GÜNTHER WEISSE

Totale Überwachung: Staat, Wirtschaft und Geheimdienste

Paradigma Media Advies

Günter Weiße

Totale Überwachung

Staat, Wirtschaft und
Geheimdienste
im Informationskrieg des
21. Jahrhunderts

Paradigma Media Advies

Omslagontwerp: DSR – Digitalstudio Rypka/Thomas Hofer,
Dobl Illustratie omslag: Archief van de uitgeverij (Menwith-Hill-Kuppel)
Vormgeving: Ecotext-Verlag, Mag. G. Schneeweiß-Arnoldstein, Wenen, Oostenrijk
ISBN/EAN: 978-90-7884-015-2
NUR-code: 631

Inhaltsverzeichnis

Vorwort

„Die Aufgabe der Politik liegt in der möglichst richtigen Voraussicht dessen, was andere Leute unter den gegebenen Umständen tun werden."[1]

Die asymmetrische Bedrohung sowohl unseres Landes bzw. unserer Partner und Verbündeten durch nachrichtendienstliche Aktivitäten fremder Staaten, als auch Wirtschafts- und Industriespionage sowie die Gewalt terroristischer Gruppierungen und schließlich Bedrohungen, die sich durch auflösende Staaten („failed states") entwickeln und jederzeit mögliche Informationsoperationen[2] auswärtiger Mächte und Gruppierungen nötig machen, erfordern vorausschauende und umfassende Schutz- und Abwehrmaßnahmen. Dieses Buch soll dazu beitragen, die Zusammenhänge zwischen den fortschreitenden technischen Möglichkeiten der Aufklärung mit elektronischen Mitteln und deren Mechanismen durch fremde Nachrichtendienste bzw. die Bedrohungen durch die transnationale organisierte Kriminalität oder Terrorgruppen transparent zu machen.

Staatliche Überwachungsmaßnahmen in allen Bereichen der Kommunikationsbeziehungen werden zukünftig nach Auffassung interessierter Kreise in der Europäischen Union noch verstärkt werden müssen und werden vermutlich tief in die „individuelle informationelle Selbstbestimmung" eines jeden Bürgers eingreifen. Aus Gründen der Sicherheit werden neuerdings mit Unterstützung durch die Europäische Union Systeme entwickelt, die eine gezielte Überwachung auch größerer Menschenansammlungen ermöglichen, was eine entsprechende Reaktion der Überwachungs- und Sicherheitskräfte zur Folge haben wird. Parallel dazu sind in der EU umfassende Maßnahmen zur „technischen Sozialkontrolle"[3] geplant.

Die Vielfältigkeit der Angriffe auf Informations- und Kommunikationssysteme aller Art und deren Abwehr erfordern profunde Spezialkenntnisse. Aus diesem Grunde soll in diesem Werk auf spezielle technische Einzelheiten nur dort eingegangen werden, wo es zum Verständnis der Materie erforderlich ist.

---

1 Otto von Bismarck, zitiert in Emde, H.: Die geheime Nachrichtendienste der Bundesrepublik Deutschland, Bergisch Gladbach 1979.

2 Informationsoperationen (InfoOps) sind „zielgerichtete, räumlich und zeitlich zusammenhängende und aufeinander abgestimmte Maßnahmen zur Beeinträchtigung fremder und Schutz eigener Informations- und Kommunikationssysteme (IKS) einschließlich dazugehöriger Prozesse". Vgl. auch: Teilkonzeption Informationsoperationen der Bundeswehr (TKInfoOPBw Bonn, 17. 2. 2005) sowie www.bundeswehr.de/portal/a/bwde/streitkräfte/transformation, aufgerufen am 15. 3. 2010.

3 Eine überaus weitsichtige Bewertung der künftigen Entwicklungen enthält Miller, A. R.: Der Einbruch in die Privatsphäre, Neuwied und Berlin 1973.

Weiterführende Literatur steht dem interessierten und fachkundigen Leser in einer fast unüberschaubaren Vielfalt zur Verfügung.

Bei der Beschreibung von Nachrichtendiensten und deren Fähigkeiten sowie Aktivitäten musste aus naheliegenden Gründen ausschließlich auf offen verfügbare Informationen aller Art zurückgegriffen werden. Dies gilt insbesondere für Aussagen über deren Struktur sowie die Voraussetzungen und Möglichkeiten der Technischen Aufklärung durch diese Dienste. Die erkennbar werdende Verwischung der Grenzen zwischen Nachrichtengewinnung durch offene Mittel und Methoden sowie die Nachrichtenbeschaffung mithilfe nachrichtendienstlicher Mittel durch fremde, auch befreundete Nachrichtendienste machen es erforderlich, auch die Aktivitäten militärischer Spezialkräfte – Special Operation Forces – in die Betrachtungen über die Gefährdung durch Informationsoperationen mit einzubeziehen. Auch die in den europäischen Nachrichten- und Sicherheitsdiensten neuerdings erkennbar werdende Tendenz, nachrichtendienstliche Aufgaben mit Aufgaben der inneren Sicherheit zu vermischen, stellt einen nicht zu übersehenden Paradigmenwechsel dar, dessen letzte Konsequenzen noch nicht absehbar sind.

In diesem Buch sollen, soweit es die Erkenntnisse[4] aus offenen Quellen zulassen, die Wechselwirkungen zwischen der signalerfassenden (Technischen) Aufklärung (SIGINT), der netzwerkzentrierten Kriegführung (Network Centric Warfare) und der Informationsoperationen sowie die begleitenden Aktivitäten fremder Staaten und Gruppen zur Nachrichtengewinnung und Aufklärung (NG&A) beschrieben werden. Auf die Einzelaspekte der nachrichtendienstlichen Beschaffung und die Gewinnung von Informationen mithilfe menschlicher Quellen (HUMINT) soll im Rahmen des Werkes nur dort eingegangen werden, wo es erforderlich ist. Ein nicht minder wichtiger Aspekt ist die umfassende Telekommunikationsüberwachung durch staatliche Stellen zur Bekämpfung des internationalen Terrorismus und internationaler organisierter Kriminalität. Nicht zuletzt die Überwachung des Zahlungsverkehrs in der Europäischen Union und die Weitergabe der dabei gewonnenen sensitiven Daten wie auch die umfassende Weitergabe von Fluggastdaten an eine ausländische Regierung stimmen bedenklich. Nicht minder bedenklich stimmen Bestrebungen interessierter Kreise in der EU zur Schaffung umfassender, nahezu alle Lebensbereiche abdeckender Datensammlungen und deren künftige Verknüpfung mit bereits bestehenden nationalen und supranationalen Datensammlungen mit dem Ziel der Terrorbekämpfung. Besonders herauszuheben sind die Bestrebungen der EU, Instrumente zur „Erkennung unsozialen Verhaltens“ bzw. zur „Mind-“ und „Crowd Control“ zu entwickeln, um diese Daten in eine umfassende künftige Datensammlung der EU zu integrieren. Dies gilt auch für eine Reihe bereits

4 Die in diesem Werk beschriebenen Sachverhalte beruhen ausschließlich auf Erkenntnissen, die aus offenen, jedermann frei zugänglichen Quellen gewonnen wurden oder offenkundig sind. Auf die entsprechenden Quellen wird im Text hingewiesen. Für die daraus abzuleitenden Folgerungen und Bewertungen trägt ausschließlich der Autor die Verantwortung. Benutzte Quellen wurden, soweit möglich, nach den Vorgaben des Chicago Manual of Style, 14th Edition, zitiert. Sie geben den Informationsstand vom Juli 2010 wieder.

bestehender Datensammlungen in Deutschland und die geplante Errichtung des Elektronischen Einkommensnachweises (ELENA)[5], in dem bereits mehr als 36 Mio. Datensätze erfasst sein sollen.

Nicht zuletzt die unter dem Aspekt des Schutzes vor Pornographie geplanten Internetsperren der EU könnten, falls dies aus Sicht maßgeblicher Kreise in der EU erforderlich sein sollte, auch auf andere Sachverhalte im Internet und möglicherweise auch auf andere Medien ausgedehnt werden. Auch wird die kaum kontrollierbare Sammlung von sensitiven personenbezogenen Daten aller Art durch Wirtschaftsunternehmen und deren Nutzung einen noch nicht absehbaren Einfluss nehmen. Die im Zusammenhang mit der Erweiterung der EU-Grenzagentur FRONTEX geplante Überwachung von Reisebewegungen, die zum Teil in Großbritannien bereits jetzt verwirklicht wurde, ist ein Beispiel für die bisher maßgeblich von Großbritannien[6] inspirierten Überwachungs- und Kontrollmaßnahmen. Nicht zuletzt die im EU-Programm INDECT[7] geplanten umfassenden weiteren Überwachungs- und Kontrollmaßnahmen auf EU-Ebene stellen eine ernsthafte, auch nicht mit Terrorbekämpfung zu begründende Kontrolle aller EU-Bürger dar.

Weiter werden der nicht minder wichtige Aspekt der Industrie- und Wirtschaftsspionage mithilfe von Informationsverarbeitungs- und Kommunikationssystemen und die Schutzmaßnahmen gegen derartige Angriffe behandelt. Dabei spielen auch die Forderungen der Vereinigten Staaten nach ungehin-

---

5 Gegenwärtig (Mai 2010) ist eine Verfassungsklage gegen die Einführung von ELENA beim BGH anhängig, die auch auf die Einführung des Elektronischen Personalausweises ausgeweitet werden soll. Insbesondere der im Elektronischen Personalausweis enthaltene RFID-Chip ist nicht gegen das Auslesen durch Unbefugte gesichert. Dieser Mangel begünstigt auch den jederzeit möglichen elektronischen Identitätsdiebstahl mit unabsehbaren Folgen für den Betroffenen. Daher verfügen amtliche Dienstpässe in Deutschland nicht über den Chip, auf dem biometrische Daten gespeichert sind.

Gegen die im Oktober 2008 eingeführte elfstellige Steuernummer, in der u. a. Name, Anschrift, Religionszugehörigkeit, Geburtsdatum, Geschlecht und die Daten der Ehepartner enthalten sind, wurden vor dem Landgericht Köln bisher 170 Klagen Betroffener eingereicht, die eine Löschung verlangen. Die Steuer-Identifikationsnummer wird vom Bundeszentralamt für Steuern (BZSt) in Bonn verwaltet und könnte, in weitere Dateien integriert, künftig als unverwechselbare Personenkennziffer dienen, vgl.: www.suedddeutsche.de/geld/2.220/steuer-identifikationsnummer

6 Aber hier scheint sich ein Paradigmenwechsel durch die neue Regierung abzuzeichnen, da diese beabsichtigt, die Vorratsdatenspeicherung und andere Maßnahmen zur inneren Sicherheit nicht länger fortzuführen. Großbritannien verfügt derzeit über mehr als 4,5 Mio. Überwachungskameras, deren Einsatz als fragwürdig bezeichnet wird; vgl. www.derstandard.at, 26. 5. 2010.

7 INDECT = Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (dt. etwa: Intelligentes Informationssystem, das Überwachung, Suche und Entdeckung für die Sicherheit von Bürgern in einer städtischen Umgebung unterstützt). Vgl. hierzu in diesem Buch insbesondere die S. 86–91.

dertem Zugang zu den Banktransferdaten[8] Europas eine gewichtige Rolle. Die Bedrohung durch den weltweit vernetzten Terrorismus unter dem Aspekt von religiös und politisch motivierten Terrorangriffen gegen Einzelpersonen, Personengruppen und jederzeit mögliche Informationsoperationen gegen Kritische Infrastrukturen im In- und Ausland sind zu einer elementaren Bedrohung der westlichen Zivilisation mit noch nicht absehbaren Folgen geworden. Dies kann auch für die Bedrohung durch die transnationale organisierte Kriminalität gelten, deren Aktivitäten zu ernsthaften Gefährdungen in vielen Lebensbereichen führen, insbesondere durch Drogenhandel, Korruption, Förderung der illegalen Migration und andere Delikte. Die derzeitigen Konfliktherde in Zentralasien, Afrika und anderen Weltgegenden werden auch die Kommunikationsumwelt nachhaltig beeinflussen.

Wir stehen zu Beginn des 21. Jahrhunderts vor Herausforderungen, hervorgerufen durch die fortschreitende Entwicklung der Waffentechnologie und ihres Einsatzes wie auch durch die Informations- und Kommunikationstechnologie, deren Auswirkungen nicht absehbar sind. Die Reaktion des Staates, nämlich die Überwachungs- und Kontrollmaßnahmen zur Abwehr terroristischer Angriffe beständig auszuweiten, könnte die Demokratie westlicher Prägung nachhaltig verändern.

Seit Erscheinen der ersten Auflage dieses Werkes[9] im Jahre 2007 sind mit Blick auf das Thema Kommunikation tiefgreifende politische und technische Veränderungen zu konstatieren, die aus Sicht des Autors eine vollständige Überarbeitung des Werkes erforderlich machten. Auf die umfassende Darstellung von Schutz- und Abwehrmaßnahmen gegen Angriffe auf Kommunikationssysteme aller Art wurde wegen der Komplexität der Materie bewusst verzichtet, da diese den Rahmen dieses Werkes sprengen würde. Hier wird auf die reichlich verfügbare Fachliteratur zum Thema verwiesen.

8 Die Nachrichten- und Sicherheitsdienste der Vereinigten Staaten bemühen sich im Rahmen des „Information Sharing“ nachhaltig um Zugriff auch auf andere Datenbestände in der EU, deren letzte Konsequenzen nicht endgültig abgeschätzt werden können.

9 Informationskrieg und Cyberwar: Die unbekannte Gefahr, Stuttgart 2007.

Konturen des Informationskrieges

Neudefinition der Rolle der Nachrichtendienste

Nachrichtendienste bzw. deren Mitarbeiter, Organisationen, eingesetzte Technik und angewandte Verfahren waren und sind noch heute mit der Aura des Geheimnisvollen umgeben. Dies hat sich auch seit dem Ende des Kalten Krieges im Wesentlichen nicht geändert. Misserfolge der Nachrichtendienste werden durch die Presse naturgemäß weit häufiger als deren Erfolge publiziert. Besonders die weltweite und regionale Erfassung eigener und die Aufklärung fremder elektromagnetischer Ausstrahlungen aller Art ist neben dem Einsatz klassischer Nachrichtenbeschaffungs- und -gewinnungsmethoden durch den Einsatz von Agenten und die Abschöpfung offener Quellen in den vergangenen Jahren ein wesentlicher Bestandteil des Auftrages eines jeden nationalen Nachrichtendienstes geworden. Daher unterliegen dessen Personal, Mittel, Verfahren und Methoden zur Nachrichtengewinnung wie auch die besonderen regionalen Interessengebiete und die Ergebnisse der Beschaffung und Gewinnung meist einem besonderen Schutz, um sie vor möglichen Bloßstellungen zu schützen. Deren Folgen können für einen Nachrichtendienst, insbesondere in Krisen und bei kriegerischen Auseinandersetzungen, zu unabsehbaren Konsequenzen führen. Derartige Vorgänge beeinflussen natürlich auch die Partnerbeziehungen eines Nachrichtendienstes so nachhaltig, dass sie durch einen befreundeten Partnerdienst eingeschränkt oder gar gänzlich abgebrochen werden können.

In den letzten Jahren ist zu den klassischen Aufgabenfeldern der nationalen Nachrichten- und Abwehrdienste und der Strafverfolgungsbehörden zunehmend die Überwachung der geschäftlichen und privaten Telekommunikationsbeziehungen hinzugekommen, die eine immer wichtigere Rolle bei der Nachrichtengewinnung und Strafverfolgung durch die nationalen Behörden spielt. Im Verbund mit der staatlichen und privaten Video-Überwachung der öffentlichen und privaten (betrieblichen) Räume und gerichtlich angeordneter Lausch- und Kommunikationsüberwachungsmaßnahmen ergeben sich hier bisher nicht erwartete Ansatzmöglichkeiten der individuellen zielgerichteten Überwachung durch die nationalen Behörden und Dienste. Die Nachrichtendienste fremder Staaten mit entsprechenden technischen Voraussetzungen bedienen sich in den letzten Jahren vermehrt der Möglichkeiten, die ihnen die grenzüberschreitende Überwachung des Fernmeldeverkehrs und die Erfassung elektronischer Ausstrahlungen aller Art bieten. Hinzu kommen die umfassenden Möglichkeiten, die sich aus dem Eindringen in Kommunikations- und Datenverarbeitungssysteme und Rechnernetzwerke, auch befreundeter Staaten, für Nachrichtendienste ergeben. Nachrichtendienste verstanden sich schon immer als nationale

Institutionen, die schon aus Gründen des Eigenschutzes und der Abschirmung vor Angriffsversuchen fremder Nachrichtendienste bestrebt waren und sind, ihre Quellen, Mittel, Methoden und Ergebnisse vor befreundeten Nationen und deren Nachrichtendiensten zu schützen. Dies schloss zeitlich und örtlich begrenzte Zweckbündnisse mit Alliierten während des Kampfes gegen einen gemeinsamen Gegner, so zum Beispiel zwischen den USA und Großbritannien während des Zweiten Weltkrieges im Rahmen der Operation ULTRA, grundsätzlich nicht aus. Aber auch hier wurden nicht alle Ergebnisse zwischen den Partnern vollständig ausgetauscht.

Diese Politik wurde auch nach dem Ende des Zweiten Weltkrieges durch die beteiligten Nationen fortgesetzt und fand in dem zwischen den USA und Großbritannien in den 1940er Jahren geschlossenen UKUSA-Agreement seinen Niederschlag. Das später andere Nationen, so zum Beispiel Kanada, Australien und weitere Nationen, diesem Übereinkommen beitreten konnten, änderte nichts an der eingeschränkten Weitergabe von Informationen durch die Dienste der Vereinigten Staaten und Großbritanniens, die besonders aus der Fernmeldeaufklärung (COMINT) gewonnen werden konnten. Hierbei handelte es sich im Wesentlichen um die Zugangsmöglichkeiten westlicher SIGINT-Dienste in die geschlossenen, hochrangigen Kommunikationsverbindungen zwischen Regierungs- und Parteidienststellen, die Kommunikation der Nachrichtendienste und die militärischen Führungsverbindungen von operativer und strategischer Bedeutung des damaligen Warschauer Paktes. Dies schloss jedoch nicht aus, dass sich die westlichen SIGINT-Dienste auch für die Kommunikation blockfreier befreundeter und neutraler Staaten interessierten. Auch im vergangenen Kalten Krieg galt dieses Prinzip zwischen Partnerdiensten, das, soweit aus offenen Quellen ersichtlich, auch heute noch unverändert in Kraft ist. Diese rigorose Politik der Geheimhaltung der Mittel, Methoden und Ergebnisse kann auch heute noch beobachtet werden und gilt weiterhin für Teilergebnisse der Kryptologie aus dem Zweiten Weltkrieg.

Auch nach Ende des Kalten Krieges sind die Nachrichtendienste und ihre Fähigkeiten wichtiger denn je für die Gewinnung und Beschaffung von Informationen aller Art und dienen damit auch der Früherkennung möglicher krisenhafter Entwicklungen, sofern die Erkenntnisse der Dienste durch die jeweilige politische Führung akzeptiert und in entsprechende Reaktionen umgesetzt werden. In Krisen und im Krieg sind die Nachrichtendienste, insbesondere deren Fähigkeiten zur Technischen Aufklärung, das einzige Instrument, das in der Lage ist, Informationen zeitgerecht zu beschaffen.

Mit dem Anwachsen terroristischer Gewalttaten, besonders durch islamistisch gesteuerte Terrorbewegungen, begann sich das Bedrohungsbild, mit dem sich die westliche Welt plötzlich konfrontiert sah, zu wandeln. Nicht erst mit dem 11. September 2001 war eine neue Situation entstanden, die ein radikales Umdenken und eine Reorganisation der Nachrichtengewinnung und -beschaffung durch die westlichen Dienste erforderte. Damit war der Kalte Krieg endgültig beendet und das Zeitalter des „Informationskrieges“ hatte begonnen.

Nach wie vor spielen sowohl Ressortegoismen als auch interne Verteilungskämpfe zwischen den nationalen Nachrichten- und Sicherheitsdiensten eine

entscheidende Rolle. Auch zeigte sich bei den meisten westlichen Diensten sehr bald, dass diese bei der Auswertung der täglich eingehenden Informationen an die Grenzen der Auswertekapazität gelangten, und zwar sowohl was den Einsatz qualifizierter Auswerter, insbesondere mit Fremdsprachenkenntnissen, als auch was den Einsatz technischer Hilfsmittel betraf. Hier war das Ausmaß des „Information Overload" unübersehbar. In der Folgezeit entwickelten insbesondere die Nachrichten- und Sicherheitsdienste der Vereinigten Staaten eine Vielzahl von Programmen zur besseren Auswertung der eingehenden Informationen. Ob diese allerdings erfolgreich waren, muss bezweifelt werden. Besonders die seit einigen Jahren zu beobachtende Vernetzung der Sensoren im militärischen Bereich bis hin auf die Ebene des „Einzelschützen" unter dem Stichwort „Situational Awareness" wird den Einzelnen in einer Weise belasten, die es ihm in einer Kampfsituation nahezu unmöglich machen wird, seinen Auftrag durchzuführen. Es besteht kein Zweifel, dass derartig umfassende Informationen auf höheren Ebenen der militärischen Führung zur Entscheidungsfindung unbedingt notwendig sind. Allerdings sollte hier auch die menschliche Aufnahmefähigkeit mit in Betracht gezogen werden. Je mehr Informationen vorliegen, um so schwerer wird es dem Auswerter/Feindlagebearbeiter im Nachrichtendienst fallen, genau die für den Ausgang des Gefechts entscheidenden Informationen aus der Vielzahl der zur Verfügung stehenden Informationen, zudem noch unter Zeit- und Entscheidungsdruck, herauszufiltern. Es sind auch Zweifel angebracht, ob die in den Nachrichtendiensten und Sicherheitsbehörden aus der Kommunikationsüberwachung und sonstigen Datensammlungen anfallenden Daten tatsächlich erforderlich sind und auch dementsprechend genutzt werden können. Hier werden die Dienste bald an technische Grenzen stoßen. Auch hier wäre weniger mehr, wenn sich die Überwachungsmaßnahmen gezielt gegen Terrorismusverdächtige oder tatsächliche Terroristen richten würden. Die Aufgaben der Nachrichten- und Sicherheitsdienste können wie nachfolgend umrissen werden:

- **Strategischer Nachrichtendienst:** Beschaffung und Gewinnung von Informationen und Gewinnung von Erkenntnissen mit langfristiger Bedeutung aus den Interessengebieten und Bereichen für die politische und militärische Führung.
- **Operativer Nachrichtendienst:** Beschaffung und Gewinnung von aktuellen Informationen zu politisch, militärisch und wirtschaftlich bedeutsamen Themen aus regional begrenzten Bereichen.
- **Militärischer Nachrichtendienst:** Beschaffung und Gewinnung von aktuellen Erkenntnissen zur Wehrlage fremder Staaten, zur Sicherheitslage im eigenen Bereich und den Einsatzgebieten, und zwar sowohl im operativen als auch im taktischen Bereich. Dies schließt naturgemäß auch die Bearbeitung strategischer, operativer und taktischer Probleme mit ein.
- Im zivil geführten **Bundesnachrichtendienst** (BND) werden sowohl Aufgaben der Nachrichtenbeschaffung mit nachrichtendienstlichen Mitteln und Methoden, der Nachrichtengewinnung mit technischen Mitteln und aus offenen Quellen, sowohl auf der strategischen als auch auf der operativen Ebene, als auch militärische Nachrichtenbeschaffung und -gewinnung

wahrgenommen. Insbesondere in den Einsatzgebieten der Bundeswehr führt dies zu einer Verwischung der Grenzen zwischen zivilem und militärischem Nachrichtendienst, wie das jüngste Ereignisse in Afghanistan gezeigt haben. Hier haben offenbar sowohl Kräfte des Nachrichtendienstes als auch Kräfte der militärischen Nachrichtengewinnung und Aufklärung (NG&A) kooperiert.

- **Abwehr- und Sicherheitsdienste:** Die meist ziviler Führung unterstellten Abwehr- und Sicherheitsdienste nehmen vorwiegend Aufgaben der Spionageabwehr und den Schutz des Staates gegen Subversion, Zersetzung und Wirtschaftsspionage wahr. In Einzelfällen sind diese Dienste auch an die nationalen Strafverfolgungsbehörden angegliedert.
- Als Sonderfall können das **Bundesamt für Verfassungsschutz** und die entsprechenden **Landesämter oder Landesbehörden für Verfassungsschutz** in Deutschland betrachtet werden, da in Deutschland aus historisch bedingten Gründen ein Trennungsverbot zwischen Strafverfolgungsbehörden und Nachrichtendiensten besteht. Allerdings sind Bestrebungen erkennbar, dieses Trennungsgebot zwischen Nachrichten- und Sicherheitsdiensten einerseits und den Strafverfolgungsbehörden andererseits im Rahmen der Terrorbekämpfung zu relativieren. Zum klassischen Auftrag der nationalen Abwehr- und Sicherheitsdienste gehören die Gewinnung und Beschaffung von Erkenntnissen zur Sicherheitslage. Aspekte der Spionageabwehr (Counter Intelligence) sind dabei besonders zu berücksichtigen, jedoch werden derartige Funktionen in der Regel durch gesonderte nationale Dienste wahrgenommen, die jedoch bei den jeweiligen Nachrichtendiensten auf enge Zusammenarbeit angewiesen sind. In den letzten Jahren wurden die Nachrichten- und Sicherheitsdienste wie auch die klassischen Polizeibehörden vermehrt in die Bekämpfung des internationalen Terrorismus und der internationalen organisierten Kriminalität mit eingebunden. Daneben gewinnen und beschaffen andere Zweige der staatlichen Verwaltung, wie Finanzaufsicht oder Steuer- und Zollbehörden, Informationen zu Personen und Sachverhalten, um diese gegebenenfalls in Ermittlungsverfahren einzuführen. Dabei hat die Kommunikationsüberwachung in den letzten Jahren an Bedeutung gewonnen, insbesondere, wenn Informationen aus der Kommunikationsüberwachung mit bereits vorhandenen Daten von mehr oder minder Betroffenen zusammengeführt und ausgewertet werden. Die Europäische Union verstärkt auf Druck interessierter politischer Kreise, hier insbesondere Großbritanniens und der USA, hin zu einer totalen Informationskontrolle und Überwachung der Bevölkerung. Auf die rechtliche Problematik bei der Bearbeitung von Fällen von Gegenspionage durch Strafverfolgungsbehörden (Legalitätsprinzip und Trennungsgebot) sei hier besonders hingewiesen.

  In den letzten Jahren haben insbesondere die Sicherheitsbehörden bei der Gewinnung von Informationen vermehrt auf die Kommunikationsüberwachung zurückgegriffen, ohne dass bisher endgültig der Beweis erbracht werden konnte, dass die Kommunikationsüberwachung tatsächlich als taugliches Mittel zur Abwehr von terroristischen Straftaten gelten kann.

> Allein der aus der künftigen Vorratsdatenspeicherung zu erwartende Umfang von Daten wird die Behörden bald an die Grenzen ihrer Auswertefähigkeit führen.

Dieses Werk widmet sich vor allem den Interdependenzen zwischen der Gewinnung von Nachrichten aller Art[10] mithilfe technischer Mittel, sei es durch Elektronische Aufklärung (Electronic Intelligence)[11], signalerfassende Aufklärung (SIGINT), Fernmeldeaufklärung (COMINT), Kommunikationsüberwachung (Lawful Interception) und, soweit erforderlich, durch Beschaffung von Informationen mithilfe menschlicher Quellen (HUMINT)[12] im Rahmen der Nachrichtengewinnung und Aufklärung (NG&A) durch nationale Nachrichten- und Sicherheitsdienste sowie überstaatliche Einrichtungen. Soweit erforderlich wird auch auf die raumgestützte abbildende (geographische) Aufklärung eingegangen. Besonders berücksichtigt werden Informationsoperationen im Rahmen der netzwerkzentrierten Kriegführung (netzwerkzentrierte Operationen [NetOpFü]) sowie der Business Intelligence[13] und die Kommunikationsüberwachung durch die Nachrichten- und Sicherheitsdienste. Dabei sollen auch Problemstellungen der „vernetzten Sicherheit" nicht außer Acht gelassen werden. In diesem Zusammenhang werden auch Kritische Informationsinfrastrukturen und deren Bedeutung für die Funktion des Staates und der Wirtschaft betrachtet. Dort wo erforderlich wird auch auf die besondere Rolle militärischer und paramilitärischer Spezialeinsatzkräfte eingegangen.

Aktionsfelder des Informationskrieges

Im Bereich des Nachrichtenwesens (Intelligence)[14] und der elektronischen Aufklärung kursiert eine Vielfalt von Begriffen und Bezeichnungen für gleichartige Tätigkeiten. Soweit möglich, wurde die nationale Terminologie für Begriffe

---

10 In diesem Zusammenhang sind Nachrichten mit dem Begriff Informationen gleichzusetzen.

11 Einen guten Überblick über die komplexe Materie gibt Grabau, R.: Funküberwachung und Elektronische Kampfführung, Stuttgart 1986. Das Werk enthält die grundlegenden Informationen zur Technik und zu den Verfahren der Fm/EloAufkl (Signals Intelligence).

12 Im Kontext hierzu soll auf die umfangreiche Literatur zur Spionage und zu nachrichtendienstlichen Operationen verwiesen werden, da eine Behandlung dieses Themas den Rahmen des Werkes sprengen würde.

13 Hier als Sammelbegriff für staatlich gelenkte Wirtschafts- und Konkurrenzspionage verstanden.

14 Im anglo-amerikanischen Sprachraum ist hierfür der Begriff „Intelligence" gebräuchlich. Zu Recht weisen Paul Todd und Jonathan Bloch in ihrem Buch „Globale Spionage" (Berlin 2003) daraufhin hin, dass der Begriff im Deutschen keine Entsprechung hat: „*Intelligence* geht weit über die Arbeit … der Geheimdienste hinaus und umfaßt ebenso den Bereich der militärischen Aufklärung sowie die Arbeit staatlicher und nichtstaatlicher Organisationen." Allgemein kann mit Todd und Bloch gesagt werden, dass Intelligence „Informationen mit einem Bezug zur nationalen Sicherheit" betrifft, die „zur Bekämpfung eines tatsächlichen oder auch nur potentiellen Gegners erforderlich sind"; vgl. S. 12–18.

des Nachrichtenwesens verwendet. Nachfolgende Definitionen sollen vorab zur Klärung der Begriffe beitragen:

Elektronische Kampfführung (Electronic Warfare)

umfasst ohne Rücksicht auf die Art der Kommunikationsbeziehung alle Maßnahmen der Aufklärung, Unterstützung, Gegen- sowie Schutzmaßnahmen im gesamten elektromagnetischen Spektrum. Das können zum Beispiel Funk, drahtgebundene Verbindungen, Lichtwellenleiter, Rechner, Netzwerke, Bündelfunk aller Art einschließlich UTMS GMRS, GPRS sowie TETRA, TETRA 25, TETRAPOL, Fernwirkanlagen, Wireless Local Area Networks (WLAN) und ähnliche Anwendungen sein. Dies betrifft auch funkgebundene militärische und zivile Führungssysteme aller Art (Luftverteidigung, militärische Ortungs- und Leitsysteme wie auch Systeme der Sicherheitsbehörden und des Katastrophenschutzes in der zivilen und militärischen Flugsicherung u. a.).

Elektronische Aufklärung (COMINT/ELINT/SIGINT),

kurz ELINT (Electronic Intelligence), hat die Aufgabe, Strahlungsquellen zu orten, zu identifizieren, technische Parameter zu evaluieren und im Verbund mit der Fernmeldeaufklärung die Erstellung von Nutzungs- und Bewegungsprofilen zu ermöglichen; so zum Beispiel die Ortung eines Mobiltelefons, die Identifizierung und Auswertung der Nachrichteninhalte und damit auch die Identifizierung des möglichen Nutzers und seiner Kommunikationsbeziehungen oder das Erstellen von Aktivitäts- und Bewegungsprofilen. Auch ist durch Manipulation des Mobiltelefons das Abhören von Gesprächen, auch bei scheinbar abgeschaltetem Mobiltelefon, technisch möglich. Die Erfassung technisch/betrieblicher Parameter bei drahtlosen (Local Area Network [LAN], Wide Area Network [WAN], Mobiltelefon) und anderen Anwendungen sowie die parasitäre Abstrahlung von Informations- und Kommunikationsanlagen richtet sich nach den örtlichen Gegebenheiten. In derartigen Fällen ist jedoch ein größerer professioneller Aufwand im technischen Bereich notwendig und erfordert Nähe zum Aufklärungsobjekt. Unabhängig hiervon können auch mit relativ einfachen Mitteln einzelne WLAN-Hot Spots identifiziert, deren Kommunikationsbeziehungen erfasst und die Inhalte ausgewertet werden.

Die Fernmeldeaufklärung[15] erfasst Kommunikationsbeziehungen und elektronische Strahlungen sowie Kommunikationsinhalte aller Art im gesamten derzeit nutzbaren Frequenzspektrum ohne Rücksicht auf das verwendete Medium (Funk, Draht, Lichtwellenleiter) und klärt sie auf. Zu unterschieden ist also zwischen:

- COMINT = Communications Intelligence = Fernmeldeaufklärung
- ELINT = Electronic Intelligence = Elektronische Aufklärung

15 Jertz, W., in: BND: Information Warfare – Kampf mit und um Informationen, Bonn 2003, S. 40.