, um Root-Zugriff auf das Gerät zu erlangen, und kontaktierte einen C2-Server, um weitere schädliche Software nachzuladen.[7]

7 CIO Insight Staff. (16.04.2012). Malware masquerading as Angry Birds game. CIO Insight. *https://www.cioinsight.com/mobile/malware-masquerading-as-angry-birds-game/* [Stand: 15.04.2025].

1.2.2 Nachrichtendienste und Geheimdienste

Bisher haben wir primär von *Nachrichtendiensten* gesprochen. Hin und wieder hat sich der Begriff *Geheimdienst* eingeschlichen. Worin besteht der Unterschied?

> Ein *Nachrichtendienst* ist eine staatliche Behörde, die Informationen sammelt und analysiert, um die nationale Sicherheit zu gewährleisten und die politische Führung eines Landes zu beraten. Ein Nachrichtendienst nutzt dafür nachrichtendienstliche Mittel.
>
> *Geheimdienste* sind eine spezielle Form von Nachrichtendiensten, die geheimdienstliche Mittel einsetzen.

Geheimdienstliche Mittel

Geheimdienstliche Mittel sind das, was einen Nachrichten- von einem Geheimdienst unterscheidet.[8] Welche geheimdienstlichen Mittel gibt es?

- *Agitation* bezieht sich auf Aktivitäten, die darauf abzielen, öffentliche Unruhe oder Unzufriedenheit zu schüren, oft durch emotionale oder provokative Reden und Propaganda. Ihr Ziel ist es, politische, soziale oder wirtschaftliche Veränderungen herbeizuführen oder zu verhindern.
- *Diversion* meint die Durchführung von Störungen, um die Aufmerksamkeit von wichtigeren Ereignissen oder Operationen abzulenken. Diversion kann auch den Einsatz von Ressourcen oder Kräften in unwichtigen oder irreführenden Bereichen beinhalten, um den Gegner auf die falsche Fährte zu locken.
- *Subversion* bezeichnet das Untergraben der Macht und Autorität einer Regierung mit dem Ziel, die bestehende Machtstruktur zu schwächen oder zu stürzen und das Vertrauen in sie zu untergraben. Das kann z. B. durch Infiltration, Propaganda oder psychologische Kriegsführung (*PsyOps*) erfolgen.
- Der Begriff *Zersetzung* wurde ursprünglich von dem *Ministerium für Staatssicherheit (MfS, »Stasi«)* verwendet und bezeichnet Methoden zur psychologischen Manipulation und Destabilisierung von Personen oder Gruppen, um deren Glaubwürdigkeit zu untergraben, Konflikte zu schüren und sie letztendlich handlungsunfähig zu machen.
- *Sabotage* bezeichnet gezielte Handlungen zur Störung, Beschädigung oder auch Zerstörung von Infrastrukturen, Anlagen, Kommunikations- oder IT-Systemen, um staatliche, wirtschaftliche oder militärische Abläufe zu beeinträchtigen.
- *Konspiration* bedeutet das geheime Zusammenarbeiten von Personen oder Gruppen zur Planung und Durchführung verdeckter oder illegaler Aktivitäten, oft politischer Natur.

8 Dietrich, J.-H. (2017). Das Recht der Nachrichtendienste [Stand: 31.03.2025].

- *Desinformation* ist der gezielte Einsatz von falschen oder irreführenden Informationen, um Meinungen oder Entscheidungen zu manipulieren. Anders als eine Fehlinformation, die unbeabsichtigt ist, wird Desinformation bewusst verbreitet, um die öffentliche Wahrnehmung zu beeinflussen oder Gegner zu täuschen.
- *Politischer Mord* bezieht sich auf die gezielte Tötung von Personen aus politischen Gründen.

Die *Stasi*, formell als das *Ministerium für Staatssicherheit (MfS)* der *Deutschen Demokratischen Republik (DDR)* bekannt, agierte von 1950 bis 1990 als zentraler Geheimdienst und Geheimpolizei Ostdeutschlands. Als eines der effizientesten und repressivsten Überwachungsorgane, die jemals etabliert wurden, spielte die Stasi eine entscheidende Rolle in der Kontrolle und Unterdrückung jeglicher Opposition innerhalb der DDR. Sie ist gleichzeitig ein Beispiel für einen Geheimdienst und begründet unter anderem das in Deutschland geltende Trennungsgebot.

> Das *Trennungsgebot* ist ein rechtliches Prinzip im deutschen Sicherheitsrecht, das eine klare institutionelle und funktionale Trennung zwischen Polizei und Nachrichtendiensten vorschreibt. Dieses Gebot basiert auf der historischen Erfahrung in Deutschland, insbesondere während der Zeit des Nationalsozialismus, als die Geheimpolizei umfassende Befugnisse sowohl in der Informationsbeschaffung als auch in der Strafverfolgung hatte, was zu schwerwiegenden Menschenrechtsverletzungen führte.

Das Trennungsgebot soll eine zu starke Konzentration von Macht verhindern, indem es sicherstellt, dass die Polizei, die primär für die Verfolgung von Straftaten und die Aufrechterhaltung der öffentlichen Ordnung zuständig ist, und die Nachrichtendienste, deren Hauptaufgabe die Sammlung von Informationen zur Abwehr von Gefahren für die innere und äußere Sicherheit ist, nicht ineinandergreifen.

Das verhindert, dass Informationen, die ohne strafprozessuale Kontrolle gesammelt wurden, direkt in strafrechtliche Ermittlungen einfließen, und schützt somit die Bürgerrechte und die rechtsstaatliche Ordnung.

In der Praxis bedeutet das, dass Nachrichtendienste keine polizeilichen Befugnisse haben, wie etwa das Recht, Personen festzunehmen oder Durchsuchungen durchzuführen. Ebenso dürfen polizeiliche Einheiten nicht die spezifischen Mittel der Nachrichtendienste verwenden. Ausnahmen und spezifische Kooperationen zwischen Polizei und Nachrichtendiensten sind nur unter strengen gesetzlichen Vorgaben und Kontrollen möglich.

Cyberspionage

Nun kommen wir zu der wohl wichtigsten Definition, die auch Namensgeber dieses Buchs ist, nämlich zur Cyberspionage:

> *Cyberspionage* ist eine Form der Spionage, bei der gezielte Cyberangriffe eingesetzt werden, um unautorisierten Zugriff auf sensible oder vertrauliche Daten sowie auf geistiges Eigentum zu erlangen.[9] Ihr Ziel ist es, Informationen aus den Bereichen Politik, Verwaltung, Wirtschaft, Wissenschaft, Technik oder Militär auszuspähen und für strategische oder wirtschaftliche Zwecke zu nutzen.[10]

Zu den Methoden der Cyberspionage gehören unter anderem das Eindringen in Computernetzwerke mittels Hacking, das Ausnutzen von Sicherheitslücken, der Versand von Phishing-E-Mails zur Gewinnung von Zugangsdaten und das Platzieren von Schadsoftware (Malware), die heimlich Daten sammelt und an den Angreifer sendet. All diese Methoden werden von einer bestimmten Berufsgruppe durchgeführt, nämlich IT-Spezialisten bzw. Hackern.

Doch was ist ein *Hacker* eigentlich? Eine Definition stammt aus dem *Jargon File*:

> *»[A Hacker is] A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.«*[11]

Demnach ist ein Hacker jemand, der Systeme verstehen, verbessern oder an ihre Grenzen bringen möchte, und nicht zwingend jemand, der Schaden anrichtet. Entscheidend ist dabei, dass Hacking nicht per se illegal ist, sondern zunächst eine Herangehensweise an Technik beschreibt.

Auch Steven Levy, der den Begriff der *Hackerethik* prägte, beschreibt Hacker nicht primär als Kriminelle, sondern als Teil einer kulturellen und technischen Bewegung:

> *»Hackers believe that essential lessons can be learned about the systems – about the world – from taking things apart, seeing how they work, and using this knowledge to create new and even more interesting things.«*[12]

In Medien wird der Begriff *Hacker* häufig mit Cyberkriminellen gleichgesetzt (dazu komme ich gleich in Abschnitt 1.2.3 noch ausführlich. Fachlich korrekt unterscheidet man jedoch zwischen verschiedenen Arten von Hackern:

- *White Hats* operieren im legalen Bereich. Sie arbeiten z. B. als Pentester, d. h., sie suchen im Auftrag von Unternehmen nach Sicherheitslücken in Systemen, um sie vor Angreifern zu schützen.

9 Edwards, S. (2022, 29. März). Was ist Cyberspionage? CrowdStrike. *https://www.crowdstrike.com/de-de/cybersecurity-1Was%20ist%20Cyberspionage* [Stand: 4. März 2025].

10 Landesamt für Verfassungsschutz Baden-Württemberg. (o. J.). Cyberspionage. Verfassungsschutz Baden-Württemberg. *https://www.verfassungsschutz-bw.de/,Lde/Startseite/Arbeitsfelder/Cyberspionage* [Stand: 4. März 2025].

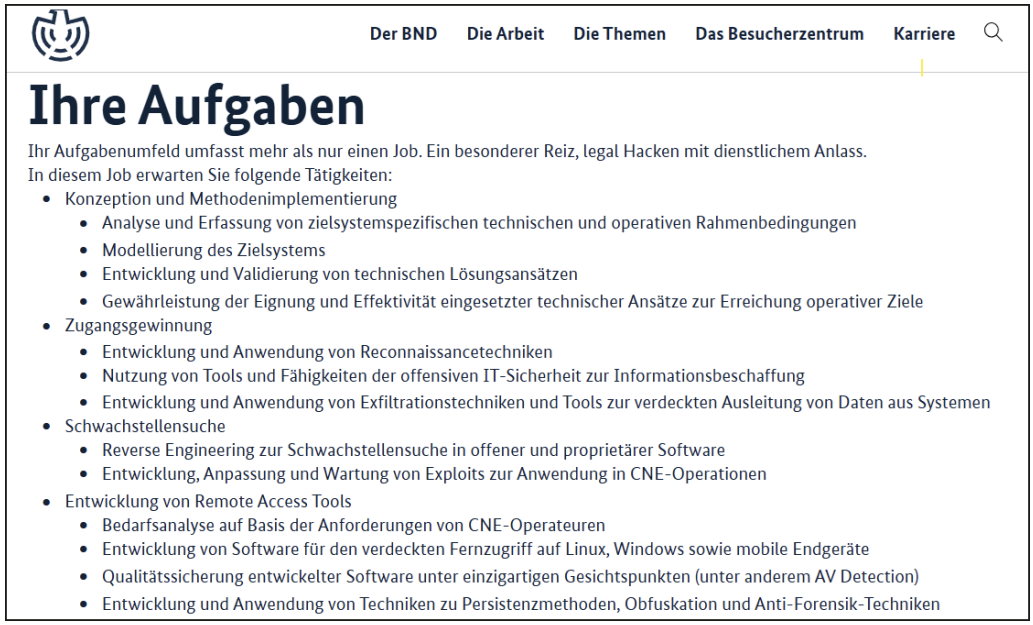
11 Raymond, E. S. (2003). The Jargon File (Version 4.4.7). *http://www.catb.org/jargon/html/H/hacker.html* [Stand: 27.12.2025].

12 Levy, S. (1984). Hackers: Heroes of the computer revolution. Anchor Press/Doubleday.

- *Black Hats* nutzen ihr Wissen hingegen für illegale Zwecke, um z. B. Cyberspionage zu betreiben, fremde Systeme zu sabotieren oder Daten zu stehlen.
- *Gray Hats* bewegen sich zwischen diesen beiden Extremen. Für die Cyberspionage werden in der Regel hochqualifizierte IT-Spezialisten mit offensiven Fähigkeiten eingesetzt, die gezielt technische Sicherheitslücken ausnutzen, Schadsoftware entwickeln oder Social Engineering einsetzen, um ihre Ziele zu erreichen. Dabei setzen sie in den meisten Fällen die gleichen Werkzeuge wie »die Guten« ein.

Auch unsere Nachrichtendienste rekrutieren gezielt Personen mit ausgeprägten technischen Fähigkeiten im Bereich des Hackings. Entsprechende Stellenausschreibungen finden sich offen zugänglich auf den offiziellen Karriereseiten der Behörden, etwa beim Bundesnachrichtendienst.

Bereits diese Transparenz verdeutlicht, dass es sich nicht um illegale Tätigkeiten handelt, sondern um institutionalisierte, rechtlich regulierte Aufgabenfelder innerhalb der staatlichen Sicherheitsarchitektur. In den Ausschreibungen wird der Tätigkeitsbereich typischerweise abstrakt und funktionsorientiert beschrieben, auch um gegnerischen Aufklärungsversuchen durch OSINT-Recherchen etwas entgegenzusetzen. Abbildung 1.1 zeigt ein Beispiel.



Der BND Die Arbeit Die Themen Das Besucherzentrum Karriere

Ihre Aufgaben

Ihr Aufgabenumfeld umfasst mehr als nur einen Job. Ein besonderer Reiz, legal Hacken mit dienstlichem Anlass.
In diesem Job erwarten Sie folgende Tätigkeiten:

- Konzeption und Methodenimplementierung
  - Analyse und Erfassung von zielsystemspezifischen technischen und operativen Rahmenbedingungen
  - Modellierung des Zielsystems
  - Entwicklung und Validierung von technischen Lösungsansätzen
  - Gewährleistung der Eignung und Effektivität eingesetzter technischer Ansätze zur Erreichung operativer Ziele
- Zugangsgewinnung
  - Entwicklung und Anwendung von Reconnaissancetechniken
  - Nutzung von Tools und Fähigkeiten der offensiven IT-Sicherheit zur Informationsbeschaffung
  - Entwicklung und Anwendung von Exfiltrationstechniken und Tools zur verdeckten Ausleitung von Daten aus Systemen
- Schwachstellensuche
  - Reverse Engineering zur Schwachstellensuche in offener und proprietärer Software
  - Entwicklung, Anpassung und Wartung von Exploits zur Anwendung in CNE-Operationen
- Entwicklung von Remote Access Tools
  - Bedarfsanalyse auf Basis der Anforderungen von CNE-Operateuren
  - Entwicklung von Software für den verdeckten Fernzugriff auf Linux, Windows sowie mobile Endgeräte
  - Qualitätssicherung entwickelter Software unter einzigartigen Gesichtspunkten (unter anderem AV Detection)
  - Entwicklung und Anwendung von Techniken zu Persistenzmethoden, Obfuskation und Anti-Forensik-Techniken

Abbildung 1.1: Stellenausschreibung für einen »Hacker« beim BND.
(Quelle: https://www.bnd.bund.de/SharedDocs/Stellenangebote/DE/Stellenangebote/AS-2025-900-enterbnd-hacking-gd.html?nn=11693764 [Stand: 27.12.2025])

Das Vorlesungsvideo zu den Definitionen in der Cyberspionage erreichen Sie über den folgenden Link:

Abbildung 1.2: https://florian-dalwigk.com/cyberspionage/definitionen

Wird der BND bald zum Geheimdienst?

Der Bundesnachrichtendienst (BND) ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und wird umgangssprachlich regelmäßig als »Geheimdienst« bezeichnet. Wie Sie schon wissen, gibt es Unterschiede zwischen Nachrichtendiensten und Geheimdiensten:

- Ein Nachrichtendienst ist primär darauf ausgerichtet, Informationen (»Nachrichten«, engl. *Intelligence*) systematisch zu gewinnen, auszuwerten und der politischen Führung zur Entscheidungsfindung bereitzustellen. Der Fokus liegt auf der Analyse, Bewertung und strategischen Einordnung sicherheitsrelevanter Entwicklungen.
- Ein Geheimdienst hat hingegen aktive Maßnahmenbefugnisse. Dazu zählen unter anderem Sabotage und das Verbreiten von Desinformationen.

Medienberichte über einen Entwurf für ein neues BND-Gesetz, das dem BND in besonderen Lagen weitergehende Befugnisse geben soll, münden in eine politisch und rechtlich kontroversen Frage, nämlich ob der BND im Kern ein Nachrichtendienst bleibt, der Informationen beschafft, auswertet und der Bundesregierung berichtet, oder ob er Kompetenzen bekommt, die ihn zu einem Geheimdienst werden lassen.

In der medialen Berichterstattung rund um vereitelte Anschlagspläne oder akute Gefährdungslagen taucht sinngemäß immer wieder eine Formulierung auf: Man habe »Hinweise« bzw. »Erkenntnisse« von ausländischen Partnerdiensten erhalten. ZDFheute berichtete im Oktober 2024, die Hinweise auf Anschlagspläne gegen die israelische Botschaft in Berlin seien offenbar »mal wieder« von ausländischen Geheimdiensten gekommen.[13]

Dieses Muster zieht sich durch zahlreiche Berichte der vergangenen Jahre. So soll der BND bei der Terrorabwehr stark von ausländischen Geheimdiensten abhängig sein, insbesondere von Mitgliedern der *Five-Eyes-Alliance* (siehe Abschnitt 1.6), und nur ca. zwei

13 Kirsch, S. (21.10.2024). Anschlagsplan in Berlin: Brauchen Geheimdienste mehr Rechte? ZDFheute. *https://www.zdfheute.de/politik/deutschland/geheimdienste-spionage-buerokratie-rechtlicher-rahmen-100.html* [Stand: 11.01.2026].

Prozent der Hinweise selbst liefern.[14] Als Gründe für die geringe Eigenleistung sieht ein hochrangiges Regierungsmitglied gesetzliche Beschränkungen, wie beispielsweise das Verbot, KI-Tools für die Auswertung zu nutzen, sowie die Pflicht, deutsche Kommunikationsdaten sofort löschen zu müssen.[15]

Die aktuellen Reformüberlegungen sehen vor, den BND deutlich stärker in die sicherheitspolitische Handlungsfähigkeit des Staates einzubinden, da Cyberangriffe, Sabotageakte, verdeckte Einflussoperationen und hybride Kriegsführung mittlerweile den Alltag prägen. Konkret geht es um Pläne, dem BND in klar definierten Ausnahmesituationen auch aktive Eingriffsbefugnisse zu erlauben. Dazu zählen insbesondere Sabotagehandlungen sowie offensive Cyberoperationen gegen gegnerische Infrastruktur.

Diese Maßnahmen sollen es ermöglichen, Bedrohungen nicht nur zu erkennen, sondern die gegnerischen Fähigkeiten gezielt zu stören oder zu schwächen, z. B., wenn von ihnen erhebliche Gefahren für die Sicherheit Deutschlands ausgehen.[16] Das könnte beispielsweise einen Gegenschlag im Falle eines Cyberangriffs bedeuten[17], was bisher in dieser Form rechtlich so nicht möglich war. Man spricht vom *Hackback*.

Die vorgesehenen aktiven Maßnahmen sollen nicht eigenständig durch den BND ausgelöst werden, sondern an eine formale politische Entscheidung gebunden sein. Voraussetzung wäre demnach das Vorliegen einer »nachrichtendienstlichen Sonderlage«. Diese Sonderlage soll vom *Nationalen Sicherheitsrat* festgestellt werden. Zusätzlich dazu soll die Feststellung erst wirksam werden, wenn zwei Drittel der Mitglieder des *Parlamentarischen Kontrollgremiums (PKGr)* im Bundestag zustimmen. Die Einbindung des PKGr wäre dabei ein Novum, weil das Gremium bislang primär kontrolliert, aber nicht als Zustimmungsinstanz für operative Maßnahmen vorgesehen ist.[18]

Bislang ist der BND rechtlich klar als Nachrichtendienst konzipiert, dessen Kernaufgabe in der Informationsgewinnung, -auswertung und -weitergabe an die Bundesregierung liegt. Würden ihm in Ausnahmefällen aktive Eingriffsbefugnisse wie Sabotage oder offen-

14 Solms-Laubach, F. (09.01.2026). Nur so kann uns der BND vor Terror besser schützen. BILD.de. *https://www.bild.de/politik/inland/nur-so-kann-uns-der-bnd-vor-terror-besser-schuetzen-695f87304d1d5f581eeafa02* [Stand: 11.01.2026].

15 Tagesspiegel.de. (08.01.2026). Große Abhängigkeit von USA: Nur zwei Prozent der Terror-Hinweise kommen offenbar vom BND selbst. *https://www.tagesspiegel.de/politik/weitreichende-abhangigkeit-von-partnern-nur-zwei-prozent-der-terror-warnungen-kommen-offenbar-vom-bnd-15114069.html* [Stand: 11.01.2026].

16 ZEIT Online. (19.12.2025). Geheimdienste: Bundesnachrichtendienst soll offenbar mehr Befugnisse bekommen. *https://www.zeit.de/politik/deutschland/2025-12/bnd-soll-mehr-befugnisse-bekommen-sabotage-cyberangriffe-gxe* [Stand: 11.01.2026].

17 n-tv.de. (19.12.2025). BND soll Cyberattacken gegen Waffensysteme starten dürfen. *https://www.n-tv.de/politik/BND-soll-Cyberattacken-gegen-Waffensysteme-starten-duerfen-id30161847.html* [Stand: 11.01.2026].

18 ZDFheute. (19.12.2025). Kanzleramt plant mehr Befugnisse für den BND. *https://www.zdfheute.de/politik/kanzleramt-bnd-nachrichtendienst-mehr-befugnisse-100.html* [Stand: 11.01.2026].

sive Cyberoperationen übertragen, könnte diese Trennung an Klarheit verlieren. Der BND würde in diesen Fällen Elemente eines klassischen Geheimdienstes übernehmen.

Das könnte zur Folge haben, dass die bislang geltende Differenzierung zwischen nachrichtendienstlicher Aufklärung und exekutivem bzw. militärischem Handeln aufgeweicht würde. Langfristig könnte die Gefahr einer schleichenden Normalisierung aktiver Maßnahmen bestehen, selbst wenn diese formell an hohe Hürden geknüpft bleiben.

Offensive Cybermaßnahmen können je nach Intensität als Verletzung der Souveränität anderer Staaten oder sogar als bewaffneter Angriff gewertet werden. Deutschland müsste sich darauf einstellen, dass solche Handlungen Eskalationsspiralen auslösen können. Hinzu kommt, man sich potenziell selbst stärker zur Zielscheibe macht. Aktive Sabotage- oder Cyberoperationen könnten nämlich dazu führen, dass Deutschland von gegnerischen Staaten noch stärker als operativer Gegner eingeordnet wird. Das würde das Risiko von Vergeltungsmaßnahmen erhöhen, insbesondere im Cyberraum, wo die Attribution (siehe Kapitel 6) sehr schwierig ist und Reaktionen niedrigschwellig erfolgen können. Kritische Infrastrukturen, staatliche Netze oder auch private Unternehmen mit Bezug zu Deutschland könnten dadurch noch stärker ins Visier geraten. Zudem könnte das Risiko wachsen, dass Cyberoperationen, die bislang als Handlungen nichtstaatlicher Akteure eingeordnet würden, künftig als staatlich verantwortete Maßnahmen interpretiert werden.

Sicherheitspolitisch könnten die Reformen die Handlungsfähigkeit Deutschlands erhöhen. In hybriden Bedrohungslagen, wie beispielsweise bei massiven Cyberangriffen auf kritische Infrastrukturen, wäre der Staat nicht mehr ausschließlich auf defensive Maßnahmen angewiesen. Nicht zuletzt hätte eine solche Neuausrichtung auch außenpolitische Folgen. Partnerdienste sehen einen handlungsfähigeren BND möglicherweise als Gewinn, insbesondere wenn Deutschland nicht mehr überwiegend auf fremde Hinweise angewiesen ist.

Frage #002: Wie viel Geheimdienst darf ein Nachrichtendienst sein?

Frage #003: Macht ein offensiv handelnder BND Deutschland sicherer oder angreifbarer?

Frage #004: Wo verläuft die Grenze zwischen legitimer Gefahrenabwehr und völkerrechtlich problematischer Machtausübung im Cyberraum?

1.2.3 Cyberspionage vs. Cyberkriminalität

Unser Leben wird immer digitaler, und die Grenze zwischen dem »analogen Leben« und der Welt des Cyberspace verschwimmt immer mehr. Smartphones sind unsere ständigen Begleiter, Daten werden digital ausgetauscht, man ist immer online. Daher nimmt auch die Bedrohung durch Angriffe im Cyberraum zu. Lassen Sie uns dabei zwei Phänomene unterscheiden: *Cyberkriminalität* und *Cyberspionage*. Obwohl beide Begriffe im öffentlichen Diskurs oft synonym oder unscharf verwendet werden, unterscheiden sie sich grundlegend in ihrer Zielsetzung und Struktur:

- Das BKA definiert *Cyberkriminalität* im engeren Sinne als Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten. Dazu zählen beispielsweise das Ausspähen von Daten, Computersabotage und Phishing-Angriffe.[19] Im weiteren Sinne umfasst Cyberkriminalität auch Straftaten, bei denen das Internet oder IT-Systeme als Tatmittel genutzt werden, etwa für Betrugshandlungen oder zur Verbreitung illegaler Inhalte. Sie können sich also merken:
  - Cyberkriminalität im weiteren Sinne sind Angriffe *mit* IT.
  - Cyberkriminalität im engeren Sinne sind Angriffe *auf* IT.
- *Cyberspionage* ist eine Form der Spionage, bei der gezielte Cyberangriffe eingesetzt werden, um unautorisierten Zugriff auf sensible oder vertrauliche Daten sowie auf geistiges Eigentum zu erlangen.[20] Ihr Ziel ist es, Informationen aus den Bereichen Politik, Verwaltung, Wirtschaft, Wissenschaft, Technik oder Militär auszuspähen und für strategische oder wirtschaftliche Zwecke zu nutzen.[21]

Cyberkriminalität und Cyberspionage unterscheiden sich trotz teilweise ähnlicher technischer Mittel grundlegend in ihrer *Motivation*, in den beteiligten *Akteuren*, in den *Zielen* sowie in den eingesetzten *Methoden*. Während Cyberkriminalität in erster Linie auf finanzielle Bereicherung oder persönliche Vorteile abzielt, steht bei der Cyberspionage die politische, wirtschaftliche oder militärische Informationsgewinnung im Vordergrund. Es geht hier nicht um unmittelbaren Profit, sondern um strategische Vorteile und langfristige Erkenntnisse.

Die Akteure

Auch die Akteure unterscheiden sich deutlich. Cyberkriminelle agieren häufig als Einzelpersonen oder in organisierten kriminellen Gruppen, deren Strukturen flexibel und vor allem gewinnorientiert sind. Cyberspionage hingegen wird überwiegend von Staaten betrieben oder zumindest staatlich unterstützt. Nachrichtendienste und *Advanced Persistent Threats (APTs)* handeln dabei im staatlichen Auftrag oder mit staatlicher Duldung und verfügen in der Regel über deutlich größere Ressourcen.

Die Ziele

Entsprechend variieren auch die Ziele der Angriffe. Cyberkriminalität richtet sich vor allem gegen Privatpersonen, Unternehmen und Finanzinstitute, bei denen sich Geld oder

19 Bundeskriminalamt (BKA). (2017). Bundeslagebild Cybercrime 2016. Wiesbaden: Bundeskriminalamt. Abgerufen von *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html* [Stand: 01.05.2025].

20 Edwards, S. (2022, 29. März). Was ist Cyberspionage? CrowdStrike. *https://www.crowdstrike.com/de-de/cybersecurity-1Was%20ist%20Cyberspionage* [Stand: 4. März 2025].

21 Landesamt für Verfassungsschutz Baden-Württemberg. (o. J.). Cyberspionage. Verfassungsschutz Baden-Württemberg. *https://www.verfassungsschutz-bw.de/,Lde/Startseite/Arbeitsfelder/Cyberspionage* [Stand: 4. März 2025].

verwertbare Daten unmittelbar monetarisieren lassen. Cyberspionage zielt dagegen auf Regierungen, Forschungseinrichtungen, kritische Infrastrukturen sowie Unternehmen im sicherheitsrelevanten Umfeld. Im Fokus stehen hier sensible Informationen, technologische Entwicklungen oder politische Entscheidungsprozesse.

Die Methoden

Trotz dieser Unterschiede überschneiden sich die eingesetzten Methoden. Cyberkriminelle nutzen häufig Phishing-Kampagnen, Ransomware[22] oder Identitätsdiebstahl, um schnell und effizient Gewinne zu erzielen. In der Cyberspionage kommen dagegen gezieltere und oft aufwendigere Techniken zum Einsatz, etwa *Spear-Phishing*, maßgeschneiderte *Trojaner* oder bislang unbekannte Sicherheitslücken (*Zero-Day-Exploits*). Diese Methoden sind auf verdeckte, langfristige Informationsbeschaffung ausgelegt.

Manchmal versuchen staatliche Akteure, die Cyberspionage betreiben wollen, ihr Handeln wie Cyberkriminalität erscheinen zu lassen. So kann beispielsweise Ransomware als Deckmantel für Cyberspionage dienen. Sie kann genutzt werden, um von tiefergehenden Spionageaktivitäten abzulenken. Die öffentliche Aufmerksamkeit richtet sich auf die Lösegeldforderung, während im Hintergrund sensible Daten exfiltriert werden. Bei einer *Double-Extortion-Strategie*, drohen die Angreifer zusätzlich zur Verschlüsselung der Daten mit deren Veröffentlichung, falls kein Lösegeld gezahlt wird. Die kopierten Daten können aber auch für geheimdienstliche Zwecke verwendet werden, was den Angriff in den Bereich der Cyberspionage verschiebt. APT-Gruppen setzen gezielt Ransomware ein, um sowohl finanzielle Mittel zu generieren als auch nachrichtendienstliche Informationen zu gewinnen.

Die Gruppe *Lazarus* aus Nordkorea wird beispielsweise mit Ransomware-Angriffen in Verbindung gebracht, deren Lösegelder in die Finanzierung des nordkoreanischen Regimes fließen.

Und auch die beiden Malware-Programme *Petya* und *NotPetya* zeigen, wie Ransomware mit Cyberspionage verbunden sein kann. Während beide Schadprogramme von der Funktionsweise her ähnlich wirken, unterscheiden sie sich grundlegend in ihrer Intention, technischen Ausführung und geopolitischen Einbettung. Die ursprüngliche Petya-Ransomware war klassisch finanziell motiviert und steht damit nicht in direkter Verbindung zur Spionage.

NotPetya tarnte sich als Ransomware, hatte jedoch keine technische Möglichkeit zur Datenwiederherstellung. Diese Eigenschaft weist darauf hin, dass es sich nicht um echte Ransomware, sondern um eine *Wiper-Malware* handelte, also um Schadsoftware, deren

22 Ransomware ist eine Schadsoftware, die Daten auf einem Computer oder in einem Netzwerk verschlüsselt oder den Zugriff darauf sperrt. Die Angreifer fordern anschließend ein Lösegeld, meist in Kryptowährungen, um die Daten wieder freizugeben.

Ziel die Zerstörung von Daten ist. Die Cyberattacke traf insbesondere ukrainische Regierungsstellen, Banken, Flughäfen und Energieversorger, breitete sich aber auch weltweit aus.

Laut NATO und mehreren westlichen Geheimdiensten war NotPetya Teil eines größeren geopolitischen Informationskriegs, insbesondere im Kontext des russisch-ukrainischen Konflikts. NotPetya zeigt, wie Ransomware-ähnliche Mechanismen genutzt werden können, um Sabotageaktionen oder Spionageoperationen zu verschleiern.

1.3 Der Geheimdienstzyklus

Der *Geheimdienstzyklus* beschreibt, wie aus einem Informationsbedarf von Nachrichten- und Geheimdiensten systematisch verwertbare Lagebilder und Entscheidungsgrundlagen entstehen. Seine Wurzeln reichen bis in die Mitte des 20. Jahrhunderts zurück.

Besonders prägend war dabei die Arbeit von Sherman Kent, der als einer der Begründer der modernen Intelligence Studies gilt.[23] In seinem Werk »Strategic Intelligence for American World Policy« formulierte er erstmals, dass Nachrichtendienstarbeit als zyklischer, wiederkehrender Prozess zu verstehen ist, der Planung, Sammlung, Auswertung und Rückkopplung umfasst (siehe Abbildung 1.3).[24] Dieses Modell wurde später insbesondere durch die CIA weiter standardisiert.[25]

Planning & Direction

Der Zyklus beginnt mit der Phase *Planning & Direction*. Darin formulieren politische, militärische oder sicherheitsbehördliche Entscheidungsträger konkrete *Intelligence Requirements*, also nachrichtendienstliche Anforderungen bzw. Fragestellungen. Diese können auf unterschiedlichen Ebenen angesiedelt sein:

- *strategisch*, z. B. bei der Einschätzung langfristiger geopolitischer Ziele rivalisierender Staaten
- *taktisch*, z. B. bei der Lokalisierung feindlicher Einheiten oder Terrorzellen
- *technisch*, z. B. bei der Analyse neuer Cyberwaffen

Diese Anforderungen bestimmen, was gesammelt wird und mit welcher Priorität dies geschieht.

23 Davis, J. (2002). Sherman Kent and the profession of intelligence analysis (Occasional Papers: Vol. 1, No. 5). Central Intelligence Agency. *https://www.cia.gov/resources/csi/static/Kent-Profession-Intel-Analysis.pdf* [Stand: 27.12.2025].

24 Kent, S. (1966). Strategic intelligence for American world policy. Princeton University Press.

25 Central Intelligence Agency. (o. J.). The intelligence cycle [PDF]. CIA. *https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf* [Stand: 27.12.2025].

Collection

Darauf folgt die Phase der *Collection*, also der eigentlichen Informationsbeschaffung. Hier kommen je nach Fragestellung unterschiedliche Spionagetechniken (siehe Abschnitt 1.4.3) zum Einsatz, darunter *Open Source Intelligence* (OSINT), *Human Intelligence* (HUMINT), *Signals Intelligence* (SIGINT), *Imagery Intelligence* (IMINT) oder *Measurement and Signature Intelligence* (MASINT). Das Ziel dieser Phase ist die möglichst vollständige Sammlung relevanter Rohdaten, unabhängig davon, ob diese bereits unmittelbar verständlich oder nutzbar sind.

Processing & Exploitation

In der Phase *Processing & Exploitation* werden die gesammelten Rohdaten technisch und organisatorisch aufbereitet. Dazu gehören unter anderem die Übersetzung fremdsprachlicher Inhalte, die Entschlüsselung oder Dekodierung abgefangener Kommunikation sowie das Filtern, Strukturieren und Zusammenführen heterogener Datenquellen. Hierbei spielen automatisierte Verfahren und Big-Data-Analysen eine zentrale Rolle, um z. B. Muster in großen Datenmengen zu erkennen oder Anomalien wie verdächtige Finanzströme zu identifizieren.

Analysis & Production

Anschließend folgt der Kern nachrichtendienstlicher Arbeit, nämlich die *Analysis & Production*. Darin werden die verarbeiteten Informationen analytisch bewertet, kontextualisiert und interpretiert. Das Ziel ist es, nicht nur zu beschreiben, was passiert ist, sondern auch zu erklären, warum es passiert ist, und abzuschätzen, was wahrscheinlich als Nächstes geschehen wird. Entsprechend unterscheidet man deskriptive, kausale und prädiktive Analysen. Die Ergebnisse sind z. B. Lagebilder oder Bedrohungsanalysen.

Dissemination & Feedback

Den Abschluss bildet die Phase *Dissemination & Feedback*. Die gewonnenen Erkenntnisse werden den jeweiligen Entscheidungsträgern in geeigneter Form zur Verfügung gestellt, z. B. als regelmäßige Lageberichte, akute Krisenanalysen oder langfristige strategische Einschätzungen.

Gleichzeitig fließt Feedback von den Empfängern der Analyseergebnisse, in Deutschland also z. B. von der Bundesregierung, zurück in den Prozess und führt zu neuen *Intelligence Requirements*, womit der Zyklus von Neuem beginnt (siehe Abbildung 1.3).

Eine Herausforderung für Geheimdienste ist es, korrekte Schlussfolgerungen zu formulieren und diese so zu vermitteln, dass Entscheidungsträger keine fehlerhaften Rückschlüsse ziehen (*Intelligence Bias*). Die Fehleinschätzung über Massenvernichtungswaffen im Irak 2003 beruhte beispielsweise auf ungenauen und teils schlicht falschen HUMINT-Berichten. Analysten neigen dazu, Informationen auszuwählen, die ihre bestehende Hypothese bestätigen (*Conformation Bias*), oder sogar nur aktiv nach Quellen zu suchen, die ihre Meinung bestätigen.

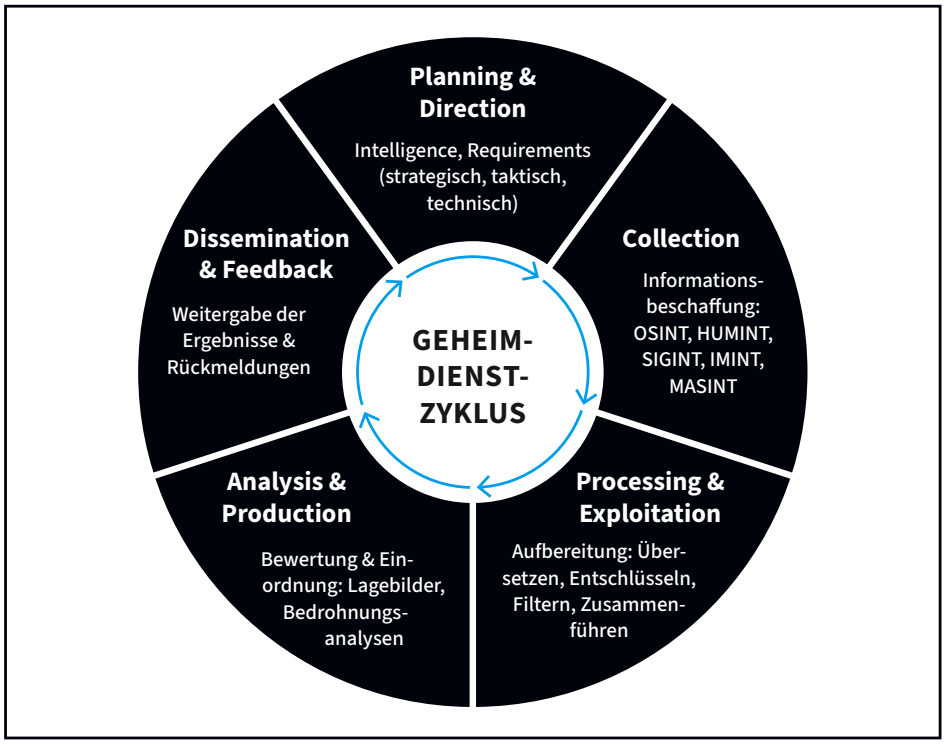


Abbildung 1.3: Die fünf Phasen des Geheimdienstzyklus

Und wenn man fälschlicherweise annimmt, dass gegnerische Staaten nach denselben rationalen Prinzipien handeln wie man selbst, dann spricht man von *Mirror Imaging*.

Das Vorlesungsvideo zum Geheimdienstzyklus erreichen Sie über den folgenden Link:

Abbildung 1.4: https://florian-dalwigk.com/cyberspionage/geheimdienstzyklus

1.4 Deutschland, deine Nachrichtendienste

In diesem Kapitel beschäftigen wir uns mit den Nachrichtendiensten, die es in Deutschland gibt. Deren hohe Anzahl wird Sie vermutlich überraschen. Deutschland hat nämlich insgesamt 19 Nachrichtendienste. Davon befinden sich drei auf Bundesebene und 16 auf Landesebene.

Auf *Bundesebene* gibt es drei Nachrichtendienste:

- Bundesnachrichtendienst (BND)
- Bundesamt für Verfassungsschutz (BfV)
- Bundesamt für den Militärischen Abschirmdienst (MAD)

Auf *Landesebene* gibt es jeweils ein Landesamt für Verfassungsschutz (LfV). Es gibt also das *LfV Bayern*, *LfV Niedersachsen* usw. Diese Struktur hat historische und verfassungsrechtliche Gründe, die eng mit dem föderalen System Deutschlands verbunden sind: Nach dem Zweiten Weltkrieg wurde Deutschland in verschiedene Besatzungszonen aufgeteilt, und es wurde vermieden, zentralisierte Machtstrukturen zu etablieren, um den Wiederaufbau eines autoritären Regimes zu verhindern. Die Gründung der Bundesrepublik Deutschland führte zur Schaffung eines föderalen Staates, in dem die einzelnen Bundesländer über eigene Regierungen und Verwaltungsstrukturen verfügen. Und das schließt auch eigene Verfassungsschutzbehörden ein.

Wir werden uns in diesem Abschnitt vor allem mit den Nachrichtendiensten auf Bundesebene beschäftigen.

1.4.1 Bundesnachrichtendienst (BND)

Der *Bundesnachrichtendienst (BND)* ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland. Er ist dem *Bundeskanzleramt (BkAmt)* unterstellt und gehört zu den drei Nachrichtendiensten des Bundes. Der BND ist für die Sammlung und Auswertung von Informationen über das Ausland zuständig, die für die Sicherheit Deutschlands von Bedeutung sind. Er soll die Bundesrepublik vor äußeren Gefahren schützen und zur politischen und sicherheitspolitischen Entscheidungsfindung der Bundesregierung beitragen.

Der Ursprung des BND liegt in der *Organisation Gehlen*, die nach dem Zweiten Weltkrieg von Reinhard Gehlen, dem ehemaligen Leiter der Wehrmachts-Aufklärung Ost, gegründet wurde. Gehlen arbeitete zunächst mit der US-amerikanischen Besatzungsmacht zusammen. Die Organisation war ein früher westdeutscher Geheimdienst zur Spionage gegen die Sowjetunion im Kalten Krieg. Am 1. April 1956 wurde der BND offiziell als Bundesnachrichtendienst gegründet. Er übernahm die Aufgaben der Organisation Gehlen und wurde ein eigenständiger Dienst innerhalb der neu gegründeten Bundesrepublik Deutschland.

Der BND beschäftigt heute (2026) ca. 6.500 Mitarbeiter, die sich in viele verschiedene Berufsgruppen unterteilen.

Der BND sammelt unter anderem Informationen über Terrorismus, politische Entwicklungen weltweit, Proliferation und auch zur organisierten Kriminalität. Diese Informationen stammen aus verschiedenen Quellen, die wir noch genauer besprechen werden. Das *Auftragsprofil der Bundesregierung (APB)* legt fest, welche Themen, Regionen oder Gefah-

renlagen für die Bundesregierung von besonderem Interesse sind, sodass der BND zu ihnen gezielt Informationen beschaffen und auswerten soll. Das APB ist der »Arbeitsauftrag« der Bundesregierung an den BND und wird als STRENG GEHEIM eingestuft.

Bis 2022 gliederte sich der BND in elf verschiedene Abteilungen, darunter z. B. Eigensicherung (SI), Informationstechnik (IT) und Technische Aufklärung (TA). Nach einer Umstrukturierung des BND gibt es die folgenden sechs Bereiche, unter denen es verschiedene Direktorate, Referate und Sachgebiete gibt: *Auswertung*, *Beschaffung*, *Nachrichtendienstliche Fähigkeiten*, *IT-Unterstützung*, *Zentrale Unterstützungsaufgaben* sowie *Innovative Technologien, Forschung und Ausbildung*.

Die zentrale Liegenschaft des BND befindet sich in der Chausseestraße 96, 10115 Berlin-Mitte. Vor 2019 befand sich die zentrale Liegenschaft in der Heilmannstraße 30, 82049 Pullach. Diesen Standort kennt man auch unter der Bezeichnung *Camp Nikolaus*. Der BND unterhält viele offizielle Standorte, die mit der Transparenzoffensive 2014 der Öffentlichkeit bekannt gegeben wurden, darunter z. B. Bad Aibling, Gablingen, Rheinhausen, Schöningen, Starnberg-Söcking und Gauting (Stockdorf). Früher verwendete der BND für seine Außenstellen verschiedene Tarnbezeichnungen, wie beispielsweise *Ionosphäreninstitut* (Rheinhausen). Wenn man als Bundeswehrangehöriger zum BND versetzt wird, erfolgt dies über die Tarnbezeichnung *Amt für Militärkunde (AMK)*.

Gesetzliche Grundlagen

Es gibt eine Reihe von Gesetzen, die zur Kontrolle des BND dienen:

- Das *Gesetz über den Bundesnachrichtendienst (BNDG)* regelt Aufgaben, Befugnisse und Schranken des BND sowie die Datenverarbeitung und Zusammenarbeit mit anderen Stellen.
- Im Grundgesetz sind vor allem *Art. 10 GG* (Schutz des Brief-, Post- und Fernmeldegeheimnisses) und *Art. 73 GG Nr. 1* (Ausschließliche Gesetzgebungskompetenz des Bundes für die auswärtigen Angelegenheiten) relevant.
- Daran knüpft das *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz)* an. Es ermöglicht unter strengen Voraussetzungen Überwachungsmaßnahmen bei Gefahren für die Sicherheit Deutschlands.
- Das *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)* regelt die Kontrolle der Nachrichtendienste durch das Parlamentarische Kontrollgremium (PKGr) des Bundestags.
- Das *Bundesdatenschutzgesetz (BDSG)* sichert den Schutz personenbezogener Daten, auch im Bereich der Nachrichtendienste. Dies wird durch den *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)* kontrolliert.
- Das *Bundesverfassungsschutzgesetz (BVerfSchG)* ist bei der Zusammenarbeit mit dem BfV, insbesondere bei gemeinsamer Aufgabenerfüllung, relevant.

- Das *Sicherheitsüberprüfungsgesetz (SÜG)* regelt die Sicherheitsüberprüfungen von Personen, die beim BND arbeiten oder Zugang zu Verschlusssachen haben.
- Der *Bundesrechnungshof (BRH)* übt die Finanzkontrolle über den BND aus und unterrichtet unter anderem das PKGr.

Die Details dieser Gesetze sind natürlich nur für Juristen und Justiziare interessant. Mitnehmen sollten Sie, dass nachrichtendienstliche Arbeit in Deutschland nicht im rechtsfreien Raum geschieht, sondern vom Gesetzgeber reglementiert wird. Die Dienste dürfen nicht tun, was sie wollen, auch nicht im Cyberspace.

Abbildung 1.5: https://florian-dalwigk.com/cyberspionage/bnd

1.4.2 Bundesamt für Verfassungsschutz (BfV)

Das *Bundesamt für Verfassungsschutz (BfV)* ist der Inlandsnachrichtendienst der Bundesrepublik Deutschland. Es ist dem *Bundesministerium des Innern und für Heimat (BMI)* unterstellt. Das BfV ist für die Sammlung und Auswertung von Informationen über verfassungsfeindliche Bestrebungen und sicherheitsgefährdende Aktivitäten im Inland zuständig. Es soll die freiheitlich-demokratische Grundordnung schützen, Extremismus und Spionage abwehren sowie die Bundesregierung bei sicherheitspolitischen Entscheidungen unterstützen.

Gegründet wurde das BfV am 7. November 1950, zunächst mit Sitz in West-Berlin, später in Köln Chorweiler. Es ging organisatorisch aus dem sogenannten *Amt für Verfassungsschutz* hervor, das unter alliierter Aufsicht stand. Mit dem Aufbau des BfV wurde eine zentrale Behörde geschaffen, um die junge Bundesrepublik gegen Bedrohungen durch extremistische Gruppierungen sowie gegen nachrichtendienstliche Tätigkeiten fremder Staaten zu schützen. Im Jahr 2024 beschäftigte das BfV ca. 4.500 Mitarbeiter. Neben dem Bundesamt für Verfassungsschutz gibt es in jedem Bundesland ein eigenständiges *Landesamt für Verfassungsschutz (LfV)*, das in föderaler Struktur mit dem BfV kooperiert. Diese Zusammenarbeit erfolgt im sogenannten *Verfassungsschutzverbund*.

Das BfV sammelt insbesondere Informationen über Linksextremismus, Linksterrorismus, Rechtsextremismus, Rechtsterrorismus, islamistischen Extremismus und Terrorismus, Spionage und Spionageabwehr, Cyberangriffe auf kritische Infrastrukturen sowie über verfassungsfeindliche Bestrebungen innerhalb sogenannter Reichsbürger- oder Delegitimierer-Szenen. Dabei kommen verschiedene nachrichtendienstliche Mittel zum Einsatz,

wie die Observation oder der Einsatz von V-Leuten. Die Erkenntnisse dienen unter anderem zur Frühwarnung, zur Beratung von Politik und Behörden sowie zur Aufklärung der Öffentlichkeit, z. B. durch den jährlich erscheinenden *Verfassungsschutzbericht*, den Sie sich unter dem folgenden Link herunterladen können:

https://www.verfassungsschutz.de/DE/service/publikationen/publikationen_node.html[26]

Die Zentrale des BfV befindet sich in der Merianstraße 100, 50765 Köln-Chorweiler. Daneben gibt es Verbindungsbeamte in den Bundesländern sowie technische und operative Standorte, deren genaue Adressen aus Sicherheitsgründen nicht öffentlich bekannt sind.

Gesetzliche Grundlagen

Es gibt eine Reihe von Gesetzen, die zur Kontrolle des BfV dienen:

- Das *Bundesverfassungsschutzgesetz (BVerfSchG)* regelt die Aufgaben, Befugnisse, Beobachtungsobjekte und die Zusammenarbeit mit anderen Behörden.
- Das Grundgesetz, vor allem *Art. 10 GG* (Schutz des Fernmeldegeheimnisses) und *Art. 20 GG* (wehrhafte Demokratie), bildet die verfassungsrechtliche Basis der Tätigkeit.
- Das *Artikel-10-Gesetz* erlaubt unter bestimmten Voraussetzungen Überwachungsmaßnahmen durch das BfV, insbesondere bei Gefahren für die freiheitlich-demokratische Grundordnung.
- Das *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)* sieht eine Kontrolle durch das PKGr des Bundestags vor.
- Das *Bundesdatenschutzgesetz (BDSG)* gewährleistet auch beim BfV den Schutz personenbezogener Daten. Dies wird durch den *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)* kontrolliert.
- Das *Sicherheitsüberprüfungsgesetz (SÜG)* regelt die Sicherheitsüberprüfungen für Bedienstete mit Zugang zu geheimhaltungsbedürftigen Informationen im BfV.
- Der *Bundesrechnungshof (BRH)* übt die Finanzkontrolle über das BfV aus und unterrichtet unter anderem das PKGr und das BMI über das Ergebnis seiner Prüfung.

Das Vorlesungsvideo zum Bundesamt für Verfassungsschutz erreichen Sie über den folgenden Link:

Abbildung 1.6: https://florian-dalwigk.com/cyberspionage/bfv

26 Geben Sie in das Suchfeld »Verfassungsschutzbericht« ein.

1.4.3 Bundesamt für den Militärischen Abschirmdienst (MAD)

Der *Militärische Abschirmdienst (MAD)* ist Deutschlands militärischer Nachrichtendienst. Er ist dem *Bundesministerium der Verteidigung (BMVg)* unterstellt und Teil der Bundeswehr. Der MAD hat die Aufgabe, sicherheitsgefährdende oder geheimdienstliche Tätigkeiten gegen die Bundeswehr abzuwehren. Er schützt somit die Streitkräfte vor Spionage, Extremismus, Sabotage und Terrorismus und trägt zur Sicherheit der Bundeswehr bei.

Der MAD konzentriert sich auf sicherheitsrelevante Vorgänge innerhalb der Bundeswehr und ist nicht für das Ausland zuständig. Das bleibt Aufgabe des *BND*. Ebenso wenig ist der MAD für die allgemeine innere Sicherheit in Deutschland verantwortlich. Diese fällt unter anderem in den Zuständigkeitsbereich des *BfV*.

Gegründet wurde der MAD im gleichen Jahr wie der BND, nämlich 1956 am 30. Januar. Seine Ursprünge reichen zurück in die frühe Phase der Bundeswehr und in nachrichtendienstliche Strukturen, die während des Kalten Krieges aufgebaut wurden. Heute (2026) beschäftigt der MAD rund 1.500 Mitarbeiterinnen und Mitarbeiter an mehreren Standorten in Deutschland.

Der MAD sammelt insbesondere Informationen zu extremistischen Bestrebungen innerhalb der Bundeswehr (z. B. Linksextremismus, Rechtsextremismus und Islamismus), zu Spionage- und Sabotageaktivitäten gegen militärische Einrichtungen, zu Versuchen ausländischer Geheimdienste, Einfluss auf die Bundeswehr zu nehmen, sowie Informationen zu sicherheitsgefährdenden Personen oder Vorfällen innerhalb der Bundeswehr.

Ein besonderes Augenmerk liegt dabei auf dem Personenschutz in der Truppe, auf der Sicherheitsüberprüfung von Soldaten sowie auf dem Schutz sensibler Informationen und militärischer Infrastruktur. Die Sicherheitsüberprüfungen für Bundeswehrangehörige erfolgen auf Grundlage des Sicherheitsüberprüfungsgesetzes (SÜG).

Der MAD gliedert sich in verschiedene Fachabteilungen und ist bundesweit in zwölf MAD-Stellen vertreten, darunter beispielsweise in Köln (Zentrale), Kiel, Hannover, München und Leipzig. Die Zentrale des MAD befindet sich im *MAD-Zentrum* auf dem Gelände der Luftwaffenkaserne Köln-Wahn in der Brühler Str. 300, 50968 Köln.

Gesetzliche Grundlagen

Es gibt eine Reihe von Gesetzen, die zur Kontrolle des MAD dienen:

- Die rechtliche Grundlage für die Tätigkeit des MAD bildet das *Gesetz über den Militärischen Abschirmdienst (MADG)*. Dieses Gesetz definiert die Aufgaben, Befugnisse und Grenzen des MAD und regelt seine Zusammenarbeit mit anderen Behörden. Das *BMVg* führt die Fachaufsicht über den MAD. Dabei überprüft es die Einhaltung gesetzlicher Vorgaben und dienstlicher Weisungen und stellt sicher, dass der MAD seine Aufgaben ordnungsgemäß erfüllt.

- Das *Bundesdatenschutzgesetz (BDSG)* gewährleistet den Schutz personenbezogener Daten. Dies wird durch den *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)* kontrolliert.
- Für Maßnahmen, die Eingriffe in das Brief-, Post- und Fernmeldegeheimnis betreffen, benötigt der MAD die Genehmigung der *G10-Kommission*. Diese prüft und genehmigt solche Maßnahmen gemäß dem *Artikel-10-Gesetz*.
- Das *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)* sieht eine Kontrolle durch das Parlamentarische Kontrollgremium (PKGr) des Bundestags vor.

In seiner Struktur gliedert sich der MAD in verschiedene Abteilungen, die spezifische Aufgabenbereiche abdecken. Diese umfassen unter anderem die Abteilungen für Spionageabwehr, Extremismusabwehr und technische Aufklärung.

Das Vorlesungsvideo zum Bundesamt für Verfassungsschutz erreichen Sie über den folgenden Link:

Abbildung 1.7: https://florian-dalwigk.com/cyberspionage/mad

1.5 Wie wird man (in Deutschland) Spion bzw. Spionin?

Die Vorstellung vom »Spion« ist bis heute stark von historischen Narrativen, Literatur und Film geprägt. Lange Zeit galt der Zugang zu nachrichtendienstlichen Tätigkeiten als exklusiv, geheimnisumwoben und häufig abhängig von persönlichen Netzwerken, familiären Verbindungen oder militärischen Laufbahnen. In der Bundesrepublik Deutschland hat sich dieses Bild jedoch grundlegend gewandelt. Der BND, der Verfassungsschutz und der MAD agieren heute als reguläre staatliche Arbeitgeber mit transparenten Rekrutierungsverfahren, formalen Stellenausschreibungen und müssen sich an die rechtlichen Rahmenbedingungen halten.

In der Frühphase der deutschen Nachrichtendienste, insbesondere während des Kalten Krieges, erfolgte die Rekrutierung häufig informell. Zugang zu sensiblen Tätigkeiten erhielt, wer als politisch zuverlässig galt, über persönliche Empfehlungen verfügte oder aus bestimmten militärischen, diplomatischen oder akademischen Kreisen stammte. Auch familiäre Traditionen spielten vereinzelt eine Rolle. Diese Praxis war nicht auf Deutschland beschränkt, sondern international üblich.[27]

27 Andrew, C. (2018). The secret world: A history of intelligence. Yale University Press.

In der jungen Bundesrepublik rekrutierte sich der BND zunächst maßgeblich aus dem Personal der Organisation Gehlen, die wiederum aus ehemaligen Wehrmachts- und Geheimdienststrukturen der NS-Zeit hervorgegangen war. Die Forschung zur frühen Geschichte des Bundesnachrichtendienstes zeigt, dass die Personalgewinnung in den ersten Jahren der Bundesrepublik stark durch personelle Kontinuitäten aus der Organisation Gehlen sowie durch informelle Netzwerke geprägt war. Erst im Verlauf der 1960er-Jahre und verstärkt in den 1970er-Jahren lassen sich im Zuge politischer, administrativer und rechtlicher Reformen Ansätze einer zunehmenden Professionalisierung und Demokratisierung der Personalstrukturen erkennen.[28]

1.5.1 Personal und Berwerbungsprozess

Heute verstehen sich unsere Nachrichtendienste ausdrücklich als Teil des öffentlichen Dienstes. Sie veröffentlichen regelmäßig Stellenausschreibungen, insbesondere für akademische Fachkräfte, IT-Spezialisten, Sprachwissenschaftler, Juristen und Ingenieure. Sie können sich auf den folgenden Seiten über aktuelle Stellenausschreibungen informieren:

- **BND**: *https://www.bnd.bund.de/SiteGlobals/Forms/Suche/erweiterte_Karrieresuche_Formular.html* [Stand: 27.12.2025].
- **Verfassungsschutz**: *https://www.verfassungsschutz.de/DE/karriere/karriere_node.html* [Stand: 27.12.2025].
- **MAD**: Der MAD rekrutiert vor allem direkt aus dem Geschäftsbereich des Bundesministeriums der Verteidigung. Das heißt, viele Stellen werden intern über das Intranet ausgeschrieben. Es gibt jedoch auch Stellenangebote für externe Bewerber, die z. B. unter dem folgenden Link zu finden sind: *https://www.bundeswehr.de/de/organisation/mad-bundesamt-fuer-den-militaerischen-abschirmdienst/ihre-karriere-beim-mad* [Stand: 27.12.2025].

Die Stellenbeschreibungen sind bewusst sachlich gehalten. Begriffe wie »Spion« oder »Agent« werden vermieden. Stattdessen ist von »Sachbearbeitern« (gehobener Dienst), »Referenten« (höherer Dienst) oder »wissenschaftlichen Mitarbeitern« (ebenfalls höherer Dienst) die Rede. Für operative oder technische Tätigkeiten können auch spezialisierte Berufsausbildungen ausreichend sein. Die formalen Anforderungen variieren je nach Dienst und Position, umfassen jedoch regelmäßig

- die deutsche Staatsangehörigkeit,
- uneingeschränkte Verfassungstreue,

28 Bundesbeauftragter für die Stasi-Unterlagen (BStU). (2011). Die Organisation Gehlen und ihre Nachfolger. Seit 2011 erforscht eine unabhängige Historikerkommission die Geschichte des BNDs. In diesem Rahmen wurden bereits einige Berichte und Darstellungen vorgelegt. Leider ist die Webseite der Kommission aktuell nicht erreichbar und kann nur archiviert abgerufen werden: *https://web.archive.org/web/20240520055807/http://www.uhk-bnd.de/?page_id=17*

- geordnete wirtschaftliche Verhältnisse,
- hohe persönliche Integrität,
- psychische Belastbarkeit und
- die Bereitschaft zur Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (siehe Abschnitt 2.2, »Achtung, Sicherheitsüberprüfung!«). Für die Nachrichtendienste des Bundes und der Länder ist eine Sicherheitsüberprüfung der Stufe Ü3 (siehe Abschnitt 2.2.3) erforderlich. Die Sicherheitsüberprüfung ist ein zentrales Element des Auswahlverfahrens. Diese dient nicht nur der Feststellung potenzieller Sicherheitsrisiken, sondern auch der Einschätzung persönlicher Stabilität und Loyalität.

1.5.2 Der Karrierepfad

Wie Sie mittlerweile wissen, gilt aus nachrichtendienstlicher Perspektive in Deutschland, dass ein Agent jede Person ist, die für einen Nachrichtendienst tätig ist oder diesem zuarbeitet. Der Begriff *Agent* umfasst damit ausdrücklich nicht nur klassische Aufklärer oder Quellenführer, sondern ebenso administrative Angestellte, IT-Fachkräfte, Übersetzer, Fahrer, technische Mitarbeiter oder auch externe Dienstleister. In diesem weiten Sinne ist auch eine Bürokraft oder Reinigungskraft Teil des nachrichtendienstlichen Apparats und damit Agent des jeweiligen Dienstes.

Der umgangssprachliche Begriff *Spion* hingegen bezeichnet keinen formalen Status, sondern eine bestimmte operative Verwendung. Ein Spion ist demnach eine Person, die aktiv und zielgerichtet Informationen beschafft, insbesondere durch verdeckte Vorgehensweisen. Diese Tätigkeit ist dem operativen Segment eines Nachrichtendienstes zuzuordnen und stellt nur einen kleinen Teil der Gesamtorganisation dar. Für diese Form der Tätigkeit existieren spezifische Verwendungen, die jedoch selten mit Begriffen wie »Spion« oder »Agent im Feld« bezeichnet werden. Stattdessen finden sich sachlich-technische Funktionsbezeichnungen wie *operative Referenten*, *Einsatzmitarbeiter* oder *Quellenführer*.

Man bewirbt sich in der Regel nicht explizit als Spion. Vielmehr führt der Karriereweg häufig über andere Funktionen. Anders, als es viele Filme und Serien suggerieren, ist der Weg zum »Spion« in Deutschland kein unerreichbares Ziel, sondern ein langfristiger, formal strukturierter Karriereprozess innerhalb deutscher Nachrichtendienste, der in der Regel über reguläre Einstiegspositionen, interne Bewährung und gezielte Auswahl für operative Verwendungen führt.

1.5.3 Eine Frage des Geldes

Was verdient eigentlich ein Spion? Wenn man an die zahlreichen James-Bond-Filme denkt, kommen einem sofort falsche Pässe, Luxusuhren, ein Aston Martin und mehrere Bankkonten sowie Kreditkarten auf falsche Namen in den Sinn. Wenn Sie sich an den Film »Casino Royale« erinnern, dann wissen Sie vielleicht noch, dass James Bond dort an einem hochdotierten Pokerturnier teilnimmt, bei dem es um ein Preisgeld von mehreren

Millionen US-Dollar geht. Dieses Geld dient im Film nicht dem privaten Vergnügen, sondern ist Teil einer geheimdienstlichen Operation: Bond soll seinem Gegenspieler durch einen finanziellen Verlust politisch und strategisch schaden. Solche Szenen prägen bis heute das populäre Bild des wohlhabenden, nahezu grenzenlos finanzierten Geheimagenten.

Gehalt nach TVöD

Die Realität der Nachrichtendienste hierzulande ist deutlich bürokratischer. Auch beim Gehalt sieht es da nicht anders aus. Dieses ist, im Gegensatz zu vielem anderen, was Nachrichtendienste betrifft, nicht geheim, sondern für jeden öffentlich einsehbar. Wer beim BND, beim Verfassungsschutz oder beim Bundesamt für den Militärischen Abschirmdienst arbeitet, wird in der Praxis wie andere Beschäftigte des öffentlichen Dienstes bezahlt, nämlich nach Entgeltgruppen und Erfahrungsstufen, die sich am *Tarifvertrag für den öffentlichen Dienst (TVöD)* auf Bundesebene beziehungsweise bei den Landesämtern für Verfassungsschutz am *Tarifvertrag der Länder (TV-L)* orientieren. Hinzu kommen gegebenenfalls verschiedene Zulagen wie eine behördenspezifische Nachrichtendienst-Zulage, eine IT-Fachkräftezulage[29] oder weitere Zuschläge in besonderen Laufbahnen und Funktionsbereichen. Diese Zulagen können das monatliche Bruttogehalt erhöhen.

Auch Nachrichtendienstmitarbeiter bewegen sich finanziell innerhalb klar geregelter tariflicher Rahmen. Es spielt außerdem eine Rolle, ob jemand Tarifbeschäftigter oder Beamter ist, da sich dies sowohl auf die Besoldung als auch auf Zulagen, Versorgung und langfristige Einkommensentwicklung auswirkt. Wir schauen uns ab jetzt die Vergütung eines Agenten bzw. Spions auf Basis einer Tarifbeschäftigung in Deutschland an.

Im TVöD ist das Gehalt immer als Kombination aus Entgeltgruppe und Stufe aufgebaut. Die Entgeltgruppe E 1 bis E 15 (und gegebenenfalls Sonderausprägungen wie E 15Ü) ergibt sich nicht aus dem Jobtitel, sondern aus der Bewertung der dauerhaft übertragenen Aufgaben nach den Tätigkeitsmerkmalen der Entgeltordnung des Bundes. Das heißt, nicht die Person wird eingruppiert, sondern die Tätigkeit, und daraus folgt dann die Entgeltgruppe.

Die Tätigkeit als Agent bzw. Spion beim BND kann sowohl technisch als auch nichttechnisch sein. Ein Hacker würde nach diesem Prinzip die technische und ein Dolmetscher die nichttechnische Laufbahn einschlagen. Die Eingruppierung in eine Laufbahn korreliert eng mit dem formalen Bildungsabschluss und dem typischen Verantwortungsniveau der Tätigkeit:

- Der *einfache Dienst* ist heute nur noch selten anzutreffen. Er ist in der Regel Tätigkeiten mit grundlegenden Anforderungen vorbehalten, für die kein formaler Berufsabschluss erforderlich ist. Typische Entgeltgruppen liegen hier im Bereich E 1 bis E 3. In Nachrichtendiensten spielen solche Funktionen kaum noch eine Rolle.

29 *https://www.verfassungsschutz.de/DE/karriere/arbeiten-beim-verfassungsschutz/ihre-vorteile/ihre-vorteile_node.html* [Stand: 26.12.2025].

- Der *mittlere Dienst* setzt üblicherweise einen anerkannten Ausbildungsabschluss voraus. Tätigkeiten in dieser Laufbahngruppe finden sich häufig in den Entgeltgruppen E 5 bis E 9a. Sie umfassen qualifizierte Sachbearbeitung, Assistenz- und operative Unterstützungsaufgaben, teilweise auch spezialisierte technische Tätigkeiten.
- Der *gehobene Dienst* ist mit einem Bachelorabschluss oder einem gleichwertigen Abschluss verknüpft. Dieser Bereich bewegt sich typischerweise in den Entgeltgruppen E 9b bis E 12. Hierzu zählen anspruchsvolle Fach- und Analyseaufgaben, Projektarbeit, IT- und Auswertungsfunktionen sowie erste Führungs- oder Koordinationsaufgaben. Gerade bei Nachrichtendiensten ist der gehobene (technische) Dienst für Informatiker, IT-Sicherheitsexperten und Analysten relevant.
- Der *höhere Dienst* setzt in der Regel einen Masterabschluss, ein universitäres Diplom oder einen gleichwertigen wissenschaftlichen Abschluss voraus. Entsprechende Tätigkeiten werden im Tarifbereich meist den Entgeltgruppen E 13 bis E 15 zugeordnet. Sie umfassen konzeptionelle, strategische und leitende Funktionen, spezialisierte Fachrollen sowie Führungspositionen mit größerer Personal- oder Budgetverantwortung. Im nachrichtendienstlichen Kontext sind hier beispielsweise die Juristen angesiedelt.

Tabelle 1.1 zeigt die vom 1. Mai 2026 bis zum 31. März 2027 gültige Fassung der Entgelttabelle, anhand derer Sie transparent nachlesen können, in welchem Gehaltsbereich sich ein Agent hierzulande bewegt:[30]

Entgeltgruppe	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5	Stufe 6
E 15Ü	7062,92	7814,11	8525,72	9000,15	9110,86	
E 15	5827,86	6208,96	6634,05	7214,39	7811,37	8204,11
E 14	5298,27	5643,35	6094,01	6594,12	7151,57	7551,78
E 13	4901,11	5279,32	5709,87	6177,31	6727,38	7025,87
E 12	4415,70	4850,91	5359,50	5923,82	6586,00	6900,18
E 11	4269,64	4669,92	5046,03	5454,10	6012,56	6326,77
E 10	4124,53	4438,16	4794,69	5181,37	5611,95	5753,35
E 9c	3978,29	4249,97	4589,09	4958,59	5359,19	5487,80
E 9b	3833,50	3956,17	4267,03	4608,13	4983,57	5297,75
E 9a	3691,52	3917,37	3981,07	4196,35	4590,80	4746,88

Tabelle 1.1: TVöD Bund, Beträge in Euro, vom 01.05.2026 bis 31.03.2027

30 *oeffentlicher-dienst.info* (o. D.). Entgelttabelle TVöD Bund 2026 (Gültigkeit: 01.05.2026–31.03.2027). Abgerufen am 26. Dezember 2025 von *https://oeffentlicher-dienst.info/c/t/rechner/tvoed/bund?id=tvoed-bund-2026&matrix=1* [Stand: 26.12.2025].

Entgeltgruppe	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5	Stufe 6
E 8	3486,40	3697,29	3843,36	3992,40	4153,50	4230,97
E 7	3294,98	3537,94	3682,69	3828,76	3969,05	4045,24
E 6	3240,30	3440,25	3580,46	3719,22	3855,50	3926,20
E 5	3124,08	3318,04	3449,05	3587,78	3716,70	3783,33
E 4	2994,17	3190,45	3355,14	3457,66	3560,17	3620,20
E 3	2953,13	3164,20	3215,57	3332,99	3421,10	3501,81
E 2Ü	2787,52	3028,30	3116,51	3234,12	3314,92	3375,24
E 2	2767,54	2975,32	3027,12	3101,04	3263,52	3433,49
E 1		2543,55	2568,83	2611,69	2651,64	2754,50

Tabelle 1.1: TVöD Bund, Beträge in Euro, vom 01.05.2026 bis 31.03.2027 (Forts.)

Die *Stufe* innerhalb der Entgelttabelle bildet die Erfahrung innerhalb der Entgeltgruppe ab. Bei Neueinstellungen erfolgt die Eingruppierung grundsätzlich in Stufe 1. Mit einschlägiger Berufserfahrung kann man direkt höher eingruppiert werden. Typischerweise wird man ab mindestens einem Jahr in Stufe 2 und ab mindestens drei Jahren einschlägiger Berufserfahrung in Stufe 3 eingruppiert. Zusätzlich dazu kann der Arbeitgeber Berufserfahrung und Ausbildungszeiten als »förderlich« berücksichtigen, was die Personalgewinnung etwas flexibler gestaltet.

Wie würde Agent Florin Dalvikov in Deutschland vergütet werden, wenn seine Sicherheitsüberprüfung ein positives Ergebnis liefern und er beispielsweise beim BND anfangen würde? Er hat ein Bachelor-Studium der Informatik mit dem Schwerpunkt IT-Sicherheit erfolgreich abgeschlossen und bereits drei Jahre Berufserfahrung gesammelt. Er würde, wenn er tarifrechtlich angestellt wird, in den gehobenen (technischen) Dienst einsteigen und könnte mit einer Eingruppierung in E 10 bis E 12 rechnen. Aufgrund seiner dreijährigen Berufserfahrung könnte er, wenn sie im öffentlichen Dienst absolviert wurde oder anerkannt wird, in Stufe 3 einsteigen. Das sind nach dem TVöD (Bund) für das Jahr 2026 in E 10 4794,69 €, in E 11 5046,03 € und in E 12 5359,50 € brutto pro Monat.

Vergleicht man diese Gehälter mit denen aus der freien Wirtschaft, stellt man zunächst einmal fest, dass der Bund transparent nach TVöD zahlt, während der private Markt stärker von der Branche, dem Standort, der Unternehmensgröße und dem eigenen Geschick in Gehaltsverhandlungen abhängt. In der Privatwirtschaft liegen die veröffentlichten Vergleichswerte je nach Jobtitel und Definition häufig in einer ähnlichen oder höheren Größenordnung, allerdings mit großer Streuung. StepStone nennt beispielsweise für

den Beruf »IT Security Engineer« in Deutschland ein durchschnittliches Jahresgehalt von rund 55.200 bis 66.400 €.[31] Für den allgemeineren Titel »Security Engineer« nennt StepStone eine Spanne von 51.300 bis 70.500 €.[32] Ergänzend hierzu weist eine Auswertung zum Hays IT-Gehaltsreport 2025[33] nach Berufserfahrung unter anderem aus, dass man mit weniger als zwei Jahren Berufserfahrung im Durchschnitt 48.500 €, mit zwei bis fünf Jahren 55.500 € und mit mehr als 10 Jahren 69.900 € verdient. Die oberen 25 % liegen bei über 83.000 €.

Nach TVöD E 10 bis E 12 Stufe 3 liegt man 2026 bei rund 57.536 bis 64.314 € Jahresgehalt. Darin sind zwölf Monatsgehälter ohne Sonderzahlungen und Zulagen enthalten. In der freien Wirtschaft werden für Security-Rollen je nach Aufgabenprofil ungefähr 55.000 bis 60.000 € als typische Größenordnung genannt, wobei man als besonders gefragte Fachkraft und abhängig von der Region bzw. Branche auch klar darüber liegen kann. Hierzu kommen gegebenenfalls noch variable Gehaltsbestandteile wie Boni oder Aktienprogramme.

Rein finanziell betrachtet, verdient man mit einem IT-Security-Profil, das im Bereich der Cyberspionage besonders relevant ist, in der freien Wirtschaft in der Regel besser als beim Staat. Der öffentliche Dienst wirbt hingegen nicht mit Spitzengehältern, sondern mit Planbarkeit, Sicherheit und langfristiger Stabilität. Das Einkommen ist transparent, steigt automatisch mit der Erfahrung (Zeit) und wird durch Zulagen ergänzt, erreicht aber selten die Gehaltsspitzen, die in der freien Wirtschaft möglich sind. Wer sich also primär am Einkommen orientiert, stellt sich außerhalb des Staatsdienstes meist besser. Wer dagegen Wert auf Verlässlichkeit und den sicherheitspolitischen Auftrag legt, akzeptiert bewusst ein moderateres Gehaltsniveau.

Frage #005: Würden Sie für eine Tätigkeit als Agent bzw. Spion bei einem Nachrichtendienst ein geringeres Gehalt in Kauf nehmen und warum?

Bestechlichkeit als Insiderbedrohung

Aus der zunächst harmlos klingenden Gehaltsfrage kann tatsächlich ein handfestes Sicherheitsproblem entstehen, nämlich durch *Bestechlichkeit*. Es geht um die klassische *Insiderbedrohung (Insider Threat)*, bei der ein eigener Mitarbeiter aus Geldnot, Gier oder Opportunismus zur Quelle eines gegnerischen Dienstes wird. Nachrichtendienste investieren viel Geld und Zeit in die Sicherheitsüberprüfungen ihrer Mitarbeiter, aber das Gehalt und die finanzielle Lage bleiben ein relevanter Risikofaktor. Schulden, teure Lebensumstände, Spielsucht oder das Gefühl, »unter Wert« bezahlt zu werden, können die Eintrittspforte sein.

31 *https://www.stepstone.de/gehalt/IT-Security-Engineer.html* [Stand: 26.12.2025].
32 *https://www.stepstone.de/gehalt/Security-Engineer.html* [Stand: 26.12.2025].
33 Hays. (2025). Hays Gehaltsreport IT 2025. Hays AG. *https://www.hays.de/en/recruitment-services-insights/study/gehaltsreport-it-2025* [Stand: 26.12.2025].

Zwar werden im Rahmen der Sicherheitsüberprüfung solche potenziellen Risiken abgefragt, allerdings gibt es immer wieder blinde Flecken.[34] Aus Sicht fremder Dienste ist Geld dabei ein besonders dankbarer Hebel, weil er schnell wirkt, kaum ideologische Apelle voraussetzt und sich schrittweise skalieren lässt. Es beginnt mit einem »kleinen Gefallen« und kann über mehrere Stufen zum systematischen Verrat werden. Sobald man einmal mit einem gegnerischen Dienst zusammengearbeitet hat, und sei es nur in Form des bereits erwähnten »kleinen Gefallens«, bewegt man sich bereits im Bereich des Landesverrats und ein Absprung wird immer schwieriger.

Dass das keine theoretische Sorge ist, zeigen mehrere Fälle aus dem Umfeld der Nachrichtendienste sehr deutlich. Beispielsweise ist der Fall Carsten L. (BND) und Arthur E. zu nennen, in dem die Bundesanwaltschaft 2023 Anklage wegen Landesverrats erhob. Nach Darstellung der Bundesanwaltschaft sollen die Angeklagten dem russischen Inlandsgeheimdienst FSB gegen hohe Bargeldzahlungen Staatsgeheimnisse geliefert haben. In der Pressemitteilung heißt es, der FSB habe Carsten L. mindestens 450.000 Euro und Arthur E. mindestens 400.000 € als Vergütung gezahlt. Arthur E. habe Geld in bar in Moskau entgegengenommen.[35]

Die von der Bundesanwaltschaft genannten Beträge zeigen, dass ein gegnerischer Dienst bereit ist, Summen zu zahlen, die ein reguläres TVöD-Gehalt um ein Vielfaches übersteigen und damit eine Versuchung schaffen, die sich oftmals nicht mit moralischen Appellen allein entschärfen lässt. In der öffentlichen Berichterstattung wurde hervorgehoben, wie zentral der Geldtransfer als operatives Element war. Ein Beteiligter sei am Flughafen an der Zollkontrolle vorbeigeschleust worden, während erhebliche Bargeldsummen im Spiel gewesen sein sollen.[36]

Ein weiterer Fall ist der des BND-Mitarbeiters Markus R. Er war beim BND nicht in einer operativen Rolle tätig, sondern arbeitete nach übereinstimmender Berichterstattung und laut Gerichtsunterlagen in einem administrativen Bereich, unter anderem in der Poststelle in Pullach. Gerade solche unauffälligen Positionen sind sicherheitsrelevant, weil sie häufig Zugang zu einer großen Bandbreite an Vorgängen und Dokumenten bieten.

Nach Darstellung der bayerischen Justizbehörden soll Markus R. zwischen Mai 2008 und Mitte 2014 geheime Dokumente und Informationen des BND an die CIA und zudem an

34 Dalwigk, F. (2024). BND Präsident: Lage der Nation [Video]. YouTube. *https://youtu.be/QNQE-y0sNfk?si=_rOhC0Us9Q5Aqbof&t=1006* [Stand: 26.12.2025].

35 Generalbundesanwalt beim Bundesgerichtshof. (2023, 8. September). Anklage wegen mutmaßlichem Landesverrat erhoben. *https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2023/Pressemitteilung-vom-08-09-2023.html* [Stand: 26.12.2025].

36 Banse, D. (2023, 13. Dezember). Agentenkrimi: BND-Beamter vor Gericht. WELT. *https://www.welt.de/politik/deutschland/article248948352/Agentenkrimi-BND-Beamter-vor-Gericht.html* [Stand: 26.12.2025].

einen russischen Nachrichtendienst weitergegeben haben.[37] Der Hauptadressat war nach der Anklageschrift bzw. der Verfahrensdarstellung die CIA. Als Gegenleistung habe Markus R. von der CIA insgesamt mindestens 95.000 € erhalten. Zusätzlich habe er sich Mitte 2014 auch Russland angeboten und dem russischen Generalkonsulat in München drei Dokumente aus dem BND-Bereich übermittelt. Gerichtsnahe Informationen und die Presse sprechen nicht von ein paar Papieren, sondern von einer jahrelangen, systematischen Weitergabe. Mehr als 200 Dokumente sollen von R. über einen langen Zeitraum weitergegeben worden sein.[38]

Das Motiv lässt sich den öffentlich berichteten Aussagen und Prozessberichten zufolge als Mischung aus finanziellen Anreizen und psychologischen Faktoren beschreiben. Markus R. habe sich im BND unterfordert bzw. unterbewertet gefühlt. Der Guardian zitiert ihn sinngemäß mit dem Gefühl, man habe ihm »nichts zugetraut«, während die CIA ihn sich »wichtig« habe fühlen lassen. Bestechlichkeit entsteht also nicht nur aus niedriger Bezahlung, sondern auch aus dem Gefühl fehlender Wertschätzung.

Problematisches Verhalten von Vorgesetzten kann dieses Gefühl noch verstärken. Der BND hat in der Vergangenheit gegen eine seiner Führungskräfte eine Disziplinarklage eingereicht, nachdem dieser Mitarbeiter durch unter anderem antisemitische, sexistische und rassistische Äußerungen aufgefallen war.[39] Laut dem Urteil des Bundesverwaltungsgerichts[40] fielen durch den Beklagten Sätze, die soweit jenseits des guten Geschmacks liegen und jede Form von Würde und Anstand vermissen lassen, dass das Gericht der Disziplinarklage Recht gab und den Angeklagten, der zuvor das Amt eines Regierungsdirektors mit der Besoldungsgruppe A 15 ausgeübt hatte, zurückstufte. In der Urteilsschrift führte das Gericht einige Beispiele aus den Zeugenaussagen auf und hielt fest, dass solche Sätze »immer mal wieder« in den »Morgenrunden« und anderen Meetings gefallen sein.

Diese strombergesken Aussagen tragen, von außen betrachtet, sicherlich nicht zur Förderung eines positiven Arbeitsklimas bei. Geld öffnet zwar die Tür für Insiderbedrohungen, aber Anerkennung, Kränkung und Frust halten die Tür offen und erhöhen die Bereitschaft, die Zusammenarbeit mit fremden Diensten fortzusetzen. So habe laut den Zeugenaussagen im Verfahren das Verhalten des Vorgesetzten »zu einer nachhaltigen Klima-

37 Oberlandesgericht München. (2015, 24. August). Strafverfahren gegen Markus R. wegen Landesverrats u. a. *https://www.justiz.bayern.de/gerichte-und-behoerden/oberlandesgerichte/muenchen/presse/2015/33.php* [Stand: 26.12.2025].

38 Oltermann, P. (2016, 17. März). No one trusted me with anything, says German triple agent. The Guardian. *https://www.theguardian.com/world/2016/mar/17/german-triple-agent-markus-reichel-started-spying-because-he-felt-under-appreciated* [Stand: 26.12.2025].

39 Handelsblatt. (10.11.2023). BND-Chef will harte Linie gegen übergriffige Mitarbeiter fahren. Handelsblatt. *https://www.handelsblatt.com/politik/deutschland/geheimdienst-bnd-chef-will-harte-linie-gegen-uebergriffige-mitarbeiter-fahren/29495722.html* [Stand: 27.12.2025].

40 Bundesverwaltungsgericht. (2022, 28. September). Urteil des Bundesverwaltungsgerichts – 2 A 17.21 (ECLI:DE:BVerwG:2022:280922U2A17.21.0). *https://www.bverwg.de/280922U2A17.21.0* [Stand: 27.12.2025].