Bundesamt für
Verfassungsschutz

Spionage

Ihre Ziele
Ihre Methoden

Spionage

Ihre Ziele
Ihre Methoden

Inhalt

Warum Spionage?

Für Regierungen nahezu aller Staaten sind präzise und rechtzeitig erlangte Informationen aus dem Ausland von entscheidender Bedeutung, um z.B. politische Leitlinien zu entwickeln oder rechtzeitig auf globale Krisen zu reagieren.

Soweit sie offen zugänglich sind, werden solche Informationen auch heute noch meist von Diplomaten gesammelt und bewertet. Diese unterrichten die Regierungen ihrer Heimatstaaten über aktuelle Ereignisse und perspektivische Entwicklungen in den jeweiligen Gastländern.

Viele Regierungen geben sich mit der Beschaffung frei verfügbarer Informationen jedoch nicht zufrieden. Sie streben danach, Erkenntnisse aus anderen Staaten zu erlangen, die nicht für die Öffentlichkeit bestimmt sind. Dadurch wollen sie einen Wissensvorsprung erwerben, um politische, militärische oder wirtschaftliche Vorteile zu erlangen.

Damit dies gelingt, muss die Informationserhebung so erfolgen, dass der Betroffene dies nicht bemerkt. Dafür werden Nachrichtendienste eingesetzt. Deren Aktivitäten definiert die Rechtsordnung des ausgespähten Staates als Spionage.

Deutschland ist aufgrund seiner geopolitischen Lage, der Rolle in der EU und in der NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie für fremde Nachrichtendienste sehr attraktiv. Die Schwerpunkte ihrer Beschaffungsaktivitäten orientieren sich an den aktuellen politischen Vorgaben oder wirtschaftlichen Prioritäten ihrer Regierungen.

Von Interesse sind Informationen aus Politik, Wirtschaft, Militär, Wissenschaft und Technik. Einige Nachrichtendienste spähen auch in Deutschland ansässige Personen und Organisationen aus, die in Opposition zu den jeweiligen Regierungen im Heimatland stehen oder versuchen, diese zu unterwandern.

Methodische Vorgehensweisen

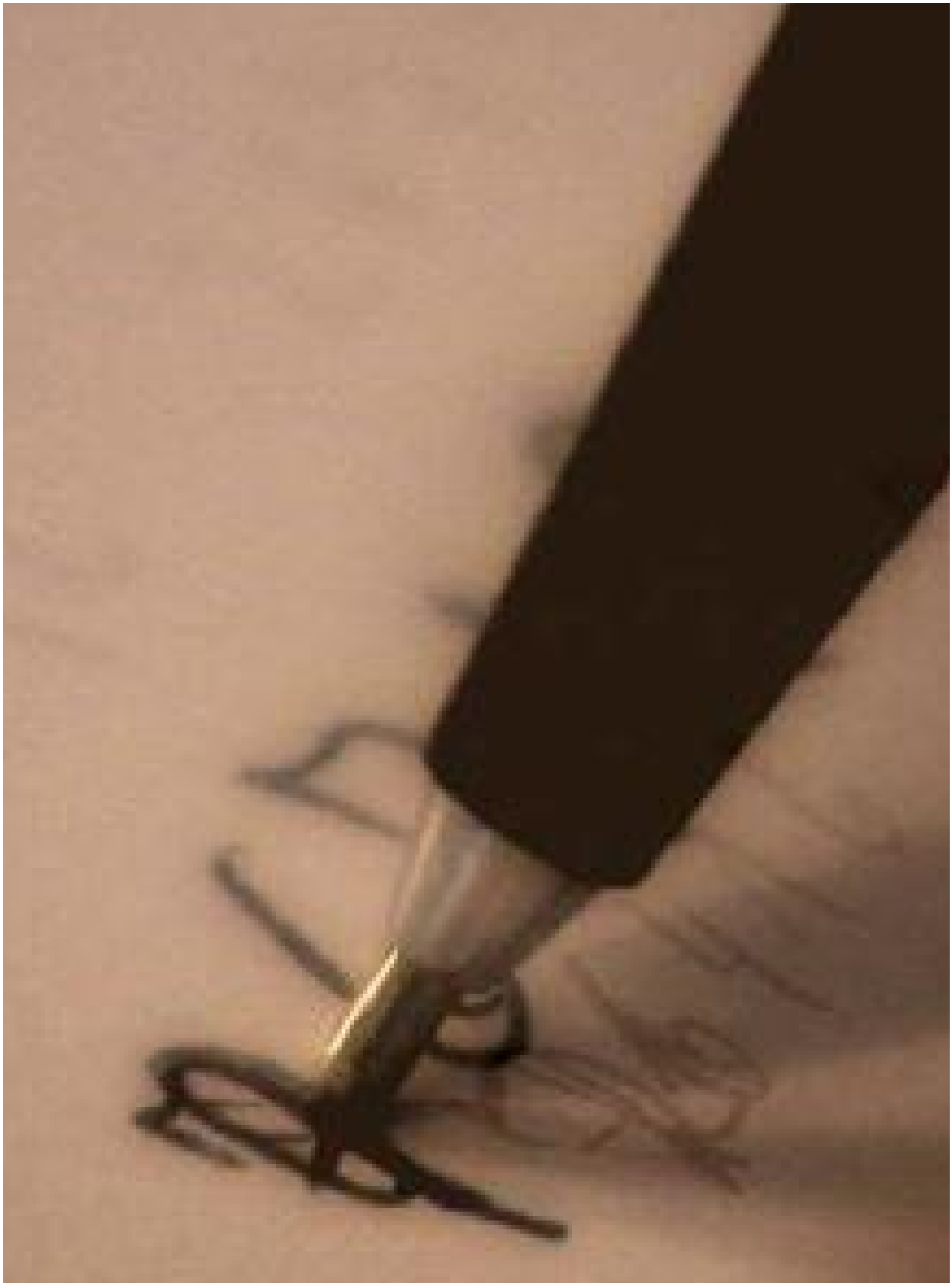
Die gegen Deutschland aktiven Nachrichtendienste nutzen traditionell menschliche Quellen zur Spionage; sie setzen aber auch technische Mittel ein. Hier sind besonders die Überwachung und Ausspähung von Kommunikationsverbindungen (Telefonie und Internetverkehr) sowie Elektronische Angriffe auf IT-Infrastrukturen zu nennen.

Diese Methoden der Informationsbeschaffung gewinnen zunehmend an Bedeutung, weil sie einen umfassenden Zugriff auf die gewünschten Informationen ermöglichen und das Risiko einer Entdeckung für den Angreifer gering ist. So wird die passive Überwachung von Kommunikationsverbindungen von der Spionageabwehr kaum erkannt, weil die hierfür genutzte Empfangstechnik keine aktiven Funksignale aussendet.

Elektronische Angriffe mit einem potenziell nachrichtendienstlichen Hintergrund zeichnen sich vielfach durch ausgeklügeltes „Social Engineering“ aus, d.h. der Inhalt der E-Mails mit der für die Ausspähung genutzten Schadsoftware ist passgenau auf die Aufgaben oder Interessen der Zielperson zugeschnitten. Außerdem sind die gefälschten Absenderadressen meist an tatsächlich existierende, den Zielpersonen bekannte E-Mail-Adressen angeglichen, sodass diese nicht misstrauisch werden. Hinzu kommt, dass die Schadsoftware selbst von technisch hochwertigen Virenschutzprogrammen häufig nicht erkannt wird.

Trotz dieser aktuellen Entwicklung ist davon auszugehen, dass fremde Nachrichtendienste auch künftig auf menschliche Quellen zurückgreifen werden. Vor allem im Bereich der politischen Spionage sind sie unverzichtbar, weil es hier darum geht, Informationen nach spezifischen Vorgaben der Nachrichtendienstzentrale zu beschaffen.

Dies erfordert regelmäßig eine Auswahl der zu beschaffenden Informationen auf dem Wege einer (vorläufigen) Bewertung durch die Quelle selbst. Abhörtechnik und Schadsoftware können diesen Akt kognitiver Erkenntnis nicht ersetzen.



Einsatz menschlicher Quellen

Legalresidenturen

Angehörige fremder Nachrichtendienste bemühen sich häufig darum, Kontakte mit Personen zu knüpfen, die über besondere Kenntnisse oder Zugangsmöglichkeiten in interessanten Zielbereichen verfügen.

In Deutschland unterhalten sie verdeckte Stützpunkte in unterschiedlicher Stärke, die an den Botschaften und Generalkonsulaten ihrer Staaten oder an halboffiziellen Vertretungen (z.B. Presseagenturen oder Fluggesellschaften) eingerichtet sind – sogenannte Legalresidenturen. In diesen Vertretungen ist das nachrichtendienstliche Personal in verschiedenen Arbeitsbereichen eingesetzt.

Die so abgetarnten Nachrichtendienstangehörigen betreiben entweder selbst – offen oder verdeckt – Informationsbeschaffung oder unterstützen nachrichtendienstliche Operationen, die direkt aus den Zentralen der Dienste in den Heimatländern geführt werden.

Oft verfügen sie über einen Diplomatenstatus. Dadurch profitieren sie von der damit verbundenen Immunität, die sie in der Regel vor Strafverfolgung im Gastland schützt. Werden solchen „Diplomaten“ allerdings statuswidrige Aktivitäten nachgewiesen, kann dies zur Ausweisung aus Deutschland führen.

Einen Großteil ihres Informationsbedarfs decken die Nachrichtendienste durch die Auswertung offener Quellen wie des Internets und anderer Medien, durch Besuche von Industriemessen und Teilnahme an öffentlichen Vortragsveranstaltungen, Tagungen und Diskussionsrunden.

Um ihre Erkenntnisse zu vertiefen, nutzen die Legalresidenturoffiziere die durch ihre offizielle Tätigkeit aufgebauten Kontakte. Zielpersonen sind insbesondere solche, die als Informationsquellen für eine längerfristige Nutzung geeignet erscheinen.

Wichtige Kriterien sind dabei die aktuellen Zugangsmöglichkeiten und beruflichen Perspektiven. So entsteht allmählich ein Netz von Gesprächspartnern, die ohne engere nachrichtendienstliche Anbindung regelmäßig oder bei Bedarf abgeschöpft werden. Durch geschickte Gesprächsführung versuchen die Dienstangehörigen, an sensible Informationen oder Hinweise auf andere potenzielle Quellen zu gelangen.

Betroffen davon sind u.a. Mitarbeiter im parlamentarischen Bereich, Vertreter deutscher Behörden und Unternehmen sowie Wissenschaftler, aber auch Angehörige der Bundeswehr.

Nachrichtendienstoffiziere wenden jedoch auch konspirative Methoden an, um besonders sensible Informationen zu beschaffen. Da verdeckte Geheimdienstarbeit und das Verleiten zum Verrat geschützter Informationen gegen den diplomatischen Status verstoßen, erweitern sie zum Schutz vor Enttarnung ihre Sicherheitsvorkehrungen für konspirative Treffen und sorgen für eine sichere Kommunikation.

Zudem halten sie ihre Zielpersonen an, den Kontakt besonders vertraulich zu behandeln. Spätestens zu diesem Zeitpunkt sollte auch eine sorglose Kontaktperson den nachrichtendienstlichen Charakter der Verbindung erkennen.

Zentral gesteuerte Operationen

Nachrichtendienste führen aber auch Operationen direkt aus ihren Zentralen heraus – ohne Beteiligung der Legalresidenturen – durch.

So nutzen sie z.B. die im eigenen Land vorhandenen Möglichkeiten der Informationsbeschaffung über ausländische Staatsangehörige. Dazu gehören u.a. die Grenzkontrollen ein- und ausreisender Personen, die Überwachung von Auslandsvertretungen sowie die Zusammenarbeit im wirtschaftlichen und wissenschaftlichen Bereich.

In ihr Blickfeld geraten vor allem Personen, die sich privat oder beruflich für längere Zeit in dem jeweiligen Land aufhalten oder regelmäßig dorthin reisen.

Insbesondere

- Angehörige deutscher diplomatischer Vertretungen
- Behördenvertreter auf Dienstreisen
- Firmenrepräsentanten sowie
- deutsche Staatsangehörige, die in dem jeweiligen Land einer freiberuflichen Tätigkeit nachgehen oder studieren

müssen mit nachrichtendienstlichen Ansprachen rechnen.

Bei diesem Personenkreis haben die Nachrichtendienste viele Möglichkeiten, ihren „Heimvorteil“ zu nutzen, da sie auf eigenem Territorium gezielt nach Ansatzmöglichkeiten suchen und sich gefahrlos mit Ausländern treffen können. In einigen Fällen bauen die Nachrichtendienstoffiziere eine „Drohkulisse“ auf, z.B. durch Hinweis auf einen – tatsächlichen oder vermeintlichen – Verstoß gegen örtliche Gesetze.

In anderen Fällen versuchen sie, ihre Zielperson für sich einzunehmen und auf freundschaftlicher Basis zu werben.

Außerdem unternehmen Nachrichtendienstoffiziere aus der Dienstzentrale im Rahmen ihrer operativen Aktivitäten vereinzelt Erkundungs- und Treffreisen in andere Länder. Dabei nutzen sie konsequent die Reisefreiheit innerhalb des Schengenraums. Auch Agenten treffen sich mit ihren Führungsoffizieren zuweilen nicht in Deutschland, sondern im Ausland.

Eine weitere Methode ist der Einsatz von „Illegalen“. Dabei handelt es sich meistens um hauptamtliche Mitarbeiter eines fremden Nachrichtendienstes, die mit einer Falschidentität ausgestattet in Zielländer eingeschleust werden. Sie erfüllen dort entweder langfristige Spionageeinsätze oder erledigen vorübergehend bestimmte nachrichtendienstliche Aufträge als Reise-„Illegale“.

Aufgrund ihrer professionellen und sorgfältigen Abdeckung sind sie durch die Spionageabwehr besonders schwer zu enttarnen. Ihre Steuerung erfolgt ebenfalls über die Dienstzentralen.

Einsatz technischer Mittel

Neben der Spionage mit menschlichen Quellen hat die technische Informationsbeschaffung in den letzten Jahren zunehmend an Bedeutung gewonnen.

Fernmeldeaufklärung

Gespräche in Telekommunikationsnetzen sind grundsätzlich nicht abhörsicher. Es ist davon auszugehen, dass fremde Nachrichtendienste erhebliche Anstrengungen unternehmen, um Kommunikationsverbindungen abzuhören. Dazu zählt die mögliche Aufklärung deutscher Kommunikations- und Internetverkehre, die z.T. über Server oder Internetknoten im Ausland geführt werden.

In Deutschland stellen z.B. die Botschaftsgebäude anderer Staaten im Zentrum Berlins sowie diplomatische Vertretungen in anderen Städten geeignete Standorte für Fernmeldeaufklärungsmaßnahmen dar, sofern sie in der Nähe von interessanten Ausspähungszielen liegen. Hinzu kommt ihr exterritorialer Status.

Insbesondere im Bereich des Regierungsviertels besteht bereits seit Langem ein konkretes Abhörrisiko für alle über Funk geführten Kommunikationsverbindungen, darunter z.B. Gespräche mit Mobiltelefonen sowie WLAN- und Bluetooth-Verbindungen. Gefährdet sind auch gespeicherte Informationen auf Laptops oder Tablet-PCs, wenn die Geräte über Funk vernetzt sind.

Die vom potenziellen nachrichtendienstlichen Angreifer genutzte Empfangstechnik sendet keine aktiven und dadurch aufklärbaren Funksignale aus. Ein technischer Nachweis solcher in der Regel passiv durchgeführter Überwachungsmaßnahmen ist für deutsche Sicherheitsbehörden daher kaum möglich.


ADD
LOAD
EXPORT

Elektronische Angriffe

Elektronische Angriffe sind gezielte Maßnahmen mit und gegen IT-Infrastrukturen, die auf eine Informationsbeschaffung oder auf eine Schädigung bzw. Sabotage der attackierten Systeme abzielen.

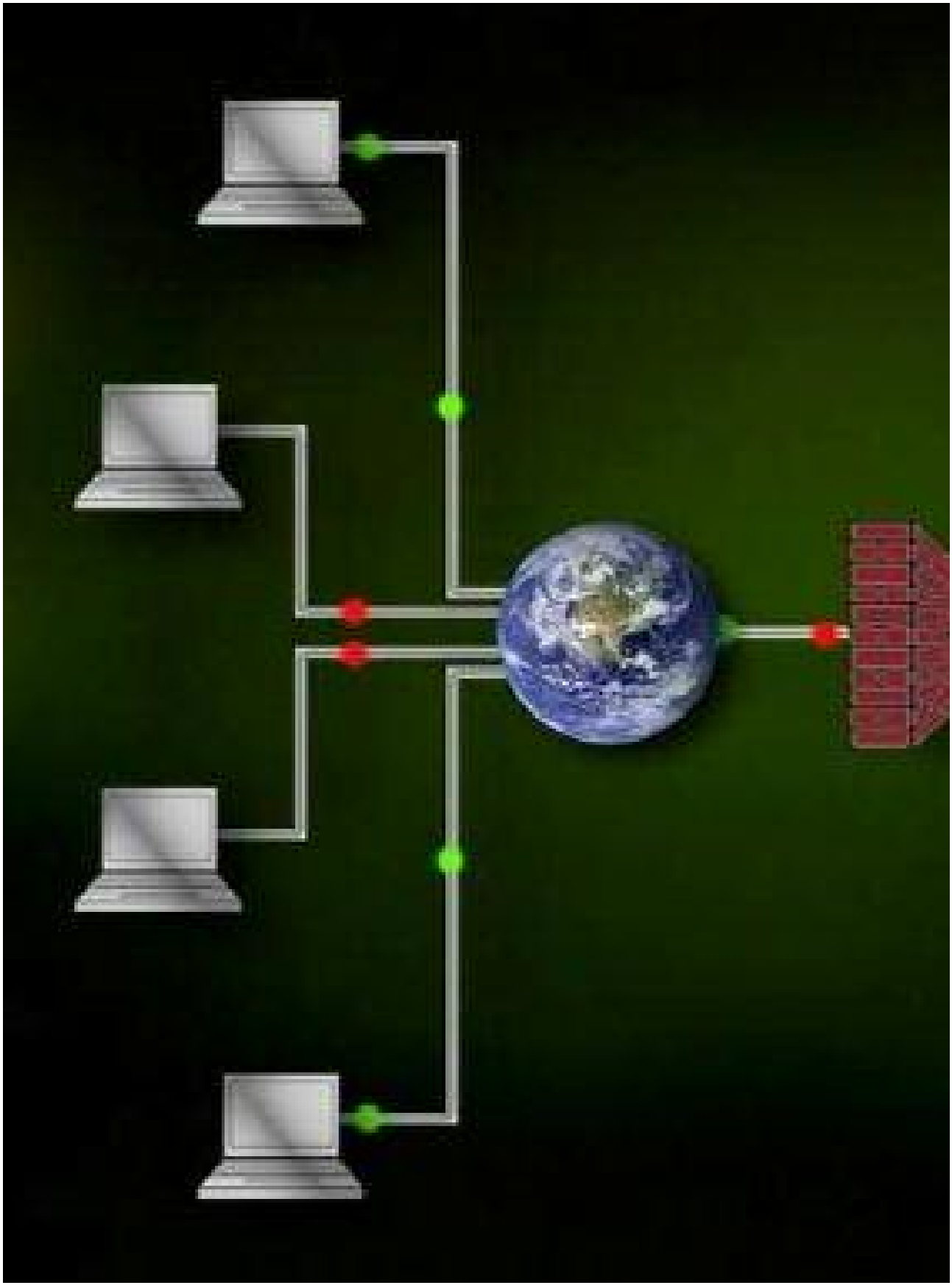
Dazu gehören das Ausspähen, Kopieren oder Verändern von Daten, die Übernahme einer fremden elektronischen Identität, der Missbrauch oder die Sabotage fremder IT-Infrastrukturen sowie die Übernahme von computergesteuerten netzgebundenen Produktions- und Steuereinrichtungen. Die Angriffe können von außen über Computernetzwerke (z.B. über das Internet) oder durch einen direkten, nicht netzgebundenen Zugriff auf einen Rechner erfolgen (z.B. über manipulierte Hardwarekomponenten wie Speichermedien).

Die Urheber Elektronischer Angriffe sind oft nicht zweifelsfrei zu identifizieren. Ergeben sich allerdings Hinweise auf eine Steuerung durch fremde Nachrichtendienste, fällt die Bearbeitung in die Zuständigkeit der Spionageabwehr.

Seit 2005 werden auf breiter Basis durchgeführte, zielgerichtete Elektronische Angriffe gegen Bundesministerien, Bundesbehörden, Personen in herausgehobenen politischen Positionen sowie gegen Wirtschaftsunternehmen festgestellt. Ein Teil der in jüngerer Zeit durchgeführten Angriffe ist technisch sehr ausgefeilt.

Sie häufen sich insbesondere im zeitlichen Umfeld bedeutender wirtschafts- und finanzpolitischer Ereignisse. So wurden beispielsweise – wie schon in vergangenen Jahren – Angriffe im Rahmen des G20-Treffens im September 2013 festgestellt.

Betroffen war neben mehreren Bundesministerien u.a. der Bankensektor. E-Mails, die eine Kommunikation der Sherpa-Gruppe (Chefunterhändler einer Regierung) vortäuschten, sollten hochrangige Entscheidungsträger und deren Mitarbeiter zum Öffnen dieser Nachrichten verleiten. Der in den E-Mails enthaltene Schadanhang bezweckte eine Infektion der Systeme.



Für fremde Nachrichtendienste sind insbesondere solche Informationen von Interesse, die bei staatlichen Stellen abgeschöpft werden können. Die große Anzahl Elektronischer Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund gegen Bundesbehörden verdeutlicht den hohen Stellenwert dieser Art der Informationsbeschaffung.

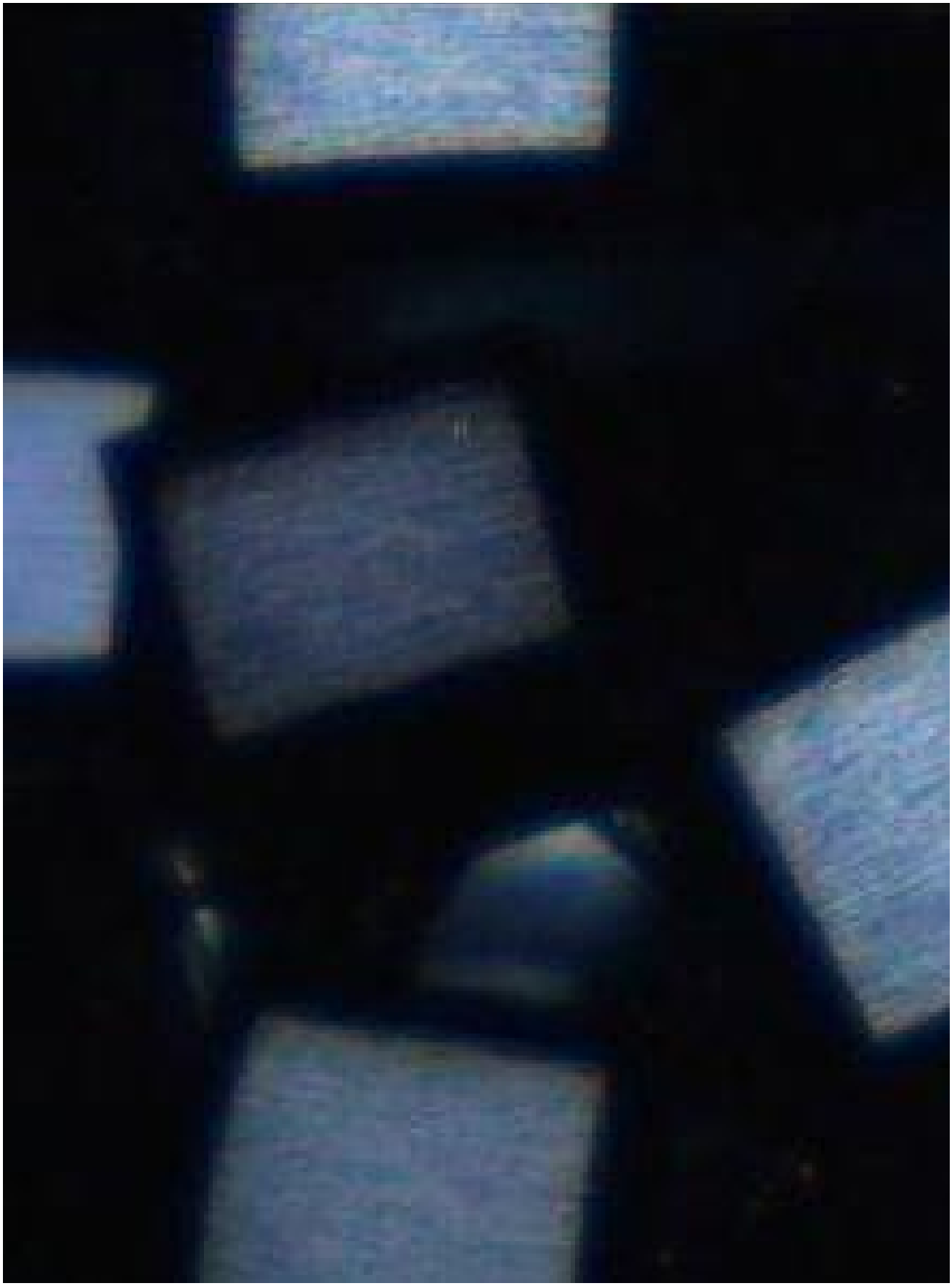
Die Dauer einzelner Angriffsoperationen und die globale Ausrichtung bei der Themen- und Opferauswahl weisen deutlich auf eine strategische und damit staatliche Aufklärung hin.

Die dafür erforderlichen Infrastrukturen und die verwendeten Schadprogramme werden kontinuierlich weiterentwickelt, sodass sich ihre Effektivität laufend verbessert.

Elektronische Angriffe haben ein hohes Gefährdungspotenzial, da sie auch von Opfern mit erhöhtem Sicherheitsbewusstsein häufig nur schwer zu erkennen sind. Dem steht auf Täterseite ein geringes Entdeckungs- und Verfolgungsrisiko gegenüber.

Hierfür sind u.a. folgende Faktoren ausschlaggebend:

- Die E-Mails weisen ein gutes „Social Engineering“ auf, d.h. sie sind so gestaltet, dass sie zu den Interessen- bzw. Aufgabengebieten der Opfer passen und dadurch zunächst einmal keinen Argwohn erregen.
- Die Absenderadressen der Schadmails werden derart gefälscht und an tatsächlich vorhandene, den Opfern bekannte Adressen angepasst, dass diese nicht misstrauisch werden.
- Zudem erkennen die Virenschutzprogramme häufig die von den Angreifern eingesetzte Schadsoftware nicht.



Die Aufklärung derartiger Angriffe wird auch deshalb erschwert, weil die Angreifer ausgefeilte Tarnstrategien zur Verschleierung ihrer Aktivitäten einsetzen. Ein Trend, der bereits seit geraumer Zeit zu beobachten ist und sich auch künftig fortsetzen wird.

Neben der klassischen Trojaner-E-Mail, bei der das Schadprogramm zumeist im Anhang eingebunden ist und erst durch dessen Öffnen aktiviert wird, werden zwischenzeitlich auch weitere, sehr spezielle und kaum erkennbare Angriffsmethoden angewandt. Deshalb ist mit einer hohen Dunkelziffer solcher Angriffe auf ausgewählte Ziele zu rechnen.

Insgesamt ist zu erwarten, dass die Gefahren für die immer weiter vernetzten IT-Infrastrukturen in den nächsten Jahren zunehmen. Dies gilt umso mehr, weil die bei Elektronischen Angriffen verwendeten Schadprogramme zur Informationsabschöpfung – also Spionageprogramme – prinzipiell auch zu Sabotagezwecken eingesetzt werden können.

Derzeit können wir in der Bundesrepublik Deutschland noch keine unmittelbare Gefährdung durch Sabotageangriffe feststellen. Dies gilt auch für den Bereich der Kritischen Infrastrukturen.

Gravierende Veränderungen der politischen Lage, z.B. eine mögliche Verwicklung Deutschlands in aktuelle kriegerische Auseinandersetzungen, bergen aber das Risiko, dass vor diesem Hintergrund Cybersabotage-Aktionen gegen deutsche Stellen durchgeführt werden. Angesichts des außerordentlichen Schadenspotenzials, das derartigen Angriffen innewohnt, sind hier weiterhin höchste Wachsamkeit und Vorsorge angezeigt.

Die Anonymität des Internets erschwert die genaue Identifizierung der Täter und deren Motivlage erheblich. Aufgrund bestimmter Merkmale und Indizien ist bei vielen Angriffen jedoch zumindest eine regionale Zuordnung ihrer Herkunft möglich.

Bewertung und Ausblick

Neben der weiterhin betriebenen Spionage durch menschliche Quellen werden die Gefahren durch technische Aufklärung mit der fortschreitenden technischen Entwicklung stetig zunehmen.

Dies gilt sowohl für die Überwachung und Aufklärung der Kommunikationsverkehre als auch für die Gefahren durch Elektronische Angriffe. Die Gründe hierfür liegen vornehmlich in dem Verhältnis von Erkenntnisgewinn zu dem relativ geringen Entdeckungsrisiko für den Angreifer, das aus deren Sicht eine solche Vorgehensweise als effizient erscheinen lässt.

Das Bundesamt für Verfassungsschutz und andere zuständige Behörden haben den parlamentarischen und behördlichen Bereich in den vergangenen Jahren regelmäßig über die bestehende Gefährdung informiert und zugleich Wege für einen verbesserten Schutz ihrer Kommunikation aufgezeigt.

Um die von fremden Nachrichtendiensten ausgehenden Bedrohungen einzudämmen, wird es auch künftig erforderlich sein, potenzielle Zielpersonen und die Entscheidungsträger vor allem in Politik und Wirtschaft über die Methoden und Konsequenzen der Ausspähung durch fremde Nachrichtendienste aufzuklären und eingehend zu sensibilisieren.


INFORMATION

Erläuterungen

Abtarnen, abgetarnt
Im Zusammenhang mit dem Begriff Legalresidentur bedeutet abgetarnt den Einsatz eines hauptamtlichen Mitarbeiters eines Nachrichtendienstes an einer diplomatischen oder halboffiziellen Vertretung seines Herkunftslandes als vermeintlich „echter" Diplomat oder sonstiger Bediensteter auf einem Dienstposten, der für den Nachrichtendienst „reserviert" ist.

Beschaffung/Beschaffungsaktivitäten
Sammelbegriff für die von Nachrichtendiensten angewandte Methode, Informationen und Erkenntnisse zu erlangen. Man unterscheidet zwei Varianten:

- Zur „offenen" Beschaffung gehören u.a. die Auswertung von Medien oder der Besuch öffentlicher Veranstaltungen mit dem Ziel, persönliche Kontakte zu knüpfen und Informationen zu erlangen.
- Die „verdeckte" Beschaffung erfolgt durch den Einsatz nachrichtendienstlicher Mittel (z.B. Observation, Überwachung des Fernmelde- und Internetverkehrs, Gewinnung von Informanten).

Einschleusung
Von einem Nachrichtendienst gesteuertes heimliches Verbringen eines Illegalen oder Agenten in sein Einsatzgebiet, häufig unter Nutzung einer falschen Identität. Darunter fällt sowohl die Einreise in das Zielland als auch die Etablierung in seinem unmittelbaren Wohn- und Arbeitsumfeld.

Erkundungsreise/Treffreise
Reise eines Nachrichtendienstoffiziers aus seinem Einsatzstaat oder der Zentrale in ein Drittland. Eine solche Reise hat häufig einen nachrichtendienstlichen Hintergrund und kann u.a. zur Vorbereitung einer Treffreise oder zum Erwerb von Erkenntnissen zu bestimmten Örtlichkeiten dieses Landes erfolgen.

IT-Infrastruktur
Gesamtheit aller IT-Komponenten, die für verschiedene Anwendungen und den Betrieb erforderlich sind. IT-Infrastruktur umfasst die gesamte Informationstechnologie, nicht jedoch die dazu gehörenden Mitarbeiter, Prozesse und Dokumentationen.

(Nationale) Kritische Infrastrukturen
Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Auf Bundesebene gibt es dazu die folgende Sektoreneinteilung:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur

Menschliche Quelle
Jede Person, die Informationen für einen Nachrichtendienst beschafft oder ihm auf andere Weise zukommen lässt. Dabei kann es sich um einen Agenten handeln, aber auch um jemanden, der den nachrichtendienstlichen Hintergrund nicht kennt.

Nachrichtendienstoffizier
Andere Bezeichnung für einen hauptamtlichen Mitarbeiter eines fremden Nachrichtendienstes.

Social Engineering
Methode, um unberechtigten Zugang zu sensiblen Informationen durch „Aushorchen" von Personen zu erlangen. Ausgenutzt werden menschliche Eigenschaften wie beispielsweise Vertrauen, Eitelkeit, Hilfsbereitschaft, Habgier, Angst oder Respekt vor Autorität.

Spionage
Als Spionage wird die Tätigkeit für den Nachrichtendienst einer fremden Macht bezeichnet, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist.
Die Beschaffung von Informationen, vor allem aus den Bereichen Politik, Wirtschaft, Wissenschaft und Militär, erfolgt zumeist unter Anwendung geheimer Mittel und Methoden.
Soweit Spionage gegen die Bundesrepublik Deutschland gerichtet ist, kommt eine Strafbarkeit gemäß §§ 93 ff. StGB in Betracht.

Zielperson/Zielbereich
Person, die in das Blickfeld eines Nachrichtendienstes gerückt ist, weil sie angesprochen werden soll, um sie z.B. als Agenten zu werben.
Als Zielbereiche bezeichnet man Bereiche eines staatlichen Gemeinwesens, für die sich Nachrichtendienste interessieren. Dabei handelt es sich regelmäßig um Politik, Militär, Wirtschaft sowie Wissenschaft und Technik, aber auch um ausländische Personen oder Gruppierungen, die in Opposition zu den Regierungen ihrer Heimatstaaten stehen.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Öffentlichkeitsarbeit
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 221/792-0
Fax: +49 (0) 221/792-2915

Gestaltung und Druck
Bundesamt für Verfassungsschutz
Print- und MedienCenter

Bildnachweis
BfV

Stand
Mai 2014

Weitere Informationen zum Verfassungsschutz finden Sie hier:

www.verfassungsschutz.de