Inhaltsverzeichnis

„Internationaler Terror macht auch vor den Grenzen Österreichs nicht halt. Manipulation und Rekrutierung von Personen werden zur Bedrohung. Diese Phänomene müssen an der Wurzel bekämpft werden.“

Regierungsprogramm
für die
XXIV. Gesetzgebungsperiode

Vorwort

Nachrichtendienste werden seit ihrer Begründung von einem grundlegenden Problem begleitet – sie können nicht auf gesicherte Informationen aufbauen, von ihnen werden aber konkrete Einschätzungen und Aussagen erwartet. Warnen sie zu oft, geraten sie als professionelle Schwarzseher in Verruf und laufen Gefahr, nicht mehr Ernst genommen zu werden. Kommt es jedoch beispielsweise zu Terroranschlägen so wird ihnen automatisch vorgeworfen, versagt zu haben. Es gibt wohl keine andere Branche, die einem so starken Dilemma unterworfen ist wie der Bereich des Nachrichtenwesens. Dazu gesellt sich das Problem, dass ihre Arbeit zumeist im Verborgenen erfolgt und sie nur höchst selten Gelegenheit haben, falsche Anschuldigungen zu widerlegen oder die Sinnhaftigkeit und den Wert ihrer Tätigkeiten öffentlich darzustellen.

An dieser Stellte ist jedoch auch anzuführen, dass Nachrichtendienste eine besondere Vertrauens- und Verantwortungsstellung innehaben, dass sie politisch missbraucht werden oder sie selber ihre Machtposition, die im Extremfall über Krieg oder Frieden entscheiden kann, missbrauchen können. Eine unabhängige politische Kontrolle über staatliches Nachrichtenwesen ist daher von eminenter Bedeutung, wenngleich sie sich naturgemäß wesentlich diffiziler gestaltet als etwa im Bereich der öffentlichen Verwaltung. Denn viele Informationen bedürfen absoluter Geheimhaltung – ein Aspekt, der Massenmedien ihres Wesens wegen und politischen Repräsentanten manchmal aus populistischen oder anderen Gründen zuwiderläuft.

Nach dem Ende des Kalten Krieges Anfang der 1990er Jahre haben sich infolge des geänderten Konflikt- und Bedrohungsbildes radikale Veränderungen für die Nachrichtendienste ergeben. Spätestens die Terroranschläge vom 11. September 2001 in den USA sowie 2004 in Madrid und 2005 in London haben auch den größten Skeptikern bewiesen, dass Gefahren existieren und Schutz nur durch systematisch gesammeltes und ausgewertetes Wissen und darauf beruhenden Gegenmaßnahmen erzielt werden kann. Dass sich das in der Praxis nicht so einfach darstellt, haben die Untersuchungen in den USA über das „Versagen“ der US-Geheim-

dienste im Vorfeld der Terroranschläge gezeigt. Mittlerweile wurde aber auch klar, dass es unmöglich ist, zu einem lückenlosen Gefahrenbild zu kommen und dass vor allem Industriestaaten verwundbar sind und bleiben werden. Damit haben sich die Anforderungen an Nachrichtendienste aber ins Unermessliche gesteigert. Sie unterliegen gleichzeitig einem enormen Erwartungs- und Anpassungsdruck, der schon dazu führte, dass private Spezialfirmen auf breiter Front in dieses Metier eindringen. Ein Umstand, der erhöhter Aufmerksamkeit und Wachsamkeit bedarf – wie die Autoren dieses Bandes besonders hervorheben.

Wolfgang Braumandl und Anton Dengg, zwei Forscher des Instituts für Friedenssicherung und Konfliktmanagement (IFK) an der Landesverteidigungsakademie, die sich mit der Entwicklung des Konflikt- und Bedrohungsbildes auseinandersetzen, bringen dem Leser in diesem Band nicht nur die besonderen Anforderungen an Nachrichtendienste nahe. Sie erklären auch, wie sie grundsätzlich funktionieren und welche Methoden zur Anwendung gelangen. Vor allem aber machen Braumandl und Dengg darauf aufmerksam, dass sich heutige „Feinde“ wie etwa terroristische Gruppierungen mittlerweile ähnlicher oder gleicher Mittel und Methoden bedienen wie Nachrichtendienste – allerdings mit dem Unterschied, dass sie keinen rechtlichen Beschränkungen unterliegen und auch in den eigenen Reihen rücksichtslos agieren.

Mit „Transforming Intelligence Services“ von Fred Schreier, einem Schweizer Experten, und dem vorliegenden Werk von Braumandl und Dengg hat das IFK im Jahr 2010 bereits zwei Bände zu Nachrichtendiensten und Entwicklungen in diesem Bereich herausgegeben. Das Institut möchte damit einen Informationsbeitrag zu einem unterbelichteten, aber an Bedeutung gewinnenden Thema leisten. Denn je komplexer und unübersichtlicher Gefahren- und Bedrohungen werden, desto dringlicher wird es sein, durch ein funktionierendes Netzwerk unterschiedlicher Informations-, Analyse- und Beratungssysteme zu einem möglichst klaren Lagebild zu gelangen. Nur dann erscheint es möglich, jenen Schutz zu gewährleisten, den sich die Allgemeinheit erwartet.

Der Leiter IFK
Walter Feichtinger

Einleitung

Wenn die Frage nach der Bedeutung von Intelligence in der internationalen Terrorismusbekämpfung gestellt wird, dann sind zuerst die dazu notwendigen Arbeitsbegriffe sowie ihre strukturellen Implikationen für die moderne Staatlichkeit abzuklären. Sicher ist, dass diese Frage eher selten von der Fachwelt und den Medien aufgegriffen wird, um sie einer breiteren Öffentlichkeit näher zu bringen. Intelligence ist jenes staatliche Instrument, mit dem westliche Industriestaaten Terrorzellen bekämpfen können, ohne gleichzeitig die gesamten rechtsstaatlichen und demokratischen Prinzipien moderner Staatlichkeit untergraben zu müssen. Dass Terrorismusbekämpfung mit demokratiepolitischen und rechtsstaatlichen Grundsätzen vereinbar ist, haben namhafte Intelligenceexperten bereits ausgeführt.[1]

Die Bandbreite an Möglichkeiten zur Bekämpfung terroristischer Vereinigungen könnte breiter diskutiert werden, um zum Einen bestehende Optionen zur Terrorismusbekämpfung näher bestimmen zu können, und zum Anderen, um das öffentliche Verständnis über Intelligenceorganisationen zu stärken. So kann die Bevölkerung z. B. nachrichtendienstliche Bemühungen in erster Linie als „Schutz“ wahrnehmen und nicht als ein abstraktes Phänomen eines „big brother is watching you“. Damit versucht die vorliegende Arbeit zwei zentrale Fragen zu klären: erstens, warum sich moderne Nachrichtendienste an die neuen Bedrohungen anpassen müssen, und zweitens, wie dieser Transformationsprozess aussehen könnte. Beide Fragen werden im Lichte eines modernen Demokratieverständnisses behandelt. Die Transformation wird also als eine Möglichkeit angesehen, bestehende institutionelle Strukturen und bürokratische Arrangements der Staatssicherheit den neuen Bedrohungsbildern anzupassen. Wissenschaftliche Untersuchungen haben gezeigt, dass „konservative“ Arbeitsmethoden in den Bereichen der Beschaffung und Analyse

[1] Vgl. hierzu Sims, Jennifer E.: Introduction. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005 und Netanyahu, Benjamin: Fighting Terrorism – How Democracies Can Defeat the International Terrorist Network. New York 2001 (Erstveröffentlichung 1995).

zur Terrorismusbekämpfung nicht mehr ausreichen. In den USA wird daher die Frage nach einer nachrichtendienstlichen Optimierung gestellt, die ohne große politische Vorbehalte (im Vergleich zu europäischen Ländern) diskutiert wird. Dabei werden die terroristischen Anschläge vom 11. September 2001 als Beispiel einer „nachrichtendienstlichen Fehlleistung“ angeführt. Um in Zukunft die Wahrscheinlichkeit von solchen Fehlleistungen zu minimieren, könnte eine Transformation nachrichtendienstlicher Strukturen vier intelligencespezifische Faktoren konzeptionell erfassen:

a) Schaffung eines adäquaten kognitiven und sozialen Umfeldes („mind-set“ und „imagination“);
b) Einführung des Prinzips der „informed“ Policy-Entscheidungen (Frage der Dissemination);
c) Verbesserung nachrichtendienstlicher Fähigkeiten (Beschaffung und Analyse);
d) Optimierungen im Intelligencemanagement.

Diese vier Bereiche werden von Jennifer E. Sims als Kernelemente nachrichtendienstlicher Transformation betrachtet. Resultat nachrichtendienstlicher Adaptionsbestrebungen könnte eine gezielte Aufklärung („precise targeting“[2]) und eine optimierte analytische Ausrichtung sein, die den politischen Entscheidungsprozess proaktiv unterstützt. In diesem Sinne könnte eine erfolgreiche Transformation zum entscheidenden Faktor defensiver und offensiver Maßnahmen der Terrorismusbekämpfung werden.[3]

[2] Vgl. Sims, Jennifer E.: Introduction. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. X.
[3] A.a.O.

Aufbau der Arbeit

Die vorliegende Studie basiert auf einem interdisziplinären Forschungszugang, der politikwissenschaftliche, ideologische, staatstheoretische und religionsimmanente Aspekte der Terrorismusbekämpfung mittels nachrichtendienstlicher Methoden umfasst. Dieser Zugang wird dort hervorgehoben, wo die ideologische Fundierung des gezielten Kampfes radikaler Fundamentalisten gegen den Okzident strukturelle Adaptionsbemühungen im Intelligencebereich hervorruft (z. B. Anstellung von Experten für Ideologie, Arabistik, arabische Kultur und Religion). Wesentlich für die Vermittlung von speziellem Wissen und Expertisen ist eine prägnante und klare Darstellung ideologiespezifischer Leitideen radikaler Islamisten. Gegen islamistische Radikalisierung und der Unterbindung von Rechtfertigungsideologien für Gewaltanwendung ist eine breitenwirksame innergesellschaftliche Diskussion unumgänglich.

Die Studie gliedert sich in folgende Abschnitte: Zu Beginn wird auf die Evolution des Intelligencebegriffes eingegangen, um die veränderten gesellschaftlichen und sicherheitspolitischen Rahmenbedingungen zu verdeutlichen. Insbesondere der 11. September 2001 stellt hier eine deutliche Zäsur nachrichtendienstlicher Aufgabenstrukturen dar, die sich aus dem diffusen Bedrohungspotential herausbildete. In diesem Zusammenhang präsentiert die Studie eine begriffliche Konkretisierung, verdeutlicht unterschiedliche Definitionsversuche, erbringt eine historische Kontextualisierung und beleuchtet die paradigmatische Genese von Intelligence. In einem weiteren Abschnitt erfolgt die Erläuterung des nachrichtendienstlichen Transformationsaspektes, der die wesentlichen Schritte des nachrichtendienstlichen Produktionskreislaufes („intelligence cycle“) berücksichtigt. Ferner werden die technologischen Implikationen einer umfassenden Transformation, das Verhältnis von Politik und Intelligence, die Herausforderung einer engen Zusammenarbeit zwischen Intelligence und Militär und die Bedeutung privater Intelligencefirmen berücksichtigt. Dieser sehr spezielle Teilaspekt des „Outsourcing“ von intelligencerelevanten Aufgaben wurde von der Forschung bislang kaum beachtet. Im dritten Abschnitt werden im Lichte einer komparativen Analyse „der Feind“ und seine Intelligenceoptionen dargestellt. Es werden Parallelen zwischen Terrororganisationen und staat-

lichen Nachrichtendiensten aufgearbeitet. Zudem wird der Strategiebegriff von Terrororganisationen, die Unterstützung von staatlichen Nachrichtendiensten für Terrororganisationen, ihre Rekrutierungs- und Ausbildungsmethoden sowie ihre Arbeitsweise und Taktik erörtert. Dadurch ist es möglich, auf die geheimdienstlichen Strukturen von Terrororganisationen zu schließen. Das vierte Kapitel der Studie bietet entsprechende Ableitungen für Nachrichtendienste im Transformationskontext an. Ihr „Empfehlungscharakter" ist allgemeiner Natur und basiert auf wissenschaftlichen Erkenntnissen aus dem Intelligencebereich.[4] Die Ableitungen stellen eine „Nennung" von Optionen zur Optimierung nachrichtendienstlicher Abläufe dar. Das letzte Kapitel ist die Konklusion, sie stellt eine kurze Zusammenschau der Argumentationslinien der Studie dar.

[4] Vgl. hierzu auch Netanyahu, Benjamin: Fighting Terrorism – How Democracies Can Defeat the International Terrorist Network. New York 2001 (Erstveröffentlichung 1995).

Intelligence – Evolution eines Begriffes

Begriffliche Konkretisierung

Der Begriff „Intelligence“ war bis Ende der 1990er-Jahre ausschließlich in einschlägigen Fachkreisen bekannt. Selbst für die kontinentaleuropäische Politikwissenschaft war der US-amerikanisch geprägte Terminus für Aufklärung und Analyse weitgehend unbekannt. Während der „allgemeine Intelligencebegriff“ aufgrund des steigenden nachrichtendienstlichen Handlungsbedarfes im Rahmen der internationalen Terrorismusbedrohung verstärkt aufgegriffen wurde, blieben speziellere Fachtermini, wie z. B. strategischer, operativer und taktischer Intelligencebegriff, auch weiterhin unbeachtet.

Der allgemeine Intelligencebegriff setzt sich aus den lateinischen Begriffen „inter“ (zwischen) und „legere“ (zusammenbringen) zusammen und impliziert damit in seiner analytisch-methodischen Präferenz eine umfassende kontextuelle Erschließung seines Objektbereiches. Dieser kann beispielsweise politischer, wirtschaftlicher und militärischer Natur sein. Auf die Erschließung von Objektbereichen mittels (geheimer) Beobachtung und Analyse haben Machthaber bereits seit über zweittausend Jahren zurückgegriffen, um die Pläne ihrer Gegner, aber auch ihrer Verbündeten aufzuklären. Aufklärung sicherte Informationsdominanz gegenüber den politischen und militärischen Mitspielern, wodurch die Umsetzung eigener Ziele erleichtert wurde.

Der US-Intelligenceexperte Michael Warner bestätigt in seinem wissenschaftlichen Artikel in der CIA-Publikationserie „Studies in Intelligence“ das Fehlen einer allgemein akzeptierten Definition von Intelligence.[5] Für Michael Warner besitzt der Intelligencebegriff zumindest nachfolgende Kernelemente:[6]

[5] Vgl. Braumandl, Wolfgang, Desbalmes, Christian: Nachrichtendienstliche Kooperation der EU im Kampf gegen Terrorismus. In: Schriftenreihe der Landesverteidigungsakademie, 1/2007, Wien 2007, S. 11.
[6] Vgl. ebd., S. 12.

- Intelligence bedeutet systematisches Sammeln und Analysieren von offenen, halboffenen und geheimen Informationen für die nationale Sicherheit und das internationale Krisenmanagement;
- Intelligence setzt die Geheimhaltung von Quellen und Methoden der Informationsbeschaffung voraus;
- Intelligence bedeutet auch die Produktion und Dissemination von Informationen und
- die Anwendung von verdeckten Operationen zur Beeinflussung von Regierungen und Organisationen.

Auf den ersten Blick erscheinen diese Kernelemente nicht nur für die Arbeit staatlicher Nachrichtendienste zutreffend, sondern auch für Tätigkeiten größerer Terrorgruppierungen. Dieser Annahme nachgehend, soll über den Zweck von Intelligence geklärt werden: Über wen sollen eigentlich mittels Intelligence Informationen eingeholt werden? Nachdem von Ähnlichkeiten in der Arbeitsweise ausgegangen werden kann, ergibt sich eine weitere Vermutung: Profitieren Terrororganisationen von Arbeitsweisen staatlicher Nachrichtendienste? Die Bearbeitung dieser Fragen soll einen kleinen Überblick über mögliche Parallelen zwischen staatlichen Intelligenceorganisationen und transnationalen Terrorgruppierungen ermöglichen.

Definitionsversuche

Intelligence ist gem. New Oxford American Dictionary „the ability to acquire and apply knowledge and skills“ bzw. „the collection of information of military or political value“.[7] Für die Clarke Task Force der Hoover Commission befasst sich Intelligence „...with all the things which should be known in advance of initiating a course of action“.[8] Die Central Intelligence Agency (CIA) sieht intelligence als „knowledge and foreknowledge“. Wie auch im Artikel von Warner zum Ausdruck

[7] The New Oxford American Dictionary, Copyright 2005-2007, Apple Inc.
[8] Warner, Michael: Wanted: A Definition of „Intelligence“. Online-Dokument: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/pdf/v46i3a02p.pdf>, abgerufen am 18.9.2008.

kommt, wären aber die erwähnten Definitionsversuche zu kurz gegriffen, wenn Intelligence lediglich auf Informationswissen basiert. Offensichtlich birgt die Bedeutung von Intelligence weit mehr in sich als bloß eine Fokussierung auf nüchternes Informationswissen.

John A. Gentry sieht als Auftrag von Nachrichtendiensten hauptsächlich „… the responsibility for identifying issues of policy relevance, collecting and analyzing information, and issuing warnings".[9] Beim Sammeln von Informationen "… intelligence agencies identify information gaps (collection requirements) and develop means to fill them".[10] Japans Nachrichtendienste entdeckten z. B. 1941 eine Lücke bei den US-Streitkräften. Erkannt wurde, dass das Militär an Wochenenden operationelle Schwächen zeigte, was schließlich Japan in Pearl Harbor nützte und in einen Sieg verwandelte.[11] Das Finden von Schwächen des Gegners scheint ein nicht unerhebliches Ziel von Intelligencearbeit zu sein.

Effektiv hat Intelligence auch mit „Wissensvorsprung" zu tun. „Wissensvorsprung" vor allem aufgrund der Brisanz möglicher Schwächen eines Gegners oder/und die Vorhersagbarkeit des Verhaltens eines Gegenübers bei möglichen eintretenden Ereignissen. Wissen, das aufgrund seiner Brisanz nicht der gesamten Bevölkerung zur Verfügung steht, sondern lediglich einer kleinen Gruppe – wird zumeist als geheim oder als vertraulich eingestuft. Dieser Umstand macht es notwendig, dass nur eine „eingeschworene" Gruppe zum erhaltenen Wissen Zugang erhält.

Intelligence verlangt hoch komplexe Organisationen mit einem enormen Aufwand an Planungstätigkeiten. Komplexes strategisches Denken muss in klar definiertes operatives Handeln umgesetzt werden und vice versa. Dazu braucht es eine aufwendige Infrastruktur, was sich in hohen Kosten widerspiegelt.

[9] Gentry, John A.: Intelligence Failure Reframed. In: Political Science Quarterly. Summer 2008, S. 248.
[10] Ebd., S. 251.
[11] Ebd., S. 263.

Historische Kontextualisierung

Welche historische Bedeutung die „geheime Aufklärung“ für Politik, Militär und Gesellschaft hatte, verdeutlicht eine Analyse von staats- und friedenstheoretischen Arbeiten. Sie haben den Mehrwert einer funktionierenden geheimen Aufklärung bereits sehr früh erkannt. Der chinesische Meister des Krieges Sun Tse (500 v. Chr.) hat in seiner Darstellung über die Prinzipien der Kriegskunst der Spionage einen zentralen Stellenwert für erfolgreiche militärische Operationen beigemessen. Sun Tse widmet dem Handwerk der geheimen Aufklärung sogar ein eigenes Kapitel in seinem Buch über die Kriegskunst. In diesem Kapitel referierte er über die Vorgehens- und Verhaltensweisen von Spionen.[12] Ebenso deutlich wie Sun Tse hat auch Niccoló Machiavelli (1469-1527) dem klugen Herrscher empfohlen, das „Kriegshandwerk“ auch in Zeiten des Friedens nicht zu vernachlässigen. Es sei wichtig, so Machiavelli, sich auch im Frieden auf den Krieg vorzubereiten. Dabei spielte das Studium der Landschaften und der Geländeeigenheiten eine kriegsentscheidende Rolle. Detailkenntnisse über Landschaften ermöglichten es dem militärischen Genius, den Angriff oder die Verteidigung besser planen und durchführen zu können. Aber nicht nur auf der konkreten Ebene sah Machiavelli wesentliche Vorteile einer genauen Auskundschaftung des eigenen sowie des feindlichen Landes, sondern auch in theoretischer und politischer Hinsicht präsentieren sich „Il Principe“ und „Discorsi“ als eindrucksvolle Plädoyers für mehr Wachsamkeit und Realitätssinn im politischen Agieren auf der Basis guter Informationen. Für Machiavelli war das Wissen über die Ziele und Absichten politischer Akteure eine zentrale Kategorie für den politischen Machterhalt.[13] Neben Sun Tse und Machiavelli hatte auch der deutsche Offizier und Kriegstheoretiker Carl von Clausewitz (1780-1831) ähnliche Überlegungen angestellt. Für Clausewitz waren akkurate Lageinformationen über die Stärken und Schwächen des Feindes von entscheidender Bedeutung (z. B. überlegener/unterlegener Feind). Ähnliche Überlegungen hatte auch bereits Machiavelli in seinem Werk über die Kunst des Krieges vorweggenom-

[12] Clavell, James (Hrsg.): Sunzi – Die Kunst des Krieges. 1988, S. 149-159.
[13] Vgl. hierzu Zorn, Rudolf: Niccolo Machiavelli. Der Fürst. Stuttgart 1978 und Ders.: Niccolo Machiavelli. Discorsi. Stuttgart 1977.

men.[14] Allerdings bleibt Clausewitz hinter den Erwartungen im Hinblick auf eine umfassende Bewertung über die militärische Bedeutung von Nachrichten im Kriege zurück.[15] Für Clausewitz waren Informationen zu ungenau, um sich auf sie verlassen zu können. Die elaboriertesten ideengeschichtlichen Überlegungen zur Bedeutung von Informationen im Politischen finden sich daher bei Machiavelli und Sun Tse.

Eine erste systematische Aufarbeitung struktureller Wesensmerkmale von Intelligence auf strategischer Ebene lieferte schließlich der US-amerikanische Intelligenceexperte Sherman Kent in den 1950er-Jahren. Seine wissenschaftliche Abhandlung über Strategic Intelligence entstand vor dem Hintergrund der Ost-West-Konfrontation und unter dem Eindruck des klassischen Realismus als bestimmendes Paradigma in der internationalen Sicherheitspolitik.[16] Kent versuchte mit seinem Werk, den nachrichtendienstlichen Ablaufprozess zu präzisieren. Dabei standen seine Ausführungen eindeutig im Zeichen des Realismus nach Hans Morgenthau, in denen die menschliche Natur primär als machtorientierte Größe angenommen wurde (z. B. Streben nach Macht, Macht als Tauschgut für Sicherheit und Weiterentwicklung im politischen Wettstreit). Für Kent mussten nachrichtendienstliche Strukturen die internationale Realität sicherheitspolitischer Herausforderungen widerspiegeln. Dabei wurde die internationale Politik als anarchistisch begriffen. Intelligence stellte in diesem politischen Kontext eine immaterielle Waffengattung zur Formulierung und Umsetzung politischer Ziele dar.[17] Kent systematisierte seine Überlegungen über strategische, nachrichtendienstliche Fähigkeiten zur Bekämpfung des kommunistischen Vorherrschaftsstrebens. In diesem Fall waren alle nur erdenklichen Mittel zum Schutze der nationalen Sicherheit erlaubt. Das Fundament für das moderne Intelligencewesen wurde bereits während der Kriegswirren des

[14] Machiavelli, Niccolo: The Art of War: University of Chicago Press 2005.
[15] Vgl. Clausewitz, Carl von: Vom Kriege. Berlin 1999, S. 84-85.
[16] Kent, Sherman: Strategic Intelligence for American World Policy. Princeton University Press, 1966. In den USA wurde eine gleichnamige Fakultät „Sherman Kent School for Intelligence Analysis“ an der CIA-Universität etabliert. Die Zielsetzung dieser universitären Einrichtung ist die Vermittlung wissenschaftlicher Erkenntnisse der nachrichtendienstlichen Analyse an die zukünftigen Mitarbeiter der US-Nachrichtendienste.
[17] Vgl. a.a.O.

Ersten Weltkrieges gelegt, indem moderne Aufklärungsverfahren und -technologien angewandt wurden. Neben den operativen und taktischen Aufklärungserfordernissen kamen nun auch politisch-strategische und militär-strategische Analysen hinzu.

Nachrichtendienstliche Beschaffungsverfahren wurden in der Zwischenkriegszeit vor allem in den USA und Großbritannien weiterentwickelt, sodass die Wortbedeutung von Intelligence nun ausschließlich auf das staatliche Gewaltmonopol im nachrichtendienstlichen Aktionsumfeld angewandt wurde. Diese begrifflich-kontextuelle Wandlung verfestigte sich schließlich im Zuge des Zweiten Weltkrieges. Intelligence wurde bereits von den Alliierten als kriegsentscheidendes Element angesehen und daher mit hoher politischer Priorität versehen, sodass ein weitverzweigtes Netz an Informanten und technischen Beschaffungseinrichtungen etabliert werden konnte.

Die modernen nachrichtendienstlichen Aufklärungsmethoden des Kalten Krieges basierten auf den technischen Innovationen des Zweiten Weltkrieges, die in Verbindung mit neuen analytischen Auswerteverfahren den Intelligencebegriff als „Instrument“ des staatlichen Gewaltmonopols festigten. Dadurch, dass die Bedrohungslage sich ausschließlich aus der Staatsprämisse ableitete, wurden auch die nationalen Intelligencestrukturen dieser „Denkweise“ angepasst. Nachrichtendienste westlicher Länder, aber auch jene des damaligen Ostblockes, beschafften geheime und vertrauliche Informationen über die politischen Absichten, Strategien sowie über die militärischen Kapazitäten des jeweiligen Gegners. Substaatliche Mitspieler, die in Form von Rebellengruppen, Milizen oder Revolutionstruppen in den Ländern der Dritten Welt auftraten, wurden im Rahmen nationaler Sicherheitsstrategien zur Eindämmung der gegnerischen Einflusssphären nachrichtendienstlich gewürdigt. Man war sich über den zentralen Stellenwert des staatlichen Gewaltmonopols gegenüber nichtstaatlichen Akteuren bewusst. Unter den politischen Rahmenbedingungen des Kalten Krieges lag die legitime Macht ausschließlich beim Staat und nicht bei substaatlichen Mitspielern, wie beispielsweise Konzernen, einzelnen Firmen oder einflussreichen Persönlichkeiten. In dieses westfälische Machtkonzept waren alle politischen und gesell-

schaftlichen Prozesse eingegliedert und konnten so durch nachrichtendienstliche Supervision teilweise gesteuert werden.

Der Stellenwert von Intelligence unter aktuellen Strukturbedingungen („Weltrisikogesellschaft“[18]) unterliegt einem ständigen Wandel. Intelligence gehört in vielen westlichen Industrieländern zur „Kernstaatlichkeit“ mit der Fähigkeit zur gesellschaftspolitischen Supervision moderner Staatlichkeit. Diese Aussage bedarf jedoch einer Betrachtung entwicklungstheoretischer Implikationen moderner Nachrichtendienste, um die strukturellen Zusammenhänge zwischen institutionalisierter Kernstaatlichkeit[19] und den sich veränderten Bedrohungsbildern verdeutlichen zu können. Intelligence Studies[20] als eine mögliche Teildisziplin der Politikwissenschaft verweisen auf zwei markante Theorien für eine Erklärung erforderlicher Adaptionen im jeweiligen sicherheitspolitischen Kontext.

Modernes Intelligence

Rasante technologische Entwicklungen zu Beginn des 20. Jhdt. hatten weitreichende und nachhaltige Auswirkungen auf bestehende Intelli-

[18] Vgl. hierzu Beck, Ulrich: Weltrisikogesellschaft – Auf der Suche nach der verlorenen Sicherheit. Bonn 2007.

[19] Institutionalisierte Kernstaatlichkeit bezeichnet einen intelligence-basierten Entscheidungsfindungsprozess der Politik. Sie zeichnet sich durch informationelle Exklusivität und Klassifikationsebenen (Zugangsbeschränkungen zu Intelligenceprodukten) aus. Das Modell der nachrichtendienstlichen Kernstaatlichkeit basiert auf den Überlegungen von Peter Gill. Vgl. Gill, Peter: Policing Politics: Security Intelligence and the Liberal Democratic State. London 1994.

[20] Als Intelligence Studies versteht man in den USA eine Teildisziplin innerhalb der Politikwissenschaft zur systematischen und interdisziplinären Aufarbeitung über die Bedeutung von Intelligence (als Organisation, Thema und Methode) in der Politik. Referenzen zu diversen Politikfeldern und Politikbereichen, wie beispielsweise zur nationalen Sicherheit, Militär, innere Sicherheit, Sicherheitspolitik, Außenbeziehungen, Intelligence in Friedens- und Kriegszeiten, etc. werden durch wissenschaftliche Programme und Projekte abgedeckt.

gencestrukturen. Rudimentäre Beschaffungsmöglichkeiten[21] vergangener Zeiten wurden fortan mit technischen und auch wissenschaftlichen Aufklärungsansätzen versehen.[22] Dadurch konnten die Nachrichtendienste noch effektiver gegen erkannte Bedrohungen vorgehen. In diesem Zusammenhang kann man von einer weiteren Professionalisierung nachrichtendienstlicher Ablaufprozesse sprechen. Spätestens seit dem Zweiten Weltkrieg wird in Human Intelligence (HUMINT) und in Technical Intelligence (TECHINT) – aufgrund unterschiedlicher Innovationen nachrichtendienstlicher Aufklärungsarbeit – unterschieden.[23] Bei der Durchsicht wissenschaftlicher Arbeiten zum Intelligencethema ist noch eine weitere Untergliederung des modernen Intelligencewesens feststellbar, die die Adaptionsfähigkeit nachrichtendienstlicher Strukturen im Sinne der Transformation verdeutlicht: Hier kann von einer ersten Phase der Professionalisierung (Beginn 20. Jhdt. bis zu Beginn des Kalten Krieges) gesprochen werden. Die zweite Phase kann insgesamt als Perfektionierung nachrichtendienstlicher Aufklärungsverfahren (bis etwa 1990) bezeichnet werden. Schon das moderne Intelligencemodell verdeutlicht die Fähigkeit von Nachrichtendiensten, sich neuen sicherheitspolitischen Rahmenbedingungen anzupassen. Dies geschieht in der Regel mit institutioneller Nachhaltigkeit und methodischen Innovationen, wie der Intelligenceexperte Ernest R. May in seinem Beitrag „The Twenty-First Century Challenge For U.S. Intelligence“ an Hand des Beispiels der CIA verdeutlicht.[24]

---

[21] Als rudimentäre Beschaffungsansätze werden Informanten, das „Spitzelwesen“, Spione und Agenten bezeichnet. Damit wird der „einfachen“ bzw. rudimentären Informationsbeschaffung entsprochen (z. B. Schwarzes Kabinett).

[22] Vgl. Piekalkiewicz, Janusz: Weltgeschichte der Spionage. München 1993, S. 266-287.

[23] Vgl. Piekalkiewicz, Janusz: Weltgeschichte der Spionage. München 1993, S. 352-409 und Andrew, Christopher, Mitrochin, Wassili: Das Schwarzbuch des KGB – Moskaus Kampf gegen den Westen. Berlin 1999, S. 102-198.

[24] May, Ernest R.: The Twenty-First Century Challenge For U.S. Intelligence. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. 3-13.

Postmodernes Intelligence

Für den Intelligenceexperten Andrew Rathmell konstituieren die neueren sicherheitspolitischen Entwicklungen nach dem Ende des Kalten Krieges ein neues – „postmodernes" Intelligenceparadigma.[25] Der Begriff der Postmoderne wird im Intelligencekontext nicht notwendigerweise auf bestimmte gesellschaftliche Entwicklungsstufen bezogen, sondern vielmehr auf eine konfliktgeladene Umwelt, einen „Wissens- und Informationsüberschuss", neue gesellschaftspolitische Werte (postheroische Gesellschaft) sowie auf historische Erkenntnisse, wonach sich die Menschheit im historischen Rückblick nicht oder nur sehr marginal über ihren „Naturzustand" erhoben habe (z. B. Fortbestand des Krieges). Das postmoderne Intelligenceparadigma zeichnet sich durch drei Merkmalsausprägungen aus: a) Fragmentierung, b) diffuses Bedrohungspotential und c) Sozialisation und Identitätsbildung/-findung moderner Intelligenceorganisationen. Unter Fragmentierung ist die themenspezifische, institutionelle und geografische Zergliederung von nachrichtendienstlichen Aufklärungszielen, Aufgaben und Beschaffungsansätzen gemeint:[26] „ ... the intelligence community has to understand multiple, overlapping and often contradictory narratives. (...) postmodern intelligence has begun to 'discover' previously marginalized targets".[27] Als zweites Erkennungszeichen gilt die Aufklärung „diffuser Bedrohungspotentiale", die ohne strukturelle Einbindung in politische und gesellschaftspolitische Abläufe und Systeme nur sehr schwer beobachtet, überwacht und kontrolliert werden können („mysteries", z. B. Terrorismus versus „puzzles", z. B. Ost-West-Konfrontation):[28] „ ... contemporary intelligence is in the posi-

[25] Vgl. Rathmell, Andrew: Towards Postmodern Intelligence. In: Intelligence and National Security. Vol. 17. 3/2002, S. 87f.

[26] Vgl. ebd., S. 97f. Die These von einem postmodernen Intelligenceparadigmas wird von Robert D. Steele, Bruce D. Berkowitz, Allan E. Goodman, Gregory Treverton und Deborah Barger vertreten. Alle genannten Intelligenceexperten favorisieren ähnliche Umweltveränderungen als Beweis für ein neues Intelligenceparadigma.

[27] Rathmell, Andrew: Towards Postmodern Intelligence. In: Intelligence and National Security. Vol. 17. 3/2002, S. 97.

[28] „Mysterien" bezeichnen eine nachrichtendienstliche Fragestellung, die selbst mit intensiver Beschaffung nicht beantwortet werden kann, weil bspw. der Gegner selbst noch keine Entscheidung getroffen hat oder noch unschlüssig ist. „Puzzles" bezeichnen

tion of not even knowing if there is a single objective reality out there that it is trying to capture".[29] Neben der Fragmentierungsproblematik und dem diffusen Bedrohungspotential ist auch die Sozialisation und Identitätsbildung zu einem Problem für Intelligenceorganisationen geworden, da die Freund-Feind-Grenze nicht mehr eindeutig auszumachen ist:[30] „During the Cold War there was no doubt for whom and against whom the Western intelligence community worked. This is changing as it becomes unclear for which government department, for which state, for which multinational organization or, indeed, for which corporation, intelligence is being produced."[31]

Die Adaptionsfähigkeit von Nachrichtendiensten wird seither stark herausgefordert, weil sich in den 1990er-Jahren grundlegende Veränderungen einstellten, und zwar nicht nur in der sicherheitspolitischen Landschaft, sondern auch in Gesellschaft und Technologie. Dabei war die sogenannte „Friedensdividende" nach dem Ende des Kalten Krieges ein Hindernis für einen raschen Transformationsprozess im Intelligencewesen (rigoroser Einsparungskurs im Verteidigungsbereich der Staaten). Vielfach glaubte man in den 1990er-Jahren an ein Jahrhundert des absoluten Friedens. Die politische Gewaltrealität der Menschheit nach dem Ende der bipolaren Konfrontation wurde durch eine quasi weltanschaulich-neoliberale „Globalisierung" ersetzt. Sie wurde als „Allheilmittel" für die noch verbliebenen Probleme ausgegeben. Heute wissen wir, dass die neoliberale Globalisierung diverse Konfliktlinien vor allem in den Entwicklungsregionen vertiefte. Soziale Probleme und die zahlreichen bewaffneten Konflikte konnten nicht gelöst bzw. befriedet werden. Diese neoliberale Sichtweise behinderte auch die politischen Entscheidungseliten bei der Neuausrichtung staatlicher nachrichtendienstlicher Sicherheitsstrukturen, da sie kaum zusätzliche Budgetmittel für Staatsinstitutionen rechtfertigen wollten. Dadurch konnten die Proponenten der privatisierten Gewalt, wie beispielsweise des internationalen Terroris-

---

dagegen jene nachrichtendienstlichen Fragestellungen die einen konkreten Umstand aufklären und beantworten können.

[29] Ebd., S. 97.

[30] Während des Kalten Krieges waren die Fronten definiert, wodurch die jeweiligen Feindbilder eindeutig zu identifizieren waren.

[31] Ebd., S. 98.

mus und der organisierten Kriminalität, nahezu ungehindert arbeiten. Aber bereits in der zweiten Hälfte der 1990er-Jahre wurde die „Friedensutopie“ durch bewaffnete Konflikte am Balkan und in Afrika erschüttert. Die Tendenz Anfang bis Mitte der 1990er-Jahre, Nachrichtendienste primär zur Wirtschaftspionage – wie dies von den Franzosen, Briten und den USA praktiziert wurde – einzusetzen, war unter dem Eindruck eines fehlenden Feindes politisch motiviert. Gegenwärtig ist diese Entwicklung etwas in den Hintergrund getreten. Experten gehen jedoch davon aus, dass sie nach wie vor eine zentrale Rolle im Wettstreit um die besten Ideen und Verhandlungspositionen einnimmt. Politische Akteure (vor allem in den 1990er-Jahren) fokussierten kaum auf regionale Konflikte; sie beachteten regionale Krisenwarnungen nur am Rande. Daher agierten beispielsweise die europäischen Staaten in Bezug auf diverse regionale Konflikte nur zögernd und reagierten in der Regel viel zu langsam. Neben dieser politischen Dimension wurden Nachrichtendienste mit der Informationsrevolution konfrontiert. Sie veränderte nicht nur die Arbeitsweisen einer breiten Gesellschaftsschicht, sondern auch staatliche Institutionen; allen voran die Nachrichtendienste. Sie mussten nun neue Informationsmanagementprinzipien berücksichtigen und implementieren. Ihr Anspruch auf Informationsdominanz wurde durch den „CNN-Faktor“[32] herausgefordert. In letzter Konsequenz behaupteten sie jedoch ihre zentrale sicherheitsrelevante Position für den Staat. Vor allem die analytischen Fähigkeiten, die Fertigkeit qualifizierter Politikberatung und ihr rasches, unbürokratisches Handeln relativierten den indirekten Wettbewerbsdruck, der durch die modernen Info-/News-Sender entstand. Als eine methodische Neuerung innerhalb der Nachrichten-

[32] Nachrichten konnten durch den raschen Zugang und die technischen Möglichkeiten zur Verbreitung von Information in nahezu Echtzeit verbreitet werden. Medienkonzerne berichteten über politische Unruhen, Katastrophen, Terroranschläge, etc., noch ehe die Dienste die Information qualifiziert verarbeiten konnten. Politiker vertrauten auf den CNN-Faktor – also auf die Medien und ihrer Berichterstattung. Allerdings wurde dadurch nur das „halbe“ Wissen vermittelt. Die tatsächlichen Hintergründe und Zielsetzungen, die mit einem bestimmten Ereignis verbunden waren, mussten nach wie vor durch die Nachrichtendienste aufbereitet werden. Dennoch wuchs die Gefahr politischer Fehlentscheidungen auf der Grundlage mangelnder Information durch den Medienfaktor drastisch an.

dienste gilt die Verwendung von Open Source Intelligence (OSINT).[33] Beschaffung und Analyse werden durch qualitative und offen verfügbare Expertisen ergänzt. OSINT kann auch als eigenständige „Disziplin“ oder als Ergänzung zu anderen Intelligenceprodukten betrachtet werden. Der Vorteil von OSINT ist der geringe Klassifikationsgrad sowie die rasche Verfügbarkeit von Expertisen, die im politischen Gebrauch als „unproblematisch“ eingestuft werden. Vorreiter des OSINT-Ansatzes ist Robert D. Steele, der zu diesem Bereich zahlreiche Publikationen wie Bücher und Konzepte verfasste.[34] Heute ist OSINT in jedem modernen Nachrichtendienst ein fester Bestandteil in der Beschaffung und Analyse von politik- und sicherheitsrelevanten Entwicklungen. Der OSINT-Ansatz projiziert eine grundsätzliche Erkenntnis über den eigentlichen Träger von Information und Wissen. Als eigentlicher Träger werden nicht staatliche Institutionen genannt, sondern in erster Linie der Mensch, der als Informant, Analyst und Experte auftritt. Nur er hat das Wissen und die Fähigkeit zur Bildung sozialer Netzwerke, die für die nachrichtendienstliche Beschaffung und Analyse von essentieller Bedeutung sind.

[33] Vgl. den Abschnitt OSINT in der vorliegenden Studie.

[34] Vgl. hierzu folgende Publikationen von Steele, Robert D.: The New Craft of Intelligence. Washington D.C. 2001; Ders.: On Intelligence – Spies and Secrecy in an Open World. Fairfax 2000 und Ders.: Relevant Information – A New Approach to Collection, Sharing and Analysis. Washington D.C. 1999.

Transformation

Der dieser Arbeit zugrunde gelegte Transformationsbegriff bezeichnet einen kontinuierlichen Prozess der Adaption nachrichtendienstlicher Strukturen. Das gilt insbesondere in Hinblick auf die aktuellen transnationalen Bedrohungsbilder, wie z. B. Terrorismus, Massenvernichtungswaffen, regionale Konflikte, Scheitern von Staaten und organisierte Kriminalität.[35] Aber auch soziale und gesellschaftspolitische Veränderungen (z. B. sinkender Lebensstandard, hohe Arbeitslosigkeit, Migration u. ä.) können als zukünftige Risiken eingestuft werden. Der hier angesprochene Prozess struktureller Weiterentwicklung im Intelligencebereich bezeichnet einen Transformationsprozess als Kontinuum. Damit ist ein fortdauernder Adaptionsverlauf gemeint. Dieser fortdauernde Anpassungsprozess tangiert nicht nur die Policy-Ebene von Intelligence, sondern auch ihre institutionellen Grundlagen und ihre analytische Komponente. Der wissenschaftliche Intelligencediskurs hat gezeigt, dass bestehende nachrichtendienstliche Strukturen moderner Demokratien seit dem Zweiten Weltkrieg auf unterschiedlichste Bedrohungsbilder durchwegs akkurat reagiert haben. Dennoch bleibt viel Raum für Verbesserungen und Restrukturierungsmaßnahmen, wie zahlreiche intelligencebezogene Fehlleistungen verdeutlichen (z. B. Pearl Harbor 1941, Kubakrise 1962, Iran-Contra-Affäre 1986, das Nichtvorhersehen des Zusammenbruches der UdSSR 1989/90, die Terroranschläge vom 11. September 2001 und der Skandal um die irakischen Massenvernichtungswaffen). Während diese intelligencerelevanten Fehlleistungen teilweise mit größeren Umstrukturierungen im personellen und rechtlichen Bereich einhergingen, wurde die Verantwortung der Politik als Fehlerquelle kaum thematisiert. Allerdings gibt es neben den konservativ-bürokratischen Restrukturie-

[35] Hauptbedrohungen gem. der Europäischen Sicherheitsstrategie (ESS). Im Jahr 2009 konnten in alleine in sechs EU-Mitgliedsstaaten 294 terroristische Aktionen verhindert werden. Dabei handelte es sich allerdings nicht nur um islamistische Terrorpläne, sondern auch um andere gewaltbereite Gruppierungen. In Bezug auf den islamistischen Terrorismus wurden im selben Jahr allerdings 110 Personen inhaftiert (ohne Großbritannien). Vgl. Roell, Peter, Worcester, Maxim: Low Intensity Terrorist Threats – A Future Trend in Europe? Institut für Strategie-, Politik-, Sicherheits- und Wirtschaftsberatung, Berlin 2010.

rungsofferten eben noch die progressivere Alternative der Transformation, um die aktuellen und zukünftigen Herausforderungen meistern zu können. Immerhin ergeben sich durch neue Technologien, kreative und innovative Beschaffungs- und Analyseansätze zusätzliche Möglichkeiten für eine „proaktive" Leistungsadaption nachrichtendienstlicher Strukturen (z. B. Fähigkeiten, Bedrohungen besser antizipieren zu können). Obwohl es diese Ansätze der Transformation gibt, darf die Rolle der Politik nicht unbeachtet bleiben, weil sie die Zielsetzungen und Beratungskultur der Nachrichtendienste bereits mehrmals instrumentalisierte. Transformation bedeutet aber auch, intelligente Lösungsansätze für spezielle Herausforderungen zu finden und umsetzen zu können. Damit bedeutet Transformation nach Jennifer E. Sims die Fähigkeit, Bedrohungen besser bekämpfen zu können, ohne grundrechtsrelevante Errungenschaften einschränken zu müssen.[36] Das „Markenzeichen" der Transformation nachrichtendienstlicher Strukturen ist allerdings die Vereinigung ausgewählter Technologien mit innovativen Strategien, um „revolutionäre Lösungsansätze und Fähigkeiten" herauszubilden. Sims fordert also eine innovative, kreative und unkonventionelle Anwendung von „Cutting-Edge-Technologien", bestehenden Intelligencefähigkeiten im Bereich der Analyse und kognitive Flexibilität zur Vermeidung von Fehleinschätzungen.[37] Im Grunde forcieren Vertreter einer progressiven Intelligenceauslegung einen Wettstreit der Ideen für mehr Sicherheit durch Intelligence.

Bedarfsfestellung

Die sicherheitspolitischen Entwicklungen seit dem Ende des Kalten Krieges führten in der ersten Sektion der strukturierten Ansatzdefinition zu weitreichenden Transformationserfordernissen im Bereich der Bedarfsfeststellung bzw. der Formulierung notwendiger Aufklärungsbereiche. Diese Bedarfsfeststellung erfolgt in der Regel durch Politiker (u. a. Entscheidungseliten im staatlichen System). Politiker als primäre Be-

[36] Vgl. Sims, Jennifer E.: Introduction. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. X.
[37] Vgl. a.a.O.

darfsträger von Intelligence sind im öffentlich-politischen Argumentationsraum verortet, wodurch die Klassifikationsthematik in Bezug auf fertige Intelligenceprodukte in der öffentlichen Debatte tangiert wird. Bei der Bedarfsfeststellung sind neben den langfristigen intelligencerelevanten Planungsinhalten auch tagespolitische Themen zu berücksichtigen, die sich rasch ändern können. Diesen tagespolitischen Bedarf nachrichtendienstlich zu würdigen, erfordert „politische Praxis". Nur in wenigen Fällen ist eine kurzfristige Bedarfsänderung tatsächlich erfolgreich umzusetzen. Kontingente Fähigkeiten werden über das Intelligencemanagement im Aufklärungsplan einer Intelligenceorganisation erfasst, strukturiert und umgesetzt. Für wirklich dringende tagespolitische Anfragen werden Notfallkapazitäten aktiviert, um eben diesen zusätzlichen Bedarf abdecken zu können. Nicht selten haben Politiker überzogene Erwartungshaltungen gegenüber den nationalen Intelligenceorganisationen in Bezug auf ihre tatsächlichen Fähigkeiten. Dadurch erhöht sich für die Intelligenceorganisation allerdings der politische Druck in Bezug auf eine erfolgreiche Umsetzung nachrichtendienstlicher Aufklärungsprioritäten. Intensive gegenseitige Konsultationen sowie der direkte Kontakt unterstützen die Bearbeitung kurzfristiger Anfragen sowie die Umsetzung des Aufklärungsplanes.

Die Bedarfsfeststellung bezeichnet also den Startpunkt im nachrichtendienstlichen Produktionszyklus. Politiker und andere Entscheidungsträger formulieren auf der Grundlage aktueller politischer Herausforderungen (Tagespolitik, Krisenmanagement, Friedensmissionen, diplomatische Verhandlungen, diverse Bedrohungen, etc.) spezielle Fragestellungen, die mit Hilfe nachrichtendienstlicher Methoden[38] beantwortet werden. Für den Experten Treverton reflektiert die Bedarfsfeststellung einen rückbezüglichen Prozess der Wissensgenerierung.[39] Zum einen muss der aktuelle und kurzfristige Informationsbedarf der Politik abgedeckt werden und zum anderen verlangt diese Dienstleistung eine perspektivisti-

[38] Darunter versteht man die Beschaffungsmethoden sowie Analyseansätze im Intelligencewesen. Die Abschnitte „Beschaffung" und „Analyse" beschreiben den Begriff der „nachrichtendienstlichen Methoden" näher.

[39] Vgl. hierzu Treverton, Gregory: Reshaping National Intelligence For An Age Of Information. Rand/University of Cambridge, Cambridge 2001, S. 177-215.

sche Intelligence-Policy; d. h. Intelligenceorganisationen müssen eine vorausschauende Beschaffungsstrategie verfolgen. Die kurzfristigen Bedarfseingaben der Politik in Bezug auf einen aktuellen Informationsbedarf sind in der Regel als Vorlaufzeit zur Intelligencegenerierung nicht ausreichend. Damit hat die Bedarfsfeststellung einen kritischen Stellenwert im gesamten nachrichtendienstlichen Produktionszyklus (Intelligence Cycle), der eine enge Interessens- und Policy-Abstimmung zwischen der Politikebene und der nachrichtendienstlichen Managementsektion einfordert.[40] Als Ergebnis dieses Abstimmungsprozesses sind, unter Berücksichtigung einer perspektivistischen Intelligence-Policy, eine entsprechende Quellenlage sowie eine möglichst aktuelle Prioritätenreihung des Aufklärungsplanes durch den Nachrichtendienst vorzusehen.

Beschaffung

Nachrichtendienstliche Beschaffung bedeutet, vorhandene Fähigkeiten zu nutzen und neue Möglichkeiten zu erschließen, die dem jeweiligen Bedrohungsschema entsprechen.[41] Die Anwendung nachrichtendienstlicher Beschaffungsansätze setzt ein Intelligencemanagement voraus, welchem die eigenen sowie fremden Möglichkeiten der Aufklärung bekannt sind. Nur so kann ein Maximum an intelligencerelevanten Erkenntnissen gewonnen werden. Das traditionelle techniklastige Beschaffungswesen während des Kalten Krieges wurde im Zuge der Bemühungen zur Bekämpfung des internationalen Terrorismus relativiert; d. h., spätestens seit dem 11. September 2001 gibt es eine Neugewichtung in Richtung „human intelligence“ (HUMINT)[42] – ein bedeutender komplementärer Beschaffungsansatz, der bis dahin vernachlässigt wurde. Die Beschaffung mittels „technical intelligence“ (TECHINT) vermag

[40] Vgl. hierzu a.a.O.

[41] Auf der Grundlage vorhandener Fähigkeiten bedeutet, dass das Beschaffungsspektrum zwar erweitert werden soll; eine Neuerfindung der Beschaffung ist im Hinblick auf das Transformationsthema aber nicht erforderlich.

[42] Vgl. hierzu Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 28 und 114f und Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington D.C. 2005.

ein großes Spektrum an gegnerischen Aktivitäten aufzuklären; allerdings erreicht TECHINT in Bezug auf „gruppeninterne“ Abläufe und Ziele seine Leistungsgrenzen. Die Kombination und flexible Anwendung existierender Beschaffungsmöglichkeiten erzielt die wohl besten Aufklärungsresultate. Zusätzliche technische Innovationen der vergangenen Jahre haben den Stellenwert der technischen Aufklärungssysteme in Bezug auf spezielle Aufgabenstellungen (z. B. Grenzraumüberwachung, Überwachung des Internets, operative und taktische Aufklärung, Überwachung globaler Kommunikationsabläufe, etc.) gestärkt.[43] Diese technischen Unterstützungssysteme zur Beschaffung und Aufklärung werden verstärkt mit Daten und Informationen aus dem HUMINT-Sektor kollationiert, um eine akkuratere Einschätzung gewonnener Informationen machen zu können. Im Vergleich zum TECHINT- stellt der HUMINT-Bereich ein individuelles und politisches Risiko dar, welches nur bedingt eingegrenzt werden kann. Aus der Sicht der Gegenaufklärung ist der HUMINT-Bereich eine potentielle Schwachstelle im Wettstreit nachrichtendienstlicher Sicherheitssysteme,[44] da es einen absoluten Schutz gegen feindliche Infiltration nicht gibt. Aber die Verlässlichkeit gewonnener Informationen unter Anwendung strenger Verhörmethoden bzw. Folter ist fraglich und aus staatstheoretischer sowie menschenrechtlicher Sicht zu verurteilen. Grundrechte und institutionelle Errungenschaften demokratischer Gesellschaften dürfen der Terrorismusbekämpfung nicht zum Opfer fallen. Die Ausheblung grundrechtsrelevanter Elemente würde einen ungeheuren politischen und gesellschaftlichen Rückschritt bedeuten.

Im Bereich der Beschaffung sind die jeweiligen gesetzlichen Mandate nationaler Dienste sowie verfassungsrechtliche Rahmenbedingungen in

---

[43] Vgl. hierzu Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 124f.

[44] Der Wettstreit nachrichtendienstlicher Sicherheitssysteme umfasst in erster Linie das Counterintelligence. Nachrichtendienste versuchen mit Hilfe des CI-Bereiches, die Eigensicherheit zu gewährleisten bzw. zu erhöhen. Der Schutz vor Spionage (Infiltration des eigenen Dienstes) bzw. bestimmter staatlicher Einrichtungen steht im Vordergrund der nachrichtendienstlichen Abwehranstrengungen. Vgl. hierzu Herman, Michael: Intelligence Power in Peace and War. Cambridge 1996.

Bezug auf deren Möglichkeiten aussagekräftig. In Verbindung mit den erwähnten Neugewichtungen im Bereich TECHINT und HUMINT ist auch die sogenannte „open source revolution“ von Robert Steele zu einer maßgeblichen Größe im nachrichtendienstlichen Beschaffungswesen geworden.[45] Der Stellenwert von Open Source Intelligence (OSINT) für die Produktion von akkuratem Intelligence nimmt heute den Hauptteil in der strategischen Analyse ein.

Analyse

Man kann nach Fred Schreier[46] Intelligence als die Summe von Information und Analyse beschreiben, wodurch im Zeitalter der Expertisen, Vernetzung und transnationalen Netzwerke die nachrichtendienstliche Analyse zentrales Element im modernen Intelligencewesen ist. Der Stellenwert bemisst sich nach den fachlichen Fähigkeiten und dem Spezialwissen von Analysten, die in der Fachliteratur als die Träger von Wissen bezeichnet werden. In Verbindung mit einer praktikablen Ethik der Professionalität tragen Intelligencanalysten unmittelbare politische Verantwortung durch die Vermittlung von Erkenntnissen. Diese sicherheitspolitisch kritischen Erkenntnisse kommen in internationalen Kooperationen zum Tragen. Dem Analysten könnten hier zusätzliche Freiheiten[47] gewährt werden, um die Zusammenarbeit der Dienste zu stärken. In diesem Zusammenhang plädiert Fred Schreier sogar für den Aufbau von soge-

[45] Vgl. Steele, Robert D.: On Intelligence – Spies and Secrecy in an Open World. Fairfax 2000.

[46] Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 21. Vgl. auch Schreier, Fred: Fighting Pre-Eminent Threats with Intelligence-led Operations. Reihe: Occasional Paper. Nr. 16. DCAF, Genf 2009, S. 51f.

[47] Als „zusätzliche Freiheiten“ können erweiterte Möglichkeiten des Analysten genannt werden, die traditionell-universitär ausgeprägt sein können. Allerdings setzt dieser Ansatz der zusätzlichen Freiheiten die Rekrutierung von interdisziplinär gebildeten Human- und Sozialwissenschaftern voraus, die nicht nur die Analyse, sondern auch das „Handwerk“ der Wissenschaft umfassend beherrschen. Sie können sich auch in unterschiedlichen sozialen Systemen bewegen.

nannten „regionalen Analyseeinheiten“ („region-wide units“),[48] die einen „holistischen“ Ansatz verfolgen könnten. Regionale Analyseeinheiten könnten mit der Unterstützung von „physischen“ und „virtuellen“ Einheiten[49] besser arbeiten, d. h. forschen, Intelligence produzieren, Langzeitanalysen erstellen, nachrichtendienstliche Anforderungen identifizieren und Beschaffungsprioritäten erstellen (Unterstützung für das Intelligencemanagement).[50] Wesentlich für die Verbesserung nachrichtendienstlicher Analysen sind formelle und informelle Übereinkommen mit den unterschiedlichsten Experten, zu internationalen Kontakten, zum privaten Sektor, Kontakte zu Universitäten und sonstigen staatlichen Forschungseinrichtungen. Diese Verortung von Wissen bezeichnet Schreier als „seats of knowledge“.[51] Die Aktivitäten regionaler Analyseeinheiten könnten im Idealfall mit eigenen Ressourcen (eigene Finanzmittel, schlanke Verwaltungsstruktur, administrative und technische Unterstützungselemente, etc.) zur Unterstützung ihrer Arbeit ausgestattet werden (z. B. Organisation von Konferenzen, Arbeitssitzungen, etc.).[52] Mit Hilfe dieser Innovationen könnten die Nachrichtendienste Analysen rascher produzieren. Damit würden die Analysen zu „Echtzeiteinschätzungen“ gelangen, die für den politischen Entscheidungsfindungsprozess maßgeblich sind.[53] Der „konkurrierende“ Charakter zeitlicher Aktualität steht im Widerspruch zur Evaluationsfähigkeit (Qualitätskontrolle) von Analysen sowie zur politischen Verantwortlichkeit regionaler Analyseeinheiten.[54] Diese Vorschläge für eine Transformation der Analyse dürfen in der Fachdiskussion von möglichen Ableitungen methodische, wissenschaftliche und soziologische Distinktionen zwischen dem sicher-

[48] Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 146ff.
[49] Vgl. a.a.O.
[50] Vgl. a.a.O.
[51] Vgl. a.a.O.
[52] Vgl. a.a.O. Diese Forderungen decken sich mit jenen von Robert Steele, der bereits Ende der 1990er-Jahre ähnliche Intelligencekonzepte von der US-Administration einforderte.
[53] Vgl. hierzu die Publikationen der beiden Experten.
[54] Vgl. Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 146ff.

heitspolitischen/nachrichtendienstlichen Analysten[55] und dem universitär verorteten Wissenschafter nicht geringschätzen.[56] Der sicherheitspolitische/nachrichtendienstliche Analyst kann daher als spezielle „Vermittlungsinstanz“ zur Überbrückung der Kluft zwischen „Spezialist“ und „Generalist“ (z. B. Politiker) angesehen werden.[57] Politiker oder andere hohe Entscheidungsträger wollen in Kürze und strukturiert unterrichtet werden. Eine ausführliche (wissenschaftliche) Problemdarstellung ist aus zeitlichen Gründen kaum oder nur selten möglich.[58] Die „politische Briefingfähigkeit“ wird als fachliche Qualifikation der staatlichen Analysten angesehen. Vor diesem Hintergrund argumentieren Experten für eine auf den Analysten fokussierte Analysetätigkeit als Grundvoraussetzung struktureller Adaptionen im Rahmen der Transformationserfordernisse, die sich aus den recht komplexen sicherheitspolitischen Herausforderungen und Bedrohungen ergeben. Der Analyst als „essentielle Komponente“ liefert also jenen Input in die strukturellen Intelligencedimensionen „Organisation“, „Prozess“, „Methode“ und „Wissen“, der den Adaptionserfordernissen entsprechen sollte.[59] Dies ist nicht nur für die Gesamtstruktur Intelligence wichtig, sondern auch für den Analysten selbst, der durch erhöhte Handlungsfreiheit und thematische Selbstver-

[55] Hier kommt die Sozialisation „staatlicher Analysten“ im Vergleich zu den Akademikern der offenen Wissenschaften zum Tragen. Das Sozialisationsthema argumentiert in Bezug auf die Vorteile der freien Wissenschaftstradition im Sinne der Fähigkeit zur selbstkritischen Reflektion, die sich in konservativ-strukturellen Staatsinstitutionen in einer veränderten Form wiederfindet.

[56] Vgl. Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 146ff.

[57] Diese Auffassung wird in zahlreichen Büchern prolongiert. Schreier reflektiert hier in seinem Argumentationsrahmen eine bereits anerkannte Position in Bezug auf die Bedeutung von (nachrichtendienstlichen) Analysten.

[58] Schreier spricht in diesem Zusammenhang von einer Seite und von drei bis vier Minuten als Umfang eines Briefings für high-level-Entscheidungsträger. Daher wird als oberste Priorität für Briefings die genaue Kenntnis über die Bedürfnisse des Bedarfsträgers angesehen. Vgl. Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 146ff.

[59] Vgl. Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 146ff.

antwortung die dynamische Bedrohungsentwicklung im internationalen Umfeld besser zu verstehen lernt. Dadurch könnten nachrichtendienstliche Erkenntnisse rascher in Analysen aufbereitet werden. Auch der Wert von Intelligence in der Politikberatung könnte sich dadurch erhöhen.

Die an dieser Stelle erörterten Vorschläge für eine strukturelle Adaption der Dienste werden im Konkurrenzverhalten des Feindes begründet. Der Feind – in diesem Falle radikale Islamisten und Terroristen – kann bereits mit vergleichsweise „rudimentären" Möglichkeiten durchaus effektive Gegenstrategien entwickeln und anwenden.[60] Vielfach geht es nicht um banale Rechtfertigungsansagen für Terroroperationen, sondern in erster Linie dient der „analytische" Ansatz des Feindes für eine bessere Einschätzung der Möglichkeiten und Fähigkeiten staatlicher Intelligenceorganisationen.[61] Er analysiert Schwachstellen im staatlichen System, in Gesellschaft und Politik. Die Erkenntnisse werden für gezielte Maßnahmen gegen die „westliche" Weltanschauung genützt. Diese Maßnahmen liegen in den Bereichen der Propaganda, Zielauswahl, Verwundbarkeit westlicher Interessen, ideologische Indoktrinierung und Radikalisierung nach regionalen Gesichtspunkten. Vor diesem Hintergrund wird die Bedeutung nachrichtendienstlicher Transformationsbestrebungen besonders im Analysebereich deutlich. Denn nur der Spezialist und Experte kann unter Rückgriff auf staatliche Ressourcen entlang des Sicherheitsauftrages feindliche asymmetrische Angriffe prognostizieren, abschwächen oder sogar zur Gänze abwehren. Dies bedingt allerdings seine Verfügbarkeit und institutionelle Verankerung im Voraus. Beide Voraussetzungen könnten durch die Zuteilung von materiellen Ressourcen die Flexibilität des gesamten Analysebereiches fördern (z. B. im Bereich der internationalen Kooperationen/Informationsaustausch).

[60] Als Gegenstrategien gelten gezielte Desinformationskampagnen, ideologische Indoktrinierung sowie die psychologische „Kriegsführung" in besonders instabilen Regionen. Radikale Islamisten nutzen das Internet zur Kommunikation und Verbreitung von Propaganda (z. B. Videobotschaften).

[61] Terrororganisationen haben in der Vergangenheit bewiesen, dass sie in bestimmten Bereichen mit Hilfe einer gezielten und strukturierten Beschaffung und Analyse gelernt haben, die Möglichkeiten von Nachrichtendiensten zu verstehen.

Der Intelligenceexperte Fred Schreier vom Genfer DCAF schlägt für eine Verbesserung der Beschaffung und Analyse im Bereich der Terrorismusbekämpfung die Berücksichtigung folgender Indikatoren vor:[62]

- ⇨ Identifikation soziogenetischer Bedingungen;
- ⇨ Bestimmung und Eingrenzung radikaler Subkulturen;
- ⇨ Beobachtung subversiver Agitation, revolutionärer oder extremistischer Publikationen und Propaganda, anti-instutionelle Demonstrationen und Aktivitäten;
- ⇨ Analyse terroristischer Stellungnahmen, ideologische Rechtfertigungen, Verantwortlichkeiten sowie mittelfristige Zielsetzungen;
- ⇨ Systematische Erfassung terroristischer Aktivitäten zur Erfassung des modus operandi sowie Verhaltensanalyse;
- ⇨ Beschaffung über technologische Neuerung innerhalb dschihadistischer Gruppierungen;
- ⇨ Analyse der Struktur von Terrororganisationen zur Bestimmung ihrer Fähigkeiten;
- ⇨ Identifizierung von Unterstützern, Bewegungen und Netzwerken;
- ⇨ Verifikation internationaler Verbindungen zur diversen Gruppierungen und etwaigen staatlichen Förderern;
- ⇨ Exploitation terroristischer Strukturen in Bezug auf Schwachstellen;
- ⇨ Bestimmung von Kooperationsmöglichkeiten mit befreundeten Staaten zur Terrorismusbekämpfung.

Die Transformation nachrichtendienstlicher Strukturen unterliegt zahlreichen politischen, funktionellen und institutionellen Schranken, die die strukturelle Adaption im Hinblick auf die aktuellen Erfordernisse erschwert. Zur Überbrückung von temporären Hindernissen für eine rasche Verbesserung nachrichtendienstlicher Analysekapazitäten im Kampf gegen radikal-islamistische Kräfte wurde auch der Rückgriff auf private Firmen (insbesondere Intelligencefirmen) in Erwägung gezogen. Ob die private Option in diesem sensiblen Bereich tatsächlich von Nutzen ist, kann derzeit noch nicht beurteilt werden.

---

[62] Adaptierte Indikatorenaufzählung nach Schreier, Fred: Transforming Intelligence Services – Making Them Smarter, More Agile, More Effective and More Efficient. In: Study Group Information. Wien 2010, S. 160f.

Um den Kampf gegen den internationalen Terrorismus zu gewinnen, verlangen Experten eine fortschrittliche Informationsarchitektur für einen verbesserten Informations- und Wissenstransfer. Eine moderne Informationsarchitektur stärkt das gesamte Spektrum nachrichtendienstlicher Analyse, weil eine Zusammenschau von potentiell relevanten Einzelereignissen möglich wird („connect the dots“).[63] Die Umsetzung dieser Forderung obliegt jedoch der Managementebene in den Diensten, die nach US-Auffassung folgende Aspekte eines erfolgreichen Intelligencemanagements berücksichtigen sollte:

- Einführung des Klassifikationsprinzips „need to share” anstelle von „need to know”;
- Implementierung innovativer IT-Strukturen zur Gewährleistung des neuen Klassifikationsprinzips;
- Schutz dieser nachrichtendienstlich relevanten IT-Struktur gegen internen und externen Missbrauch;
- Begründung einer neuen proaktiven Beschaffungskultur, einer integrierten Analyse sowie einer umfassenderen Dissemination von Produkten;[64]
- Kollationierung und Ergänzung datenrelevanter Begleitaspekte der Beschaffung[65] und ihre Vermittlung an die Analyseebene (engere Zusammenarbeit zwischen Beschaffung und Analyse);
- verstärkte Erschließung von so genannten „high value targets“;
- Verbesserung des allgemeinen Informationsmanagements.

[63] Vgl. Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington D.C. 2005, S. 109.

[64] Modifizierter Aspekt im Lichte neuerer wissenschaftlicher Erkenntnisse aus dem Bereich der Intelligence Studies. Die „integrierte Analyse“ favorisiert „need to know“, den OSINT sowie eine generative Wissensbasis durch den Analyseträger (Kontakte zu externen Institutionen, Think Tanks, Experten, etc.). Vgl. auch Schreier, Fred: Fighting Pre-Eminent Threats with Intelligence-led Operations. Reihe: Occasional Paper. Nr. 16. DCAF, Genf 2009, S. 52.

[65] Als relevante Begleitaspekte können Umfeldeindrücke und persönliche Einschätzungen der Beschaffung angesehen werden, die eine genaue Analyse bzw. Einschätzung/ Beurteilung einer Information deutlich erleichtern.

Technologische Implikationen

Ein wesentlicher Bestandteil nachrichtendienstlicher Transformationsbestrebungen betrifft die technologischen Aspekte der Aufklärung.[66] Jeder fortschrittliche Nachrichtendienst versucht, sich den Zugang zur modernen Informationstechnologie zu sichern, um bestimmte Bedrohungen präventiv aufklären zu können. Modernste Technologien – damit sind die gesamten Systemvoraussetzungen für eine vollständige Partizipation in der Informations- und Kommunikationsumwelt genauso angesprochen wie speziellere Hardware für TECHINT-basierte Aufklärung mittels Trägersystemen (z. B. IMINT, RADINT, MASINT etc.)[67] – haben den nachrichtendienstlichen Ablaufprozess von der Policy-Ebene über die Management-Ebene bis hin zur operativen Umsetzung erteilter Aufträge nachhaltig verändert. Eine der wohl markantesten Innovationen nachrichtendienstlicher Beschaffung ist die Inklusion des OSINT-Ansatzes[68] zur Unterstützung für die Erstellung von Analysen. Der große Vorteil des OSINT-Ansatzes liegt darin, dass er bürokratischen Institutionen mit relativen rigiden (Denk-)Strukturen zu neuen externen Sichtweisen verhilft. So müssen moderne Nachrichtendienste eine gewisse Flexibilität, Innovationsfreudigkeit sowie „Kreativität“ zur Bekämpfung aktueller Bedrohungen entwickeln. Teilweise unterstützen moderne Technologien im Kommunikationsbereich die Öffnung der Dienste in Bezug auf eingefahrene Sichtweisen. Damit können technologische Neuerungen methodische Innovationen hervorbringen und nachrichtendienstlichen Fehleinschätzungen vorbeugen. Wie bereits erwähnt, stellt der Ansatz der offenen Beschaffung eine besondere Bereicherung für die Dienste dar, wie im folgenden Abschnitt näher ausgeführt werden soll.

---

[66] Technische Weiterentwicklungen im Bereich der Aufklärung haben in manchen Ländern spezialisierte Aufklärungsdienste entstehen lassen, wie beispielsweise die US-amerikanische NSA oder NRO. Aber auch in Australien (DSD und DIGO), Russland (FAPSI) und Großbritannien (GCHQ) wurden ähnliche Dienste gegründet. Vgl. Schreier, Fred: Fighting Pre-Eminent Threats with Intelligence-led Operations. In: Occasional Paper. Nr. 16. DCAF, Genf 2009, S. 53.

[67] Vgl. Schreier, Fred: Fighting Pre-Eminent Threats with Intelligence-led Operations. In: Occasional Paper. Nr. 16. DCAF, Genf 2009, S. 50.

[68] Vgl. ebd., S. 49.

OSINT

Nach dem Fall des Eisernen Vorhanges kam es nicht nur zu einer strukturellen Neuausrichtung (in thematischer und institutioneller Hinsicht),[69] sondern auch zu methodischen Innovationen in den Nachrichtendiensten.[70] Eine dieser Innovationen kam mit den neuen Informations- und Kommunikationstechnologien zur Anwendung. Dabei handelt es sich um die verstärkte Nutzung offener Informationsquellen (Open Source Intelligence, OSINT). OSINT kann im Sinne von Robert D. Steele, Gregory Treverton, Amy Sands u. a. nicht nur als offenes Informationsmaterial angesehen werden, sondern ist durch die thematische Weiterverarbeitung auch „Expertise“ und (schriftliche) Analyse. Diese Veränderung wurde notwendig, weil die traditionelle Spionage mittels Agenten oder TECHINT der interdependenten Weltordnung im Zeitalter der Globalisierung nicht mehr entsprach. Es dauert jedoch rund zehn Jahre, bis die verantwortlichen Entscheidungsträge großer Dienste die geänderten informationellen Umfeldbedingungen erkannten. Klassifizierte Informationen – die man vormals nur durch einen exklusiven Zugang erhielt – reichten zur Abdeckung transnationaler Bedrohungen (Terrorgruppierungen, OK-Netzwerke, illegaler Waffenhandel, privatisierte Gewaltakteure, etc.) nicht mehr aus.[71] Für Amy Sands gibt es drei wesentliche Gründe, die für die grundlegende Veränderung des informationellen Umfeldes ausschlaggebend waren bzw. sind: Erstens gibt es im Zeitalter der Globalisierung eine Vielzahl an relevanten Akteuren (Staaten, nichtstaatliche Akteure, Gruppierungen, etc.) und Aufklärungserfordernisse. Zweitens kam es in der Vergangenheit zu einer (illegalen) Verbreitung von gefährlichen Technologien („destructive technologies“), die sich im Begriff der Dual-Use-Güter wiederfindet. Drittens wurde durch die modernen Technologien die Verletzbarkeit der Gesellschaften erhöht, d. h.

[69] Beispielsweise in thematischer Hinsicht: Verstärkung der Wirtschaftspionage, Querschnittsthematik Terrorismus und organisierte Kriminalität; in institutioneller Hinsicht: Ausbau eines weltumspannenden Abhörsystems (Echelon), Gründung neuer Einrichtungen für eine gezielte Aufklärung neuer Bedrohungen.

[70] Vgl. Sands, Amy: Integrating Open Source into Transnational Threat Assessments. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. 63f.

[71] Vgl. ebd., S. 63-78.

sie sind leichter angreifbar als noch zu den Zeiten der bipolaren Konfrontation zwischen Ost und West.[72] Vor diesem Hintergrund sprechen sich Experten für „open-source" Informationen aus. Sie ermöglichen die Produktion von „high-quality intelligence assessments".[73] Während des Kalten Krieges wurden strategische Analysen, Bedrohungseinschätzungen etc. auf der Grundlage klassifizierter Informationen erstellt. Heute basieren Intelligenceanalysen zu rund 90 Prozent auf OSINT.[74] Im Zusammenhang mit den veränderten sicherheitspolitischen Rahmenbedingungen streicht diese Schätzung von Experten den Stellenwert von OSINT für die modernen Dienste hervor. Die größte Herausforderung im OSINT-Bereich ist die Qualitätssicherung verfügbarer Informationen. Oftmals müssen offene Informationen erst verifiziert werden, um überhaupt als Analysegrundlage verwendet werden zu können. Damit folgt auch der OSINT-Bereich einem nachrichtendienstlichen Produktionszyklus, der mit dem theoretischen Modell des Intelligence Cycle vergleichbar ist. Trotz der allgemeinen Vorteile von Informationen geringer Klassifikationsstufen kann OSINT nur jene Bereiche abdecken, die mit einer „offenen Gesellschaft" verbunden sind. „Geschlossene Gesellschaften" – die sich also gegen die modernen Errungenschaften aus Gründen der nationalen Sicherheit verwehren – sind nur sehr bedingt oder überhaupt nicht mittels OSINT aufzuklären. In diesen Fällen greifen die Dienste auf traditionelle Methoden der Aufklärung zurück. In der Fachwelt spricht man hier von sogenannten „denied areas", bei denen man mit technologischen Entwicklungsprogrammen versucht, sie in das Zeitalter der Information zu führen. So erdachte der US-Experte Steele die Möglichkeit, einen Marshall-Plan für den IKT-Bereich in der Dritten Welt ins Leben zu rufen. Davon würden nicht nur die Gesellschaften profitieren, sondern eben auch die Intelligencearbeit im Bereich der Krisenfrüherkennung (konfligierende Interessen rechtzeitig erkennen). OSINT erfüllt aber auch eine kritische Selektionsaufgabe für politische

[72] Vgl. hierzu Sands, Amy: Integrating Open Source into Transnational Threat Assessments. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. 63.
[73] Vgl. Sands, Amy: Integrating Open Source into Transnational Threat Assessments. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. 63.
[74] Einschätzung von Robert Steele im Rahmen eines Vortrages in Graz 2004.

Entscheidungsträger im Hinblick auf Bedrohungsanalysen und verfügbaren sicherheitspolitischen Informationen. Hier verbindet sich der geringe Klassifikationsstatus von OSINT mit dem Loyalitätsprinzip staatlicher Institutionen in Bezug auf die nationalen eigenstaatlichen Interessen. In diesem Falle stellen die Dienste unter Rückgriff auf ihre fachlichen Kompetenzen die Qualität von OSINT sicher (Qualitätskontrolle und Ergänzung). Aufgrund von OSINT veränderte sich auch der nachrichtendienstliche Produktionsverlauf für Intelligenceprodukte. Heute gleicht der nachrichtendienstliche Ablaufprozess eher einer interaktiven und reziproken Kommunikation (traditioneller versus realer Intelligence Cycle).[75]

Politik und Intelligence

Ein wesentlicher Aspekt in der aktuellen Transformationsdebatte nachrichtendienstlicher Strukturen demokratischer Staaten betrifft die Interaktionsebene zwischen Intelligence und Politik. Dabei handelt es sich idealerweise um einen strukturierten Dialog zwischen beiden Ebenen. In der Realität gestaltet sich das Zusammenwirken beider sozialer Ebenen als problematisch und zwar aus verschiedenen Gründen. Zum einen muss auf die unterschiedlichen sozialen Komponenten beider Ebenen hingewiesen werden. Während im Intelligencebereich eine Loyalitäts- und Vertrauenskultur vorherrscht, muss die Politikebene zusätzlich auf soziale Interaktionsebenen und politische Entscheidungen und Programme Rücksicht nehmen. Damit kommen parteipolitische Präferenzen, medienwirksame Inhalte, demokratiepolitische Grundsätze, parlamentarische Kontrollinstanzen und Beschlüsse zum Tragen, die ein Entscheidungsumfeld im Sinne von Machiavelli entstehen lassen. Politische Entscheidungen werden demnach nicht nur nach „rationalen“ Grundlagen im Sinne objektiviertem Wissen getroffen, sondern durchwegs nach „praktischen“ Erwägungen, die sich allerdings längerfristig nicht immer als die beste Lösung eines (sicherheits)politischen Problems darstellen

[75] Vgl. hierzu Braumandl, Wolfgang, Desbalmes, Christian: Nachrichtendienstliche Kooperation der EU im Kampf gegen den Terrorismus – Eine Bestandsaufnahme 2006. Schriftenreihe der Landesverteidigungsakademie Wien, 2007, S. 20.

müssen. Zum anderen sollten auch die Arbeitsvoraussetzungen beider Interaktionsebenen nicht unbeachtet bleiben. Die Politik kann und muss unter demokratischen Bedingungen ihre Entscheidungen durch öffentliche Diskussionen legitimieren. Die Legitimation durch öffentliche Diskussion ist in vielen Fällen ein sehr aufwendiger politischer Steuerungsprozess, der die Mitwirkung der Medien erfordert, um dem Anspruch der positiven Koordinierung gesellschaftspolitischer Partikularinteressen gerecht zu werden. Allerdings ist auch dieser sehr aufwendige demokratiepolitische Legitimierungsprozess (als wesentliche Komponente positiver Koordinierung) zunehmend der Gefahr ausgesetzt, kurzfristige und oberflächliche Interessen zu forcieren, die sich längerfristig als „Irrtum" erweisen können. In diesem Zusammenhang könne man auch von einer „Mediokratie" sprechen, also von einer Demokratieform, die in der Mittelmäßigkeit qualitativen Arbeitens verweilt. Die Politik der demokratischen Mittelmäßigkeit reflektiert allerdings realpolitische Verhältnisse, die sich den Wahlperioden anpassen. Politiker haben in modernen Demokratien nur ein sehr kleines Zeitfenster, in denen sie tatsächlich substantielle Arbeit leisten können. Je näher eine Wahl kommt, umso öffentlichkeitswirksamer müssen auch die Politikinhalte werden. Aus diesem Grunde ist es besonders wichtig, dass moderne Demokratien über eine ausprägte nachrichtendienstliche Kernstaatlichkeit zur Forcierung strategischer Interessen verfügen. Sie kann die demokratie-bedingte Ämterdiskontinuität durch objektive Inhaltsvermittlung und Politikberatung etwas abschwächen, um so die Kontinuität (sicherheits-)politischer Entscheidungen nach innen wie auch nach außen zu stärken. Die „Beratungstätigkeit" politischer Repräsentanten erfolgt entweder über inoffizielle oder offizielle Kontakte (in Form eines strukturierten Dialoges). Bei diesem Zusammentreffen zwischen Politikern und nachrichtendienstlichem Personal können zwei unterschiedliche soziale Welten aufeinander treffen. Dadurch sind Kommunikations- und Verständnisdefizite in fachlichen Fragen möglich. So besteht nach Auffassung US-amerikanischer Intelligenceexperten das Risiko der politischen Instrumentalisierung oder unter den Voraussetzungen der Privatisierungsprämisse (Auslagerung von nachrichtendienstlichen Aufgaben an private Intelligencefirmen) sogar eine indirekte Steuerung von politischen Agenden im Sinne großkapitalistischer Interessen (z. B. Konzerne und regionale Wirtschaftsinteressen sowie Stärkung der Rüstungsindustrie).

Zur Vermeidung dieser politischen Instrumentalisierung forcierten US-Intelligenceexperten in den 1950er-Jahren den sog. „Trennungsimperativ“ zwischen Politik und Intelligence. Dabei ergab sich allerdings das Problem mangelnder Kommunikation zwischen beiden Ebenen und damit verbunden kam es zu einem Verlust im Bereich der Informationsdominanz zur Beherrschung von Bedrohungen. Dieser Trennungsimperativ wird von Gregory Treverton mit seinem Modell der „bright line“ – also eines ausgeprägten strukturierten Dialoges – ergänzt. Dabei steht die Vernetzung von Intelligence und Politik an erster Stelle, so sollen in erster Linie Kommunikations- und Verständnisdefizite minimiert werden. Allerdings beherbergt dieser sehr aktive Austauschprozess das Risiko minimierter Objektivität aufgrund des Naheverhältnisses von Intelligence zur dominanten Politik. Für Treverton bieten die neuen Informations- und Kommunikationstechnologien Möglichkeiten nachrichtendienstlicher Informationsvermittlung vor allem im Bereich von OSINT. Dabei müssen die analytischen Kernkompetenzen eindeutig im staatlichen Bereich liegen, um der Gefahr der „militanten Zusammenarbeit“ (im Sinne von Rolf Uesseler[76]) zwischen Politik und Wirtschaft und der politischen Instrumentalisierung von Intelligence durch die Politik vorbeugen zu können.

Militarisierung von Intelligence

Durch veränderte sicherheitspolitische Rahmenbedingungen kam es seit Mitte der 1990er-Jahre zu einer grundlegenden Neuausrichtung nachrichtendienstlicher Auftragsstrukturen, die sich seither verstärkt auf den militärischen Anwendungsbereich zubewegten, wodurch es zu einer sogenannten Militarisierung von Intelligence kam.[77] Die militärische Primärorientierung nachrichtendienstlicher Auftragserfüllung bezieht sich ganz einfach auf den gestiegenen Intelligencebedarf im militärischen Bereich und insbesondere im Zug von Anti-Terroroperationen sowie Einsätzen im Ausland. Dadurch, dass sich das Feindbild vom staatlichen

[76] Uesseler, Rolf: Krieg als Dienstleistung – Private Militärfirmen zerstören die Demokratie. Berlin 2006, S. 129f.
[77] Vgl. Treverton, Gregory F.: Reshaping National Intelligence For An Age of Information. Cambridge 2001, S. 62ff.

zum nichtstaatlichen Akteur verlagert hat, wurden neue nachrichtendienstliche Aufgabenfelder für militärische Anwendungsbereiche erschlossen, die den Einsatz von Spezialisten einfordert. Dadurch kam es in den letzten zehn Jahren zu einer verstärkten Zusammenarbeit zwischen Militär und Intelligence. Damit wurde eine umfassende Kooperation begründet, die sich auf alle Beschaffungs- und Analyseebenen auswirkt. Für Gregory Treverton liegt der Grund für die aktuelle militärische Primärorientierung von Intelligence im neuen Gefechtsfeld, das sich aus kleineren Einheiten zusammensetzt. Der „unsichtbare" Feind lässt sich in der Regel schwerer identifizieren als ein staatlicher Kontrahent. Aber selbst der traditionelle Aufmarsch von zwei gefechtsbereiten Armeen sieht nach Treverton heute anders aus, weil die Informationsdimension des sogenannten „Info-Warriors" über Sieg oder Niederlage entscheidet. Die hohe Präzision weitreichender Waffensysteme würde große Einheiten rasch vernichten, daher wurden große durch kleinere und flexiblere Verbände abgelöst, wie es die USA unter Verteidigungsminister Donald Rumsfeld in Afghanistan 2001 und im Irak-Krieg 2003 praktizierten. Eine wesentliche Veränderung erfährt die Kriegsführung durch jene Waffensysteme, die über Tausende von Kilometer nahezu punktgenau gegen feindliche Ziele eingesetzt werden können. Dabei steuert bereits heute privates Vertragspersonal solche Waffensysteme, wodurch auch die klare Unterscheidung zwischen militärischem und zivilem Personal immer schwieriger wird. Das Gefechtsfeld der Zukunft wird von neuen Technologien beherrscht werden, die den modernen Krieger aus sicherer Entfernung agieren lässt. Damit könnte für große Teile moderner Armeen das Kampfgeschehen zu einem PC-Game „degenerieren", bei dem man ohne jegliche menschliche Empfindungen feindliche Ziele eliminieren lässt. Auch hier wird die Differenzierung zwischen Militär und Zivilpersonen immer schwieriger, weil eine Unterscheidung aus der Entfernung kaum eindeutig ausfallen kann. In diesem Zusammenhang wird man dann wohl auch weiterhin sogenannte Kollateralschäden in Kauf nehmen. Die militärische Primärorientierung von Intelligence wurde bereits in den Golf-Kriegen 1991 und 2003 deutlich, in denen SOFs als Beobachtungsposten im Feindgebiet eingesetzt wurden, die wiederum als Relaisstationen zur Bekämpfung irakischer Einheiten dienten, ohne jedoch selbst in den Kampf eingreifen zu müssen. Integration von HUMINT-Fähigkeiten in das militärische Führungsver-

fahren haben in den USA bereits zu einer institutionellen Verzahnung zwischen Militär und der IC geführt. Spezialoperationen der CIA beispielsweise werden mit militärischer Präzision durchgeführt und mit den lokalen eigenen Truppenteilen auch koordiniert, wenn dies erforderlich ist. Aber auch zahlreiches privates Vertragspersonal von privaten Sicherheits- und Militärfirmen ist im Vorfeld eingebunden. Obwohl es zu einer verstärkten HUMINT-Komponente im modernen Kriegen kommt, wird diese im Informationsbereich zusätzlich noch durch umfassende TECHINT-Elemente ergänzt, deren Wertigkeit allerdings mit zunehmender Distanz zum eigentlichen Geschehen abnimmt, weil die Unmittelbarkeit bessere Resultate produziert. D. h., militärische Entscheidungen basieren auf einer komplementären HUMINT-TECHINT-Komponente, die wiederum in Verbindung mit dem Prinzip der Unmittelbarkeit am effektivsten ist. Im Rahmen dieser sogenannten „support for military operations“ (SMOs) werden eigenständige Programme innerhalb der IC entwickelt, um in erster Linie Aufträge und Prioritäten sowie in zweiter Linie entwicklungstechnische Programme festlegen zu können.[78] Sie sollen einen reibungslosen Zugriff auf Intelligenceressourcen für militärische Operationen sicherstellen. Die militärische Primärorientierung von Intelligence wird auch im Counterinsurgency deutlich.

Intelligence und Counterinsurgency

Die Rolle von Intelligence im Counterinsurgency (Kampf gegen Aufständische) unterscheidet sich dramatisch von den Anforderungen konventioneller Kriegsführung. Während die „traditionelle“ militärische Aufklärungsarbeit durch[79] moderne Technologien in den Bereichen SIGINT, RADINT, MASINT, IMINT etc. unterstützt wird, um so feindliche Kampftruppen erfassen zu können, gestaltet sich die Beschaffung nachrichtendienstlicher Informationen über z. B. Aufständische im Irak oder die Taliban-Kräfte in Afghanistan wesentlich schwieriger. Die nachrichtendienstliche Aufklärung der Ziele und Absichten von Terro-

[78] Vgl. Treverton, Gregory: Reshaping National Intelligence For an Age of Information. Cambridge 2001, S. 62-65.
[79] Corum, James: Getting Doctrine Right. NDUPress, Issue 49, 2/2008, S. 93-97.

risten, Widerstandskämpfern und Aufständischen ist aufs engste mit den jeweiligen HUMINT-Fähigkeiten einer Intelligenceorganisation im Einsatzraum verbunden. Hierzu gehört vor allem die Fertigkeit, die Sprache, Kultur und Gebräche der lokalen Bevölkerung verstehen zu können. Aber auch die politischen und ideologischen Empfindungen im Einsatzraum sind ausschlaggebend für gute Aufklärungsergebnisse. Vor allem die US-Intelligenceorganisationen haben diese speziellen HUMINT-Voraussetzungen erkannt und entsprechende Adaptionen in ihren HUMINT-Ops durchgeführt. Trotzdem sind noch einige Defizite vorhanden, wie James S. Corum vom Department of Joint and Mulitnational Operations vom General Staff College in Fort Leavenworth festhält. Dabei ist es entscheidend, dass die HUMINT-Erfordernisse eines Einsatzes im Bereich Counterinsurgency bereits vorab auf- und ausgebaut werden. Nur so könne nach Auffassung von James Corum adäquates HUMINT zur Bekämpfung von Terroristen und Widerstandsgruppen produziert werden.[80] Der soziale, ideologische und strukturelle Kontext von Widerstandsgruppen könne nur von HUMINT analysiert und verstanden werden. Während sogenannte Fernerkundungssensoren (IMINT, MASINT, etc.) faktische Gegebenheiten reflektieren und Aufschlüsse über z. B. militärische Aufmarschpläne geben können, vermag HUMINT die Gründe, Ziele und Absichten ausführender Stellen darzustellen. Daher werden „highly effective intelligence analysts“ benötigt, die allerdings nicht immer in erforderlichem Ausmaß vorhanden sind. Um in diesem Bereich der HUMINT an Flexibilität zu gewinnen, und um die geforderten HUMINT-Kapazitäten überhaupt aufbringen zu können, greift die US-Regierung auf private Intelligence-Firmen zurück, die entsprechend qualifiziertes Personal (Kenntnisse lokaler Gegebenheiten, Sprachbeherrschung, kulturelle Erfahrungen, etc.) mitbringen. Dabei übernehmen solche privaten Firmen allerdings quasi hoheitliche Aufgabenstellungen im nachrichtendienstlichen Bereich, der bereits zu heftigen politischen Diskussionen führte. Im Policy-Bereich einer Intelligenceorganisation ergibt sich die Problematik der Kompetenzschaffung unter Berücksichtigung aktueller und zukünftiger Konflikte in bestimmten Regionen. Allerdings bedingen konservativ-bürokratische Grundvoraussetzungen andere Vorgaben, wodurch eine langfristige Planung für die Anschaffung

[80] Vgl. Corum, James: Getting Doctrine Right. NDUPress, Issue 49, 2/2008, S. 96.

von HUMINT-Assets oftmals nicht möglich ist. Strukturkonservatie Bürokratien bezahlen allerdings für ihre Starrheit oft einen sehr hohen Preis, wenn man HUMINT-Erfordernisse vor dem Hintergrund des internationalen Terrorismus betrachtet. Rechtzeitig vorhandene HUMINT-Spezialisten für Sprache, Kultur, Religion und Ideologie hätten mit großer Wahrscheinlichkeit Konflikte und Auseinandersetzungen bereits im Vorfeld verhindern können. Die aktuellen Probleme im Bereich HUMINT werden auf die weitreichenden Kürzungen und auf den Personalabbau im HUMINT-Bereich nach dem Ende des Kalten Krieges zurückgeführt.[81] Den Preis dafür zahlen in erster Linie unsere Soldaten im Einsatz.

Verdeckte Operationen

Während in 1990er-Jahren verdeckte Operationen – sogenannte Covert Actions/Operations – nur zögerlich durch die politische Führung angeordnet wurden, bedienen sich größere Staaten wieder vermehrt verdeckter Operationen, um bestimmte Ziele zu erreichen. Politische Irritationen als Resultat gescheiteter Missionen gab es und wird es auch immer geben, allerdings scheint die Bereitschaft, solche Irritationen auszutragen, gestiegen zu sein. Die USA nehmen solche politischen „Unebenheiten" in den internationalen Beziehungen mittlerweile ganz bewusst in Kauf, weil sie sich durch die Anwendung verdeckter Operationen einen Mehrwert an nationaler Sicherheit erwarten. Nach dem 11. September 2001 beurteilten die USA, dass verdeckte Operationen und sogar gezielte Attentate oder die Entführung von vermeidlichen Terroristen notwendige nachrichtendienstliche Mittel in der Terrorismusbekämpfung sind. Selbst internationale Vorbehalte und Kritik von Seiten der eigenen Politiker änderten an der Beurteilung der US-Administration nichts. Daher erscheint es unbedingt erforderlich, diesen Bereich näher zu betrachten, weil er ein fester Bestandteil der nachrichtendienstlichen Transformation ist. Vor allem im Bereich der operativen Aufklärung haben sich große Veränderungen ergeben, die die Fähigkeit zur proaktiven Adaption nachrichtendienstlicher Strukturen hervorheben. Das entscheidende Dis-

[81] Vgl. Corum, James: Getting Doctrine Right. NDUPress, Issue 49, 2/2008, S. 96.

tinktionsmerkmal adaptiver verdeckter Operationen liegt in ihrer operationellen Diversifikation in Bezug auf eingesetzte Personen, Methoden, Zielsetzungen sowie Operationsgebiete. Dabei wird heute noch viel weniger auf nationale Gesetze Rücksicht genommen. Internationale Bestimmungen, die sich auf völkerrechtsrelevante Quellen in Bezug auf den Schutz von Personen und Grundrechten beziehen, sind nahezu obsolet geworden. Vor allem für die großen und mächtigen Länder scheinen verdeckte Operationen zu einem utilitaristischen Hilfsmittel geworden zu sein, auf das sie sich bei der Bekämpfung terroristischer Elemente abstützen. Auf die Grundrechte der Betroffenen wird dabei eigentlich nur im Zuge weiterführender Ermittlungen genommen. Obwohl verdeckte Operationen ein genuin nachrichtendienstliches Element der operativen Aufklärung darstellen, scheinen sie sich im Zuge der 1990er-Jahre immer mehr zu einem „politischen" Machtelement entwickelt zu haben, das primär dann angewendet wird, wenn der Staat keine anderen Mittel zur Bekämpfung einer bestimmten Bedrohung mehr hat. Verdeckte Operationen stellen einen ursprünglich politischen Bezugsrahmen her, der allerdings über die nachrichtendienstliche Institution „umgeleitet" wird, um einen direkten Sachzusammenhang zwischen verdeckter Operation und politischen Entscheidungsträgern negieren zu können. In den USA wird dieses Verfahren als Instrument der plausiblen Negation von Verantwortung bezeichnet („plausible deniability"). Die Transformation im Bereich der verdeckten Operationen verdeutlicht eines sehr genau, und zwar die Tatsache, dass die Staatenwelt unter realistischen Umfeldbedingungen funktioniert. Anarchie, Selbsthilfeprinzip und Balance-of-Power gehören zu den macht- und sicherheitspolitischen Determinanten, die mit Hilfe moderner Intelligencearbeit abgedeckt werden sollen. In diesem realpolitischen Kontext verlassen sich staatliche Akteure grundsätzlich nur auf eigene Fähigkeiten. Je umfassender diese eigenen (Intelligence-)Fähigkeiten zur Bewältigung des staatenweltlichen Bedrohungsumfeldes sind, umso intensiver werden diese auch gegen andere staatliche und nichtstaatliche Akteure angewendet. Verdeckte Operationen werden nach realpolitischen Gesichtspunkten appliziert und erst in zweiter Linie kommen politische und rechtliche Aspekte hinzu. Die politischen und rechtlichen Aspekte treten dann in Erscheinung, wenn eine verdeckte Operation fehlgeschlagen ist. Dabei versuchen die verantwortlichen Akteure, ihre Aktionen in der Regel nachträglich zu legitimieren,

zu dementieren oder neu zu interpretieren. Staatlicher Eigenschutz mit Hilfe verdeckter Operationen zu Erlangung eines politischen oder militärischen Vorteils wird dabei durchwegs höher bewertet als rein rechtliche Bestimmungen, die z. B. die Festnahme, das Verhören mit härteren Methoden oder eventuell sogar die gezielte Tötung eines als Feind erkannten Akteurs nicht erlauben würden. Allerdings birgt diese staatliche Handlungsoption zusätzliche Gefahren in sich, die sich in einer höheren reziproken Gewaltbereitschaft niederschlagen und das internationale Rechtssystem erodieren. Dabei können auf internationaler Staatenebene durchwegs zwei Strömungen herausgenommen werden. Während die großen Länder der Welt, wie z. B. die USA, Russland und China progressiv an verdeckten Operationen festhalten, um ihre nationalen Sicherheitsinteressen zu wahren, verhalten sich Mittel- und Kleinstaaten wesentlich zurückhaltender und akzeptieren internationale Normenvorgaben bei der Gestaltung ihrer nationalen Außen- und Sicherheitspolitiken. Für sie sind verdeckte Operationen in entlegenen Gebieten keine wirkliche Option. Allerdings könnte sich bei zunehmenden terroristischen Aktivitäten und regionalen Konflikten auch diese Position verändern, die wiederum auf nationale Intelligenceorganisationen rückwirken könnte, weil sich durch höhere Gewaltdichte der politische Handlungsdruck vermehrt. So könnte die Tendenz der engeren Zusammenarbeit in Form nachrichtendienstlicher Kooperativen auch den Bereich der verdeckten Operationen erfassen. Als besonderes Beispiel könnten hier die geheimen Verbindungsflüge US-amerikanischer Behörden mit gefangen genommenen Terroristen genannt werden. Sie erhielten in der Öffentlichkeit eine breitere mediale Aufmerksamkeit, die auch zu diversen parlamentarischen Anfragen in unterschiedlichen europäischen Ländern führte. Diese Entwicklung könnte sich auch auf andere Bereiche ausbreiten, was schließlich zu einer quasi aktiven Partizipation an verdeckten Operationen der USA oder anderer Nationen führen könnte. Damit verlieren jedoch auch Kleinstaaten ihre „Unschuld“ im Kampf gegen den Terrorismus. Heute kann davon ausgegangen werden, dass es keine westlichen Staaten mehr gibt, die nicht im internationalen Kampf gegen den Terrorismus eingebunden wären. Diese Darstellung hat jedoch nicht nur für den Bereich der verdeckten Operationen seine Gültigkeit, sondern auch für andere staatliche Bereiche im nachrichtendienstlichen Nahebereich.

Private Intelligencefirmen

Aufgrund der vielfältigen sicherheitspolitischen Herausforderungen mit ihren diversifizierten Kompetenzanforderungen bedienen sich die USA (und einige andere westliche Staaten) mittlerweile nicht nur mehr traditioneller Instrumente zur Aufklärung von Gegnern, sondern auch privater Sicherheits- und Militärfirmen, einschließlich spezialisierter privater Nachrichtendienste. Über die Auswirkungen auf das staatliche Gewaltmonopol, die Rechtstaatlichkeit und demokratische Kontrollinstanzen ist noch recht wenig bekannt. Es wird allerdings bereits vor allzu umfassenden Auslagerungen von derart sensiblen Aufgabenbereichen in den Privatsektor für die staatliche Sicherheit gewarnt. Aber selbst dieser Aspekt ist Teil des Ganzen und gliedert sich damit in den weltweit geführten Krieg gegen die Feinde des Westens ein. Der Feind kann uns daher nicht nur auf der konkreten und gegenständlichen Ebene mittels Bombenanschlag Schaden zufügen, sondern kann uns auch auf der abstrakteren Systemebene massiv in unseren Freiheiten einschränken, indem beispielsweise unsere demokratiepolitischen Errungenschaften durch nichtstaatliche Akteure unterwandert werden. Wie in dieser Arbeit noch verdeutlicht wird, ist die Grundvoraussetzung für eine erfolgreiche nachrichtendienstliche Transformation eine gefestigte Staatlichkeit, die über die gesellschaftspolitische Steuerungskompetenz verfügt. Nur so können vorhandene flexible und innovative Konzepte zur Terrorismusbekämpfung eingefordert und appliziert werden. Dazu gehört auch die private Option aufgrund ihres Innovations- und Ideengehaltes. Staaten, die sich für die private Option entschieden, dürfen die oberste Verpflichtung von Staatlichkeit nicht vernachlässigen. Hier gilt der ideengeschichtliche Grundkonsens der klassischen Staatslehre, wonach die Institutionen der inneren und äußeren Staatssicherheit (Militär, Polizei, Gerichtsbarkeit) den Schutz der eigenen Bevölkerung vor äußeren Angriffen zu bewahren haben.[82] Gleichzeitig muss die Regierung mittels staatlicher Supervision die positive Koordinierung von gesellschaftspolitischen Partikularinte-

[82] Vgl. Waltz, Kenneth N.: Man, the State and War – A Theoretical Analysis. New York 2001, S. 95f.

ressen sicherstellen,[83] um zum einen die Staatlichkeit zu festigen und zum anderen Sicherheit und Gerechtigkeit gewährleisten zu können. Allerdings begehen die westlichen Regierungen zahlreiche Fehler bei der Auslagerung von staatlichen Sicherheitsaufgaben aufgrund einer neoliberalen Grundhaltung, wonach der Aspekt der Kosten-Nutzen-Frage unreflektiert zu weitreichenden Privatisierungsvorhaben führt(e). Sicherheit ist aber Allgemeingut und gewährleistet das soziale und gesellschaftspolitische Zusammenleben der Bürger im Staat. Der Versuch, Sicherheit nach ökonomischen Grundsätzen kalkulieren und quantifizieren zu wollen, negiert essentielle immaterielle Aspekte staatlicher Sicherheit, deren Nutzen erst durch langfristige Entwicklungen sichtbar wird. Privatisierung von Sicherheit bedeutet heute die Entgrenzung von Sicherheit und führt zu einer ungleichen Verteilung, die sich nach den finanziellen Möglichkeiten orientiert. Nur wer sich Sicherheit leisten kann, bekommt diese auch. Damit werden allerdings innergesellschaftliche Konfliktlinien geschaffen, deren Auswirkungen in Zukunft durchaus dramatisch sein können. Es sind daher die entsprechenden gesetzlichen Rahmenbedienungen zu schaffen, um einer ungleichen Verteilung von Sicherheit vorzubeugen. Es können ideengeschichtlich nur Staaten sein, die über das rechtlich legitimierte Gewaltmonopol nach innen wie auch nach außen verfügen, weil ausschließlich sie zur Gewaltanwendung bestimmt sind, um Ungerechtigkeit oder Angriffe gegen die territoriale Unversehrtheit abwehren zu können.[84] Der ideengeschichtliche Kriegsbegriff wird so zum gesellschaftspolitisch-immanenten Normalzustand nach Thomas Hobbes, wonach der Kampf eines jeden gegen jeden unaufhörlich tobt. Sollte das staatliche Gewaltmonopol durch die zunehmende Auslagerung von Sicherheitsaufgaben weiter betrieben werden, dann besteht die Gefahr des Verlustes des staatlichen Gewaltmonopols. Diese Entwicklung würde die Preisgabe der Sicherheit an den privaten Bereich bedeuten, wodurch die Entscheidung über Krieg oder Frieden

[83] Der Begriff der Supervision und seines Teilkonzeptes der positiven Koordination gesellschaftspolitischer Partikularinteressen wurde von Helmut Wilke übernommen. Vgl. Wilke, Helmut: Supervision des Staates, Suhrkamp 1997.

[84] Angelehnt an die Aussage des ehemaligen britischen Außenministers, Sir Edward Grey, wonach der Staat Krieg zur Aufrechterhaltung des Gesetzes führen darf. Vgl. Waltz, Kenneth N.: Man, the state and war – a theoretical analysis. New York 2001, S. 97.

nicht mehr staatlich wäre, sondern von kapitalstarken Konzernen oder Einzelpersonen getroffen würde. Die Erkenntnis, wonach der Rückzug des Staates eher die Ungerechtigkeit in der Ressourcenverteilung fördert, könnte dann auch auf den Bereich der Sicherheit ausgeweitet werden. Dabei wäre allerdings der Großteil der Bevölkerung in negativer Weise betroffen. Zur Vermeidung einer solchen Entwicklung staatlicher Sicherheitsgewährleistung sollte der Staat als soziale Institution die politische Regulierungsinitiative im Hinblick auf die Auslagerung von Sicherheitsdienstleistungen ergreifen. Dabei ist entscheidend, dass der Staat nicht nur die Regulierung entlang funktionaler Gesichtspunkte verfolgt, sondern insgesamt als das ultimative Steuerungsmedium für eine positive Koordinierung gesellschaftspolitischer Partikularinteressen fungiert. In diesem Kontext übernimmt Intelligence eine politische Beraterfunktion, indem nachrichtendienstliche Erkenntnisse die Informationsdominanz staatlicher Entscheidungsgremien fördern. Politische und vor allem sicherheitspolitische Herausforderungen könnten mit Hilfe von Intelligenceanalysen rational beherrscht respektive bewältigt werden. Die US-amerikanische Intelligenceexpertin Jennifer E. Sims spricht in diesem Zusammenhang von „Entscheidungsvorteilen" für Politiker, Militärs, Diplomaten und andere Regierungsbeamte, um die nationalen Interessen in Zeiten des Friedens wie des Krieges zu bewahren.[85] Aus diesem Grund scheint die Bewahrung einer nachrichtendienstlichen Kernstaatlichkeit als Ausdruck der Supervisionsfähigkeit des Staates als unbedingt erforderlich. Sie ist Ausdruck einer kooptiven Methode zur Prävention von Konflikten und Kriegen, weil sie im Sinne eines kooperativen Gedankengutes die positive Koordination (und damit auch den konstruktiven Wettbewerb der Ideen) der Gesellschaftsinteressen fördert. Die Supervisionsfähigkeit des Staates basiert auf den nachrichtendienstlichen Fähigkeiten der institutionalisierten Kernstaatlichkeit. Sie wird in den modernen Demokratien in der Regel durch sogenannte Informationsbarrieren als Ausdruck der Informationssicherheit zur Erlangung von Informationsdominanz begrenzt. Methoden der nachrichtendienstlichen Beschaffung und der exklusive Zugang zu den Intelligenceanalysen gewähren jene politische Handlungsfreiheit, die für eine positive Koordi-

[85] Sims, Jennifer E.: Understanding Friends and Enemies. In: Sims, Jennifer E., Gerber, Burton (Hrsg.): Transforming U.S. Intelligence. Washington, D.C. 2005, S. 16.

nierung unterschiedlicher Interessen notwendig ist. Die nachrichtendienstliche Kernstaatlichkeit ist für sicherheitspolitische und militärstrategische Entscheidungen von besonderer Bedeutung, da es sich hierbei in der Regel um gesamtstaatliche Entscheidungen von weitreichender Bedeutung handelt. Aber auch der einsatzbezogene Arbeitscharakter erfordert institutionalisierte Prozesse und Abläufe, die genuin staatlicher Provenienz sind.

Bedeutende Intelligencefirmen

Einer der erfolgreichsten privaten Intelligenceanbieter ist die Sicherheits- und IT-Firma CACI mit dem Leitspruch „Ever Vigilant“.[86] Ihre Dienstleistungen umfassen „Solutions“ in den Bereichen der Systemintegration, Netzwerksysteme, Logistik, Informationsmanagement u. a. CACI wurde jedoch noch aus einem anderen Grund „berühmt“; sie war in den US-Folterskandal im irakischen Gefängnis Abu Ghraib involviert. Die genaue Rolle von CACI und anderen privaten Sicherheitsfirmen wurde in zahlreichen Artikeln und offiziellen Untersuchungen beleuchtet. Um den schweren Vorwürfen von Seiten der Politik und Öffentlichkeit entgegenzutreten, publizierte das Management von CACI ein eigenes Buch mit dem Titel „Our Good Name“. Diese proaktive Krisenbewältigung sollte die Kritik der Gegner am Vorgehen abschwächen und die Reputation der Firma in der Öffentlichkeit wiederherstellen.

Eine andere bedeutende Intelligencefirma ist Total Intelligence Solution (TIS), die zur Prince Group gehört. TIS verfügt über ein Global Fusion Center (GFC), das intelligencerelevante Informationen beschafft, auswertet, analysiert und an den jeweiligen staatlichen oder nichtstaatlichen Auftraggeber weiterleitet.[87] Die Intelligencefirma erhält ihre Aufträge von US-Behörden und von größeren Firmen und Konzernen (Top 100 Unternehmen der USA). So können Klienten von TIS auf eine umfassende intelligencespezifische Sicherung ihrer finanziellen Interessen und

[86] Vgl. die Webseite der Firma CACI. Online-Dokument: <www.caci.com>, abgerufen am 9.6.2008.
[87] Vgl. die Webseite der Firma Total Intelligence Solution. Online-Dokument: <www.totalintel.com>, abgerufen am 10.6.2008.

Assets abstellen. Im Falle einer akuten Bedrohung oder Krise werden die verantwortlichen Akteure innerhalb kürzester Zeit über die aktuelle Sicherheitslage informiert. Bei Bedarf können sogar Notfallpläne in Kraft gesetzt werden, die z. B. für die Evakuierung von Personal aus einer Krisenzone vorgesehen sind. In diesem sehr spezifischen Fall können TIS-Klienten sogar auf IMINT (elektro-optische Satelliten), hochwertige topografische Karten sowie auf eine Lagebeurteilung zurückgreifen, was für eine Evakuierung besonders bedeutsam sein kann. Dabei sieht der Notfallplan auch sogenannte „safe places" vor, sollte eine Evakuierung nicht durchgeführt werden können. Ein solcher Notfallplan ist nach TIS-Angaben auch mit den offiziellen Regierungsstellen der US-Administration akkordiert.[88] Das GFC erfüllt jedoch auch noch andere, durchwegs beeindruckende intelligencerelevante Funktionen. So werden durch Spezialisten im GFC sieben sicherheitsbezogene Sektoren abgedeckt. Hierzu zählen:

a) politische Gewalt und Terrorismus,
b) Schutz kritischer Infrastruktur,
c) geopolitische Entwicklungen,
d) internationale Kriminalität,
e) soziale Unruhen und politische Konflikte,
f) Umwelt und Gesundheit sowie
g) makro-ökonomische Analysen und Prognosen.

Diese sieben Analysesektoren des TIS-GFC werden entlang funktioneller Kriterien bearbeitet, um eben den Anforderungen der Klienten entsprechen zu können.[89] Vor diesem Hintergrund erstellt das GFC von TIS für seine staatlichen und nicht-staatlichen Auftraggeber entsprechende Produkte. GFC erstellt Intelligence Assessments, Bedrohungsanalysen, tagesaktuelle Zusammenfassungen (Daily Intelligence Summaries), sogenannte Optionenanalysen (Alternative Analyses) und Langezeitprognosen. Darüber hinaus bietet TIS auch eine Unterstützung für Operationen an, wie beispielsweise die Bereitstellung von Sprach- und Überset-

[88] Vgl. die Webseite der Firma Total Intelligence Solution. Online-Dokument: <www.totalintel.com>, abgerufen am 10.6.2008.
[89] Vgl. a.a.O.

zungskenntnissen,[90] um eben diese Bandbreite an Expertisen und Dienstleistungen abdecken zu können.

Während die meisten Intelligencefirmen ihre Dienste anderen Wirtschaftsubjekten anbieten, gibt es natürlich auch für Privatpersonen spezielle Schutzdienste, die auf Intelligence basieren können. So bietet beispielsweise die britische Sicherheitsfirma Maritime Asset Security & Training (MAST) intelligencebasierte Schutzmaßnahmen für exklusive Jachten an. Der Werbetext der Sicherheitsfirma verspricht ihren Kunden Schutz vor Angriffen und Piraterie.[91] Diese und andere Firmen verdeutlichen nicht nur den gestiegenen Bedarf an Sicherheit für besonders exponierte Persönlichkeiten, sondern auch die Tatsache, dass die nationale Politik für Sicherheit nur mehr marginal aufkommen kann. Allerdings verweist diese Situation bereits auf eine starke ungleiche Verteilung von Ressourcen, die als zunehmendes Sicherheitsproblem (weltweit) erkannt wird. Sicherheit und Schutz gibt es vor allem für jene, die sich Sicherheitsdienste leisten können. Diese akkordierte Zusammenarbeit zwischen Kapital und dem privaten Sicherheitssektor stellt eine erfolgreiche Strategie der „Verursacher" von Ungleichheit, Lebensmittelknappheit (Spekulationsobjekte) und allgemeiner Ressourcenverteilung dar. Jene, die aufgrund von Spekulationen hart getroffen werden, weil sie sich wegen der Spekulationen die Preise für Lebensmittel nicht mehr leisten können, sind jedoch der vollen Bandbreite an Unsicherheit ausgesetzt.[92] Diese Entwicklung ist in zahlreichen Regionen feststellbar. Eine Verschärfung dieser bereits ungleichen Verteilung von Sicherheit erfahren allerdings auch westliche Demokratien, indem sie neoliberale Politikagenden weiterverfolgen und selbst den Sicherheitssektor der Privatisierung unreflektiert und unreguliert öffnen. So stellt die Privatisierung von intelligencerelevanten Aufgaben und Instrumenten einen maßgeblichen Einschnitt in das souveräne Gewaltmonopol dar, weil durch die Privatisierung von Intelligence die Informationsdominanz auf den außerstaatlichen Sektor überzugehen droht. Staatliche Entscheidungsprozesse wer-

[90] Vgl. a.a.O.
[91] Vgl. Maritime Asset Security&Training Online-Dokument: <www.mast-yacht.co.uk>, abgerufen am 12.6.2008.
[92] Vgl. hierzu Uesseler, Rolf: Krieg als Dienstleistung. Berlin 2006.

den so einer indirekten Steuerung im Sinne einiger weniger Wirtschaftsakteure preisgegeben. Privatisierung von Intelligence und Sicherheit wäre idealerweise erst dann eine gute Option, wenn alle involvierten staatlichen Institutionen mit Hilfe von gesetzlichen Bestimmungen und funktionellen Regelungen die Privatisierung von Sicherheit umfassend kontrollieren und überwachen könnten. Diese idealistische Grundvoraussetzung ist bis dato nur sehr rudimentär existent, wodurch sich der Bedarf einer umfangreichen politischen Debatte in Europa (aber auch international) ergibt. Staaten sind schon sehr oft in eine falsch verstandene neoliberale „Privatisierungsfalle“ getappt, die für die breite Masse und den Staat mit Mehrkosten, Subventionen und Korruption verbunden war. Eine ähnliche Entwicklung könnte auch den Intelligencebereich in den westlichen Ländern treffen. Eine unkontrollierte Privatisierung von Intelligence würde den Machtverlust der nachrichtendienstlichen Kernstaatlichkeit bedeuten und damit die Staatlichkeit weiter untergraben.

Negative Auswirkungen des liberalisierten Marktes können mit Hilfe von privaten Sicherheitsakteuren beherrscht werden. Insbesondere die Intelligencefirmen stellen hier jenes Wissen zur Verfügung, das die zunehmenden Sicherheitsrisiken für einen Wirtschaftsakteur begrenzt. Dadurch kam es in den letzten Jahren zu einer umfassenden Entstaatlichung von Sicherheit. Selbst demokratische Länder sind davor nicht gefeit. Politische Wachsamkeit ist daher unbedingt notwendig, um nicht auch noch die letzten Elemente gefestigter Staatlichkeit zu verlieren. Denn spätestens seit Thomas Hobbes, Niccolo Machiavelli, Hans Morgenthau und Kenneth Waltz sollten die realpolitischen Funktionsprinzipien und Strukturen von Politik und Macht bekannt sein. Vor diesem sehr problematischen und kritischen Hintergrund neuerer politischer Entwicklungen seit dem 11. September 2001 sollten Entscheidungen von Intelligenceorganisationen in Bezug auf die private Intelligenceoption genauestens reflektiert und kalkuliert werden. Sie tragen eine wesentliche Verantwortung für die Aufrechterhaltung der nachrichtendienstlichen Kernstaatlichkeit als Ausdruck einer funktionierenden Staatlichkeit nach demokratischen Prinzipien. Das Problem ist allerdings die bürokratische Starrheit existierender Institutionen, die durch die ideologisch motivierten Akteure überholt werden, weil sie die ultimative Motivation im Kampf gegen den Westen besitzen. Ihre ideologische Verklärung resul-

tiert in einer weltweit akkordierten Strategie zur Verbreitung von Terror und Angst. Kreativität, Flexibilität und Innovationskraft können mit Hilfe externer Elemente privater Innovationen teilweise erreicht werden. Allerdings bedürfen diese wiederum einer entsprechenden Tätigkeits- und Qualitätskontrolle.

Der ehemalige Vizeadmiral Herbert A. Browne sprach in Anlehnung an US-Präsident Eisenhower von einem „Intelligence-Industrial Complex", der bereits 70% des Intelligencebudgets beansprucht.[93] Seit zehn Jahren betreibt die US-Intelligence Community (US-IC) eine umfassende Auslagerung von nachrichtendienstlichen Aufgaben in den privaten Bereich. Nach Tim Shorrock managen PIF Spionagenetzwerke, betreiben SIGINT, führen verdeckte Operationen durch und verhören sogar vermeintliche Terroristen.[94] Problematisch an dieser Entwicklung ist die Tatsache, dass die Finanzmittel nicht zum Auf- und Ausbau eigener nationaler Expertenpools, IT-Fertigkeiten für TECHINT und Informationsmanagement geschaffen werden, sondern eine „ganze Armee von Analysten und Experten innerhalb des privaten Sektors" geschaffen wurde. Damit bekommen Rüstungskonzerne über ihre PIF nachrichtendienstliche Kompetenzen und Zugang zu den höchsten sicherheitspolitischen Entscheidungsgremien. Diese Entwicklung markiert eindeutig einen Paradigmenwechsel struktureller Zusammenarbeit zwischen Staat und Privatsektor. Der Staat verliert in diesem Bereich rasant an Einfluss, weil er die Analysen der PIF kaum kontrollieren kann. Nicht die Interessen des Staates, sondern die der Wirtschaftskonzerne stehen hier im Vordergrund. Herbert A. Browne bezeichnet den Paradigmenwechsel im Intelligence-Sektor als Triumph kapitalistischer Innovationen, der ein neues Zeitalter der Zusammenarbeit zwischen Wirtschaft und Regierung markiert:

> "The fact that we can have a professional intelligence organization outside of the government to support the government is no more offensive to me than the fact that we have 80 percent of our military communications traveling on

[93] Schätzung des ODNI gem. Shorrock, Tim: Spies for Hire – The Secret World of Intelligence Outsourcing. New York 2008, S. 13.
[94] Vgl. Shorrock, Tim: Spies for Hire, 2008, S. 12.

> commercial satellites or commercial fiber optics. […] In fact, I find it very healthy for the nation."[95]

Kritiker sehen diese Entwicklung weniger positiv. Vor allem aus rechtlicher Perspektive ergeben sich zahlreiche Schwierigkeiten, wenn es um gesetzeskonforme Ermittlungs- und Befragungsmethoden von vermeintlichen Terroristen geht. Rechtsstaatlichkeit und Grundrechtsschutz werden durch die Auslagerung von nachrichtendienstlichen Aufgaben untergraben; dies könnte fatale Auswirkungen auf Politik und Gesellschaft entfalten, da die Glaubwürdigkeit der Justiz sowie das Vertrauen in die Zuverlässigkeit staatlicher Institutionen gefährdet wird. Durch die Auslagerung von intelligencerelevanten Aufgaben werden demokratiepolitische Entwicklungen in Gang gesetzt, die auch die Bedeutung nationaler Parlamente als Kontrollgremium unterwandern. Mit anderen Worten negieren die USA (und andere Demokratien) staatsrechtliche Funktionsprinzipien zentraler Bereiche von Staatlichkeit. Erkenntnisse funktioneller Differenzierung staatspolitischer Verantwortungsbereiche werden so ad absurdum geführt. Dadurch werden hobbesianische Handlungsstrukturen revitalisiert und drohen so, den Anarchiegehalt auf nationaler aber insbesondere auf internationaler Ebene dramatisch auszuweiten. Mögliche Resultate dieser Entwicklung können vermehrte Konflikte und kriegerische Auseinandersetzungen sein, weil das Vertrauen in institutionelle Grundpfeiler staatlicher Bürokratien und Verwaltung relativiert wird. So entsteht das Verlangen nach mehr privater Sicherheit, weil staatliche Sicherheitsverantwortung reduziert wird. Diese Entwicklungslinien sind sowohl für nationale wie auch für internationale Strukturen von Bedeutung. Tim Shorrock lässt keinen Zweifel daran, dass das „spying for hire" zum „way of life" in den Vereinigten Staaten von Amerika des 21. Jhdt. geworden ist.[96] Shorrock untermauert seine Behauptung mit empirischen Daten. So arbeitet für die CIA mittlerweile mehr privates Personal als eigene Staatsbedienstete.[97] Zudem sollen 50 bis 60% des CIA-Budgets an PIF vergeben werden. Auch die Mitarbeiter des CIA National Clandestine Service (CIA-NCS) sollen bereits zur Hälfte aus priva-

[95] Herbert A. Browne zit. nach Shorrock, Tim: Spies for Hire, 2008, S. 13.
[96] A.a.O.
[97] Die CIA soll über 17 500 eigene Mitarbeiter verfügen. Ebd., S. 13f.

tem Vertragspersonal bestehen. Ihre Tätigkeiten umfassen Rekrutierung von Informanten sowie die Durchführung/Partizipation an verdeckten Operationen weltweit.[98] Eine noch dramatischere Auslagerung hat die National Security Agency (NSA) seit der zweiten Hälfte der 1990er-Jahre in Angriff genommen. Durch die rasante Neuerung am IKT-Sektor sah sich die NSA-Führung gezwungen, Firmen zu beauftragen, um eine effektive Beschaffung, Auswertung und Analyse von intelligencerelevanten Informationen gewährleisten zu können. Dienstleistungen des Privatsektors werden als „vital" eingestuft. Auch im Bereich des Pentagons (Department of Defense, DoD) kam es im Zuge der Operationen in Afghanistan und Irak zu einer umfassenden Auslagerung nachrichtendienstlicher Funktionen in den Bereichen IMINT und SIGINT. Shorrock schätzt, dass rund 35% des DIA-Personals (Defense Intelligence Agency) privates Vertragspersonal von PIF sind.[99] In welchem Umfang die Auslagerung von Intelligenceaufgaben staatlich überwacht und kontrolliert werden kann, ist fraglich, weil selbst der US-Kongress offensichtlich nur begrenzten Zugriff auf Verträge mit PIF hat.[100] Durch die mangelnde Transparenz von PIF-Aktivitäten im Intelligenceumfeld wird ein günstiges Umfeld für Korruption geschaffen. Immer dort, wo es keine Kontrolle gibt, besteht ein besonders hohes Risiko des Machtmissbrauches. Über das Volumen und den Umfang von Korruption lassen sich keine gesicherten Aussagen treffen, es kann aber davon ausgegangen werden, dass im Vergleich zu den PMF-Korruptionsfällen durchwegs hohe Belastungen für den Steuerzahler zu erwarten sind. Auch über den angeblichen Kostenvorteil durch die Auslagerung bestehen gravierende Zweifel. So werden durch private Firmen professionelle Mitarbeiter von Nachrichtendiensten abgeworben, die schließlich wieder im Rahmen eines Vertrages im Intelligencewesen eingesetzt werden. Dabei werden die Kosten für die Ausbildung und Personalentwicklung (Ausbau von Ex-

[98] Vgl. ebd., S. 14.
[99] Vgl. a.a.O.
[100] Überprüfungen von Verträgen der Regierung mit PIF können durch einem Verweis auf erforderliche Geheimhaltung und nationale Sicherheit verhindert werden. Vgl. Aftergood, Steven (FAS) bei Shorrock, Tim: The Corporate takeover of U.S. intelligence. Online-Dokument: <www.salon.com/news/features/2007/06/01/intel_contrators>, abgerufen am 16.6.2008.

pertisen) nicht gegengerechnet.[101] Diese Kosten trägt der Steuerzahler. Er trägt auch die höheren Kosten für das private Vertragsverhältnis durch die Rechnungslegung einer PIF als Auftragnehmer. Das Senate Intelligence Committee kommt in einem offiziellen Bericht zu dem Schluss, dass die Intelligence Community ihre Abhängigkeit in Bezug auf privates Vertragspersonal reduzieren sollte. Das Komitee errechnete, dass ein Regierungsbeamter in einer Intelligencefunktion etwa 125 000 US-D pro Jahr kostet, wohingegen ein privater Vertragsnehmer einer PIF mit 250 000 US-D pro Jahr errechnet wurde.[102]

In diesem Kontext wird von kritischen Kommentatoren auch die Frage gestellt, inwieweit beispielsweise der President's Daily Brief (PDB) überhaupt noch die offizielle staatliche Sichtweise reflektiert, wenn private Akteure am Entstehen des PDB maßgeblich (wenn nicht sogar führend) beteiligt sind. Diese Frage ist insofern berechtigt, weil sich wirtschaftliche Interessen auf die Selektion von Informationen auswirken können. Gesamtgesellschaftliche Entwicklungen könnten dabei in den Hintergrund treten, weil sie für wirtschaftliche Akteure keine oder nur eine geringe Relevanz aufweisen. Daher ist das Selektionskriterium von Informationen im Zuge von analytischen Arbeiten kritisch zu beleuchten. Immerhin sind SAIC, CACI International, Northrop Grumman, Center for Intelligence Research and Analysis (CIRA) u. a. führend am PDB beteiligt. Daher muss die Frage gestellt werden, wer denn überhaupt diese Firmen kontrolliert, ihre Arbeiten überwacht und ihre Produkte evaluiert. Für Steven Aftergood von der Federation of American Scientists stellt die Auslagerung von Intelligence eine Transformation der nachrichtendienstlichen Arbeitsweise dar, die allerdings von privaten Interessen dominiert wird.[103] Das Problem der staatlichen Kontrolle und Trans-

---

[101] Vgl. The US Intelligence Community's Five Year Strategic Human Capital Plan. Online-Dokument: <www.odni.gov/Publications/DNIHumanCapitalStrategicPlan18 October2006.pdf>, abgerufen am 16.6.2008.

[102] Vgl. hiezu Select Committee on Intelligence. 110th Congress, 1st Session, Report 110-75. Online-Dokument: <http://intelligence.senate.gov/11075.pdf>, abgerufen am 16.6.2008.

[103] Vgl. Aftergood, Steven (FAS) bei Shorrock, Tim: The Corporate takeover of U.S. intelligence. Online-Dokument: <www.salon.com/news/features/2007/06/01/intel_ contrators>, abgerufen am 16.6.2008.

parenz hat sich sehr deutlich im Folterskandal von Abu Ghraib gezeigt, wo privates Vertragspersonal Gefangene verhörte und dabei Verhörmethoden anwendete, die nicht erlaubt waren. Strafrechtliche Konsequenzen aus dem Folterskandal gab es für das verantwortliche Personal so gut wie keine. Vor allem diese äußerst prekäre Angelegenheit der Verhöre sollte explizit eine staatliche bleiben. Bedauerlicherweise hat die US-Regierung sogar die Ausbildung von Verhörspezialisten in den Privatsektor ausgelagert.[104] Auch das National Reconnaissance Office (NRO) könnte ohne privates Vertragspersonal den Betrieb von Satelliten nicht mehr gewährleisten. Nahezu die gesamte Wartung und der technische Betrieb der NRO-IMINT-Ressourcen wird von sogenannten „highly integrated industrial government team(s)“[105] wahrgenommen.[106] Die Firma In-Q-Tel[107] ist ein ausgezeichnetes Exempel für den hohen Verschmelzungsgrad zwischen Intelligence und Wirtschaft. In-Q-Tel wurde 1999 von George Tenet (ehemaliger CIA-Direktor) gegründet. Dabei handelt es sich um eine Beteiligungsgesellschaft, die nach privaten Intelligenceapplikationen Ausschau hält. Brauchbare Intelligenceapplikationen werden gekauft und weiterentwickelt. In-Q-Tel hält nach Darstellung von Tim Shorrock an über 90 Firmen äquivalente Beteiligungen. Dabei werden führende Positionen in Entwickler-Firmen mit ehemaligen CIA-Mitarbeitern besetzt.[108] Shorrock spricht von einem ganzen Industriekomplex, der mittlerweile von drei Interessensorganisationen vertreten werde. Was für die privaten Militärfirmen (PMF) die International Peace Operations Association (IPOA, USA) ist, ist für die PIF die Intelligence and National Security Alliance (INSA)[109] oder die Armed Foreces Communications and Electronics Association (AFCEA).[110]

---

[104] Vgl. Shorrock, Tim: Spies for Hire, 2008, S. 14.
[105] Kerr, Donald M. zit. nach Shorrock, Tim: Spies for Hire, 2008, S. 14.
[106] A.a.O.
[107] Vgl. die Webseite der Firma In-Q-Tel. Online-Dokument: <www.inqtel>, abgerufen am 17.6.2008.
[108] Vgl. Shorrock, Tim: Spies for Hire, 2008, S. 14
[109] Intelligence and National Security Alliance. Online-Dokument: <www.insaonline.org/>, abgerufen am 17.6.2008.
[110] Armed Foreces Communications and Electronics Association. Online-Dokument: <www.afcea.org/>, abgerufen am 17.6.2008.

Der Umfang der Auslagerung nachrichtendienstlicher Aufgaben in den Privatsektor wird von Experten als Teil einer grundlegenden Transformation im Intelligencewesen begriffen. Für Steven Aftergood repräsentiert die 70%-Marke eine absolute und risikoreiche Trendwende im Intelligencebereich. Für ihn ist dieser Teilaspekt nachrichtendienstlicher Transformation etwas „Neues", das von privaten Intelligencefirmen dominiert wird.[111] Daher wird bereits von einer „contratctor-dominated bureaucracy" gesprochen. Privatisierung staatlicher Bürokratien kommuniziert eine hochgradige tautologische Entwicklung. Man könnte aber auch davon sprechen, dass von nun an die Interessen kapitalistischer Organisationen eine schleichende Revolution lenken, die das Staatsganze und seine Bürger dem Wohlwollen einiger sehr mächtiger Gruppen aussetzt, weil damit sowohl demokratiepolitische und grundrechtsrelevante Prinzipien staatlicher Bürokratien negiert werden. Bereits anhand der mangelnden Transparenz im Vergabeprozess von millionenschweren Aufträgen wird die Problematik der politischen Kontrolle sichtbar. Ohne Transparenz gibt es keine effektive Kontrolle und damit werden korrupte Strukturen gefördert. Welche gesamtgesellschaftlichen negativen Auswirkungen durch korrupte (Staats)Strukturen möglich sind, hat uns die russische Politik und Gesellschaft in den 1990er-Jahren veranschaulicht. Westliche Staaten sollten daher nur entlang effektiver Regulierungsinstrumente Auslagerung betreiben sowie die „kapitalistisch-instrumentalisierte Privatisierungsthese" distanzierter und kritischer betrachten. Vor allem in den USA wurde auf diese Problematik durch das „Project on Government Oversight" hingewiesen. Aber auch offizielle Stellen, wie beispielsweise der US-Kongress oder das „Government Accountability Office" (GAO) kennen die Problematik mangelnder Transparenz und ihre negativen Auswirkungen. Gleichzeitig bedeutet Geheimhaltung nicht nur mangelnde Transparenz auf der Auftraggeberseite, sondern birgt auch betriebswirtschaftliche Probleme für Firmen in sich, da es teilweise nicht möglich ist, erhaltene Regierungsaufträge öffentlich zu machen. Damit können gewünschte Effekte wie z. B. Kurzgewinne an den Börsen nicht immer realisiert werden.[112] Um dennoch ein gewisses Vertrauen von Aktionären zu bekommen, werden Verträge – deren In-

[111] Aftergood, Steven zit. nach Shorrock, Tim: Spies for Hire, 2008, S. 19f.
[112] Vgl. Shorrock, Tim: Spies for Hire, 2008, S. 22.

halt nicht bekannt gegeben werden kann – umschrieben. Konzerne und ihre PIFs sprechen z. B. von Aufträgen zur „Unterstützung von Intelligencemissionen im Kampf gegen den Terrorismus“.[113] Shorrock schlussfolgert, dass die zehn wichtigsten PIF in allen Intelligencebereichen involviert sind. Sie werden von ihm als die „Giganten der Spionageindustrie“ bezeichnet.[114] Private Vertragsnehmer betrachten sich daher nicht als Firmenmitarbeiter, sondern vielmehr als offizielle Vertreter staatlicher Einrichtungen. Immerhin – so deren Argumentation – leiste man ja einen umfangreichen Dienst an der Nation und bekämpfe aktiv den internationalen Terrorismus. In dieser Tradition steht auch CACI International, das darüber hinaus den Intelligencesektor auch noch als besonders „attraktiv“ bezeichnet, weil die Regierungsaufträge in der Regel für fünf bis zehn Jahre (!) vergeben werden.[115]

Das vorläufige Fazit der Auslagerung von intelligencerelevanten Aufgaben in den Privatbereich manifestiert eine strukturelle Abhängigkeit von Intelligenceorganisationen nicht nur im technischen Betriebs- und Wartungssektor, sondern auch im analytischen Bereich. Dieser Befund ist aus staats- und demokratiepolitischer Perspektive ein sehr bedenklicher, weil dadurch die Unabhängigkeit politischer Handlungsfunktionäre und des militärischen Sicherheitsbereiches nicht mehr gewährleistet ist. Die Interessen der Wirtschaft und des Kapitals korrumpieren explizit oder implizit die Präferenzen des Staates als Institution der Gesamtheit der Bürger. Durch die enge Zusammenarbeit zwischen beiden gesellschaftspolitischen Elementen kann eine Beeinflussung respektive Steuerung von Kommunikationsprozessen im Entscheidungsfindungsverlauf festgestellt werden. Die Entscheidung über den Zuschlag für die Erneuerung der US-amerikanischen Tankerflotte an EADS und Northrop verdeutlicht nicht nur die politische Tragweite, sondern auch die enormen finanziellen Mittel, die im Zuge von Ausschreibungen vergeben werden.[116] Es kann daher nur im Interesse demokratiepolitischer Institutionen sein, solche Vergabegrößen transparent zu gestalten, weil die Gefahr

[113] Firma ManTech zit. nach Shorrock, Tim: Spies for Hire, 2008, S. 22.
[114] Ebd., S. 24.
[115] Ebd., S. 27.
[116] Journal of International Peace Operations, Volume 5, Number 1, July-August 2009.

und das Ausmaß möglicher Korruption minimiert werden muss. Nur wenn sich Parlamente und deren Kontrolleinrichtungen (Ausschüsse und Sonderausschüsse) nachhaltig mit den Vor- und Nachteilen der Auslagerung von Sicherheit und insbesondere auch mit der „Privatisierung“ und Auslagerung von Intelligence auseinandersetzen, kann die nötige demokratiepolitische Transparenz dieses speziellen Auslagerungsprozesses erreicht werden. In den USA hat das Informations- und Kontrollverlangen des Kongress schließlich zur Übermittlung von Daten über das Ausmaß der Auslagerung von intelligencerelevanten Aufgaben geführt. Allerdings sollte dieser politische Druck kontinuierlich aufrechterhalten bleiben, damit eine noch höhere Transparenz sowie verbesserte gesetzliche Regelungen für eine funktionelle Regulierung privatisierter Sicherheitsaufgaben erzielt werden können. Shorrock verortet im ODNI bereits ein „Trainingscamp“ für zukünftiges privates Vertragspersonal,[117] was wohl kaum im Interesse der Politik und des Staates sein kann. Es macht den Anschein, als ob Privatisierung und Auslagerung ohne kritische Reflexion in Bezug auf ihre politischen und rechtsstaatlichen Dimensionen verfolgt werden. Trotz der hohen staatspolitischen und rechtlichen Gewichtung der nachrichtendienstlichen Aufgabendislozierung in den privaten Bereich ist die Politik in westlichen Demokratien noch recht passiv, was die öffentliche – und damit demokratiepolitische Legitimierung – dieses Aspektes angeht. Aufgrund der thematischen Komplexität und sicherheitspolitischen Bedeutung bietet dieses Thema nur geringes politisches Profilierungspotential. Daher ist dieser politische Sicherheitsaspekt für die Politik von zweitrangiger Bedeutung. Das heißt aber nicht, dass die entsprechenden politischen Referenten und Experten dem Thema vollkommen passiv gegenüberstehen.

[117] Shorrock, Tim: Spies f or Hire, 2008, S. 18.

Der Feind

Die politikwissenschaftliche Literatur ist sich darüber einig, dass Intelligenceorganisationen ein einzigartiges Instrument darstellen, um den internationalen Terrorismus bekämpfen zu können. Nachrichtendienste sind die erste Verteidigungslinie gegen den internationalen Terrorismus, mit deren Hilfe bereits zahlreiche Anschläge verhindert werden konnten. Bedauerlicherweise haben politische Integrationsmaßnahmen die Herausbildung von „Homegrown Terrorism" nicht verhindern können. Daher sind die Nachrichtendienste im Bereich der umfassenden Sicherheitsvorsorge ein zentraler Bestandteil geblieben, den auch die Politik als solchen erkennt.

Ob bildungspolitische Integrationsmaßnahmen sowie Maßnahmen gegen Radikalisierung jugendlicher Muslime in Europa ausreichen, um islamistisch-motivierten Terrorismus vermeiden zu können, ist fraglich. Solange es islamistische Hassprediger gibt, die in der EU relativ ungehindert reisen können, werden die oben angesprochenen Maßnahmen gegen Radikalisierung konterkariert. Aus der Sicht von Experten werden gemäßigte Imame zu Vermeidung von Radikalisierung junger Muslime immer noch zu wenig in die Pflicht genommen. Aber auch das Internet biete nahezu jede Möglichkeit radikale Inhalte konsumieren zu können, die kaum kontrollierbar sind.

Eine Analyse ideologischer Grundpositionierungen von Ayman al-Zawahiri – dem Chefideologen der al-Qaida – untermauert das terroristische Gefahrenpotential in den westlichen Industrieländern. Er ist allerdings nur einer von hunderten führenden Ideologen, die Islamexperten benennen. Sie gelten als die führenden Köpfe eines weltweit angeleiteten bewaffneten Dschihadismus.[118] In ideologischer Hinsicht konstruierte al-Qaida eine Art „Bekennerideologie", die die Formierung kleinerer Gruppen ermöglicht, ohne dass die einzelnen ideologisch-motivierten Bekennergruppen miteinander kommunizieren müssen. Dieses Konzept

[118] Vgl. hierzu auch die Studie von Prucha, Nico: Die Stimme des Dschihad. Hamburg 2010.

leitet sich aus den Aussagen von al-Zawahiri ab, weil er in der Kommunikation als Schnittstelle einen schwachen Punkt für ein globales Islamisten-Netzwerk erkannte.[119] Ob die aktuellen Bemühungen der Terrorismusbekämpfung effektiv genug sind, lässt sich nur mittels einer eingehenden Untersuchung feststellen. Erkenntnisse von Experten über die Möglichkeiten, den modernen Terrorismus unter Einhaltung demokratischer und rechtstaatlicher Rahmenbedingungen zu bekämpfen, sind politisch schwer umsetzbar.[120] Die Terrorismusforschung wirft der Politik vor, lediglich eine Symptombehandlung zu betreiben; die eigentlichen sozio-ökonomischen, historischen und religiösen Ursachen bleiben weitgehend ausgespart.[121] Dennoch war es den Nachrichtendiensten möglich, einige beachtliche Erfolg in der Terrorismusbekämpfung zu erzielen. Dadurch bleibt die intelligencegeleitete Terrorismusbekämpfung weiterhin auf der „politischen Agenda" der EU.

Gewaltbereite Islamisten agieren durchwegs nach rationellen Gesichtspunkten. Sie analysieren nachrichtendienstliche und militärische Methoden der Terrorismusbekämpfung und adaptieren ihre eigene Kampfführung je nach Bedarf. Der Feind betreibt in diesem Sinne so etwas wie „Counter-Counter-Terrorism". Informationen westlicher Akteure (z.B. SOF in Afghanistan), die in die Hände der Terroristen gelangen, werden genau gelesen und ausgewertet. Die taktische Lernfähigkeit der Terroristen wird in diversen Internetforen unter Beweis gestellt (z.B. Anschlagsvideos).[122]

Um die Erfolge im Kampf gegen Radikalisierung und Terrorismus fortführen zu können, müssen die Experten in den Intelligenceorganisationen ihre Gegner kennen. Das folgende Kapitel versucht die subversive Arbeit radikal-islamistischer Gewaltgruppierungen näher zu beleuchten.

---

[119] Vgl. insbesondere Kapitel II der Studie von Prucha, Nico: Die Stimme des Dschihad. Hamburg 2010, S. 73-116.

[120] Vgl. Netanyahu, Benjamin: Fighting Terrorism – How Democracies Can Defeat the International Terrorist Network. New York 2001.

[121] Vgl. Johnson, Scott: Dilemmas of the Horn. In: Newsweek, 28. April 2008, S. 32. Obwohl bis vor kurzem zwischen der al-Turki-Miliz und al-Qa'ida keine Verbindung bestand, versucht die Miliz – nach Aussagen ihres Sprechers Sheik Mukhtar Robow – diese nun im Lichte der US-Operationen herzustellen.

[122] Vgl. hierzu die Studie von Prucha, Nico: Die Stimme des Dschihad. Hamburg 2010.

Intelligencearbeit in Terrororganisationen – Der Versuch eines Vergleiches

Parallelen zwischen Terrororganisationen und staatlichen Nachrichtendiensten?

Auf den ersten Blick scheinen Warners Kernelemente des Intelligencebegriffes Parallelen zu strategischen und taktischen Überlegungen größerer Terrororganisationen zu haben. Lässt man zunächst den Kostenfaktor von Intelligenceorganisationen beiseite und betrachtet lediglich die Komplexität derartiger Organisationen, kann man sich dem Zweifel von Robert Baer, dass eine Anschlagsplanung in der Größenordnung von 9/11 kaum aus einer „Höhle“ in Afghanistan vorstellbar ist,[123] nur anschließen. Sollten derartige Anschläge tatsächlich aus solchen „Kommandozentralen“ zu planen sein, muss die Effizienz technisch hochgerüsteter westlicher Intelligenceorganisationen hinterfragt werden.

Die Anwendung verdeckter Operationen ist eine Voraussetzung für terroristische Gruppierungen, um so effektive Anschläge durchführen zu können und damit Regierungen und Organisationen zu beeinflussen. Vor allem Anschläge größeren Ausmaßes wie z. B. jene des 11. September 2001 in den USA sowie Madrid 2004 und London 2005 bedingen eine längere Planungsphase, um die logistische Herausforderung eines Anschlags zu meistern. Dazu zählt das Sammeln unzähliger Einzelinformationen, die ausgewertet und analysiert und zu einem Gesamtplan zusammengestellt werden müssen.

Strategie

Je kleiner eine Terrorgruppierung ist, desto kurzfristiger muss ihre Strategie sein. Kleinere Gruppen bedeuten gleichzeitig auch, dass diese schwieriger aufzuspüren sind. Dies hat ebenso Einfluss auf die Intelli-

[123] Baer, Robert: Der Niedergang der CIA. München 2003, S. 10.

gencearbeit der Terrorgruppierung, was sich in der Dauer von Planungsschritten und somit in der vorgestaffelten Informationsbeschaffung auswirkt. Ehemalige Soldaten, die in Afghanistan eingesetzt waren, bestätigen dies: "In our portion of Afghanistan, most enemy leaders did not view their IO (Anm.: information operations) as part of a long-term goal and assumed they could create an advantage by releasing outrangeous propaganda."[124] Dies hat wiederum Auswirkungen auf die Strategie der Gruppierung. Große Wirkung zu erreichen, erfordert auch eine ausgeklügelte Strategie, die einen längeren Zeitraum in Anspruch nimmt.

Um ein frühzeitiges Vereiteln von Anschlägen zu verhindern, muss eine Terrororganisation Anschlagsvorbereitungen möglichst geheim halten. Auch die Produktion bzw. die Verbreitung/Ausstreuung von Informationen/Desinformationen kann entweder vor oder/und nach einem Anschlag für den Zweck terroristischer Anschläge entscheidend sein. Anschläge haben für Terrororganisationen nur dann Sinn, wenn sie mit den Attentaten ihre Botschaft möglichst großflächig verbreiten. Dies erfordert exakte Planung und Wissen über Kommunikationsstrategien und deren Auswirkungen, was wiederum eine gewisse Organisationsgröße voraussetzt, um gute Intelligencearbeit durchführen zu können.

Größere Anschläge bedürfen eines größeren Planungsaufwandes und somit einer dementsprechend größeren, effizienteren Organisation. Ebenso steigen die Anforderungen an die Intelligencearbeit. So fanden laut 9/11 Commission Report bereits zwischen 1998/99 die ersten Planungsschritte für den späteren Anschlag statt.[125] Demzufolge befand sich zu Beginn 2001 in New York auf Anweisung Osama bin Ladens ein Kundschafter in New York, um lohnende wirtschaftliche und jüdische Ziele auszumachen.[126]

Terroranschläge sind demnach mit verdeckten militärischen Operationen (covert actions) – die wiederum nur mit guten Intelligenceergebnissen

[124] Captain Andrew J. Knight. FA: Tactical IO in Afghanistan. In: Artillery Journal 3/07, S. 38.
[125] Vgl. The 9/11 Commission Report, S. 150.
[126] Vgl. a.a.O.

erreicht werden können (oder auch als Teil von Intelligence zu bezeichnen sind) – durchaus zu vergleichen. So ist eine verdeckte Aktion „an option short of military action to achieve objectives that diplomacy and other policy means cannot".[127] Versucht wird dies mit Propaganda, Unterstützung von ausländischen politischen oder militärischen Interessensgruppierungen und der Ausführung gesetzlich umstrittener Aktivitäten auf fremden Boden.

Somit implizieren „covert actions" eine starke Ähnlichkeit mit Aktivitäten von Terrororganisationen. Dies kann auch aus einer Studie des Geneva Centre for the Democratic Control of Armed Foces (DCAF) analysiert werden. Die Absicht von Intelligence kann gemäß dieser Studie sein:[128]

- die Zurverfügungstellung von Analysen über bestimmte Regionen;
- die Hilfe zur Erkennung von Vorhaben gegenwärtiger oder potentieller Gegner;
- Planung militärischer Operationen;
- Schutz militärischer Operationen;
- Schutz von Geheimnissen;
- verdeckt zu agieren, um Entwicklungen der Interessen zu beeinflussen.

Daraus ist abzuleiten, dass Terrororganisationen ebenso einen „Bedarf" an Intelligence haben. Haben sie einen solchen, stellt sich die Frage nach dem Aufbau der Organisation und deren Grundsätzen. Wird nach rationellen Methoden und Grundlagen entschieden? Gibt es Ähnlichkeiten zu Nachrichtendiensten oder unterscheiden sie sich von diesen? Essenziell sind auch die finanziellen Ressourcen. Sind Budgets westlicher Nachrichtendienste generell geheim, so zeigt dennoch eine Studie der Federation of American Scientists, dass das US Intelligence Budget seit 1980

[127] DCAF Backgrounder: Intelligence Services (03/2006). Online-Dokument: <http://www.dcaf.ch/_docs/bg_intelligence_services.pdf>, abgerufen am 18.8.2008, S. 2.
[128] A.a.O.

signifikanter anstieg als das Verteidigungsbudget.[129] Betrug das Intelligence Budget 1998 26,7 Mrd. US-D, wurden für 2007 43,5 Mrd. US-D veranschlagt. Somit gab es seit 9/11 einen „upward trend in intelligence spending".[130] Es ist davon auszugehen, dass auch terroristische Gruppierungen ein ökonomisch relevantes Äquivalent zu westlichen Nachrichtendiensten haben. Dies aber nur dann, wenn die Terrorgruppierung oder -organisation eine gewisse Größenordnung erreicht.

Wird von der Metapher Machiavellis ausgegangen, nach der das Militär das Dach eines Hauses darstellt und daraus gefolgert, dass moderne Nachrichtendienste dabei ein tragendes Element sind, so muss dies für alle ähnlich gearteten Organisationsformen Gültigkeit besitzen. Demnach müssen Terrororganisationen nicht nur nach adäquaten Mustern aufgebaut sein, sondern auch ähnlich arbeiten. Haben also Terrororganisationen analoge Schemen zu westlichen Intelligenceorganisationen (wie z. B. Strukturen und Arbeitsweisen) und welche Rückschlüsse können daraus gezogen werden?

Dass in erster Linie große Terrororganisationen strategisch, operationell und taktisch zugleich agieren, zeigen die zuletzt durchgeführten großen Terroranschläge in den USA 2001, Madrid 2004 und London 2005.

Die Geister, die ich rief …

Parallelen zu Terrororganisationen werden immer wieder durch Gerüchte geschürt, in denen einigen Nachrichtendiensten die Gründung und Unterstützung von Terrororganisationen vorgeworfen wird. So wird zum Beispiel dem pakistanischen Nachrichtendienst (Inter-Service Intelligence – ISI) unter anderem vorgeworfen, hinter den Anschlägen in Mumbai im November 2008, bei denen 163 Menschen starben, zu stehen. Offizielle pakistanische Stellen dementierten allerdings diese Vorwürfe stets. Anfang Dezember 2008 wurden Mitglieder der Terrororga-

[129] Vgl. Online-Dokument: <http://www.fas.org/irp/budget/index.html>, abgerufen am 6. Jänner 2009.
[130] Vgl. a.a.O.

nisation „Lashkar e-Taiba“ in einem ihrer Lager in Pakistan von pakistanischen Sicherheitskräften festgenommen. Die Festgenommenen werden verdächtigt, die Anschläge in Mumbai geplant und gelenkt zu haben. Erwähnenswert ist insbesonders, dass laut amerikanischen Geheimdienstquellen diese Gruppierung durch den ISI nicht nur ins Leben gerufen worden sei (für den Kampf gegen Indien in Kashmir), sondern von ihm auch geschützt und unterstützt worden wäre.[131]

Staatliche Nachrichtendienste beschäftigen für unterschiedlichste Aufgaben IT-Spezialisten. Die Arbeit reicht dabei von der technischen Aufklärung, Rekrutierung bis hin zu Werbemaßnahmen, Informationsarbeit- und Desinformationsmethoden. Das Internet spielt hierbei eine zunehmende Rolle.

Gibt es bei Terrororganisationen eine „lessons learned“ aus dem nachrichtendienstlichen Bereich bzw. lernen beide voneinander? Wenn ja, woher erhalten Terrorgruppierungen ihre „lessons learned“ und wie wirken sie sich aus?

Rekrutierungs- und Ausbildungsmethoden

Insbesondere Anschläge größeren Ausmaßes erfordern gut geschultes Personal. Rohan Gunaratna spricht im Zusammenhang mit al-Qaidas Trainingscamps von einem dreiteiligen Curriculum der Ausbildung:[132]

- einem basic,
- einem advanced und
- einem specialized training.

Die Unterschiede ergeben sich vor allem in den unterschiedlichen Lehrinhalten. Die am meisten verbreitete Form war allerdings jene des recruit, basic oder general trainings. All diese Formen benötigen neben

[131] Vgl. Pakistan Arrests Suspects in Mumbai Attacks. Online-Dokument: <http://www.nytimes.com/2008/12/09/world/asia/09pstan.html?hp=&pagewanted=print>, abgerufen am 8.12.2008.
[132] Gunaratna, Rohan: Inside Al Qaeda. New York, 2003, S. 95ff.

einer guten Infrastruktur auch ausgeklügelte Organisationsstrukturen und -schritte in Verbindung mit Geheimhaltungsmaßnahmen. So wurden zum Beispiel aus den angeblich zehntausenden in al-Qaidas Trainingslagern Ausgebildeten lediglich einige Tausend für den innersten Zirkel der Organisation auserkoren. Entsprechen die genannten Zahlen der in den Lagern ausgebildeten Dschihadis nur annähernd der Realität, dann bedarf es einer ausgeklügelten Infrastruktur und Planung. Ausbildungsvorhaben dieser Größenordnung können nicht ohne Wissen der westlichen Welt und insbesondere ihrer Nachrichtendienste geschehen sein.

Ähnlichkeiten von westlichen Organisationssystemen und der Terrororganisation al-Qaida sind auch an ihren Rekrutierungsmethoden zum Erhalt neuer Mitglieder ersichtlich. Während die USA durch den Aufruf zum „War on Terror“ versuchen, Unterstützer zum gemeinsamen Kampf zu vereinigen, versuchte al-Qaida, durch Terroranschläge und Videobotschaften neue Anhänger zu gewinnen.

Auch Lenin erkannte die Wichtigkeit einer Auslese bei der Rekrutierung: „Das einzige, erste Organisationsprinzip muss für die Funktionäre unserer Bewegung sein: strenge Konspiration, strengste Auslese der Mitglieder, Heranbildung von Berufsrevolutionären, die einander das volle und kameradschaftliche Vertrauen entgegen bringen.“[133] In Trainingslagern führten auch Guerillas Ausleseverfahren mit ähnlichen Prinzipien durch.

Derartige Verfahren totalitärer Regimes, von Guerillas und Spezialeinsatzkräften westlicher Staaten erinnern demnach stark an Trainings- und Auswahlverfahren bei Terrororganisationen. Für Beitrittsrituale muss der Beitrittskandidat bereit sein, größtmögliche Erniedrigungen zu ertragen. Jugendbanden haben ähnliche „Rituale“. Dabei ist es möglich, dass Neuankömmlinge eine Tracht Prügel über sich ergehen lassen müssen ohne sich zu wehren. Schläge und Demütigungen müssen dabei wegsteckt werden.[134] Wehleidig zu sein oder nachtragend zu reagieren, ist ein Ausscheidungskriterium. Gerade größere Terrorgruppierungen

[133] Pohrt, Wolfgang: Brothers in Crime. Edition Tiamat. Berlin 2000, S. 24.
[134] Vgl. Pohrt, Wolfgang: Brothers in Crime. Edition Tiamat, Berlin 2000, S. 31.

scheinen stark an solchen Auswahlverfahren angelehnt zu sein und erzeugen so einen enormen Gruppendruck. Nur so ist absolute Zuverlässigkeit, Verschwiegenheit und Unterordnung in dem mit terroristischer Taktik geführten Kampf überprüfbar und letztendlich garantiert. Als Beispiel dient der ungeheuere Gruppendruck, der auf Hasib Hussain nach seinem wahrscheinlich ersten misslungenen Bombenanschlag (London im Juli 2005) gelastet haben muss, um trotz allem sein Attentat doch noch auszuführen.

Nachrichtendienste dürften auf junge Menschen als potentielle Bewerber eine ähnlich mystische Ausstrahlung ausüben wie Terrororganisationen für deren Sympathisanten. Auch beim ehemaligen US-Agenten Robert Baer wurde – erstmals mit dem Namen CIA konfrontiert – die Neugier geweckt. Baer gestand ein, „ … bei all den Makeln, die der CIA anhafteten, schien es so etwas wie Romantik pur zu sein, für den Geheimdienst zu arbeiten“.[135] Nachdem Baer bei der CIA anrief, musste er zunächst mehrere umfangreiche Fragebögen detailliert ausfüllen, um schließlich zum ersten Vorstellungsgespräch zugelassen zu werden. Einer der letzten Tests, die Baer zu absolvieren hatte, war ein zeitintensiver Lügendetektortest in einem Hotel. Die Überprüfung des direkten und indirekten Umfeldes des Bewerbers ist eine zusätzliche Hürde für eine Aufnahme in den Kreis der „Gemeinschaft“. Den Abschluss bildeten laut Baer unterschiedliche intensive und zum Teil zermürbende Trainingsprogramme. Dabei wurde versucht, die Teilnehmer zu Fehlern zu provozieren und so einem psychischen Druck auszusetzen. Ziel war die Belastung der Probanden zu testen, um die Besten auszuwählen.

Dies sind Zeichen dafür, dass sich Nachrichtendienste nicht nur vor Infiltration schützen wollen, sondern auch die für die jeweilige Arbeit notwendigen Charaktere ausfiltern.

Ähnliche Ausbildungs- und Ausleseverfahren – allerdings noch inhumaner – wandte man in Guerilla-Trainingslagern an. Demnach versuchte man in einem als „Assessment Center“ benannten Ausbildungslager das

[135] Siehe Baer, Robert: Der Niedergang der CIA. München 2003, S. 37ff.

„Innerste der Kandidaten nach außen zu kehren“.[136] Damit wird die „soziale Kompetenz“ der Person getestet. Kontrolle gibt es durch einen ständig anwesenden Beobachter sowie durch die Gruppe und deren Konformitätsdruck. Derartige „Ausleseverfahren“ nehmen auf die Selbständigkeit des Individuums keinerlei Rücksicht. Vergleicht man diese Verfahren mit jenen von Terrorcamps, so dürfte es starke Affinitäten geben. Speziell religiös radikalisierte Gruppierungen zielen noch stärker auf die Abkoppelung des Menschen von seinen Individualrechten ab. Unterordnung wird begründet mit dem Willen eines höheren Wesens – eben jenes in Form einer Gottheit – den es zu befolgen gilt, selbst unter Aufopferung des eigenen Lebens.

Staatliche Nachrichtendienste haben ähnliche, mit jenen von Terrororganisationen durchaus zu vergleichende, aktive Werbungsmethoden. So zum Beispiel wirbt der britische Auslandsnachrichtendienst MI6 im Internet mit proaktiven Mitteln um Nachwuchsagenten. Mitglieder sozialer Netzwerkplattformen sind Zielgruppe von Werbebotschaften mit der Überschrift „Spion gesucht“.[137] Gelangweilte sollen so zum Jobwechsel bewogen werden. Geworben wird aber nicht nur im Internet sondern ebenso mit Hilfe von Zeitungsannoncen und Radiospots. Diese Werbemethoden sind sich insbesondere bei islamistischen Terrororganisationen nicht unbekannt.

Arbeitsweise und Taktik

Generell wird Wissen über Arbeitsweisen von Intelligenceorganisationen geheim gehalten. Denn Arbeitsweisen verraten nicht nur viel über interne Abläufe im Intelligencebereich, sondern mit ihnen können Zugangsmöglichkeiten erkannt und somit die Effizienz der jeweiligen Organisation beurteilt werden. Hinzu kommt, dass ein derartiges Wissen auch politisch instrumentalisiert werden kann.

---

[136] Vgl. Pohrt, Wolfgang: Brothers in Crime; Critica Diabolis 68, Edition Tiamat, Berlin 2000, S. 25.

[137] Vgl. Online-Dokument: <http://www.taz.de/1/leben/internet/artikel/1/mi6-sucht-agenten-bei-facebook/?type=98>, abgerufen am 30.12.2008.

Besonders prekär werden in diesem Zusammenhang ausscheidende Mitarbeiter oder „geschwätzige“ Intelligenceangehörige betrachtet. Als Beispiel dafür dient der Anschlag in Mumbai (Indien) im November 2008. Laut Darstellung eines indischen Polizeioffiziers organisierte die pakistanische Extremistengruppe Lashkar-e-Taiba die Ausbildung der Terroristen. Aufhorchen lässt allerdings, dass ein früheres Mitglied der ehemaligen Armee die Ausbildung der Attentäter geleitet haben soll.[138] Sollten Hintermänner der Anschläge nicht aus dem Bereich des pakistanischen Geheimdienstes kommen, so ist dennoch eine generelle Verstrickung nicht auszuschließen. Was, wenn Angehörige mit dem Wissen über derartige Strukturen, Abläufe, Verfahren und Handlungsweisen aus dem Intelligencebereich die „Seite“ wechseln oder Teile ihres Wissens preisgeben? Wie brisant diese Problematik ist, ist auch im jüngsten Fall von Spionage in Estland erkennbar. Der Abteilungsleiter des estnischen Verteidigungsministeriums und Verschlusssachenbeauftragte Herman Simm wird verdächtigt, sensible NATO-Informationen jahrelang an einen russischen Auslandsgeheimdienst-Offizier (SWR) weitergegeben zu haben. Vertrauliche „Analysen der NATO zur Kosovo-Krise, dem Georgien-Krieg und zum Raketenabwehrprogramm“[139] sollen so in russische Hände gekommen sein. Dabei ist es unerheblich, ob finanzielle, ideologische oder racheähnliche Gründe ausschlaggebend sind. Interessant ist, wie man derartige Gefahren minimieren kann. Warum sollten insbesondere transnationale religiös motivierte Terrororganisationen derartige Infiltrationsversuche nicht planen und durchführen?

Guidelines – also Verhaltensweisen in bestimmten Situationen – finden sich bei unterschiedlichen westlichen Organisationsstrukturen und bei Terrororganisationen. Auch al-Qaida verwendete sie für die Ausbildung ihrer Attentäter im Bereich „for the use of public (trains, buses) and private (cars, motorcycles) transport“.[140] Trainiert wird ein unauffälliges Verhalten bei der Benützung von Verkehrsmitteln. Analoge Ausbildungsthemen betreffend „cultural awareness“– wenn auch in etwas an-

[138] Vgl. Attentäter von Mumbai in Pakistan ausgebildet. In: Neue Zürcher Zeitung, 2.12.2008, S. 2.
[139] Siehe Stark, Holger: Dicker Fisch. In: Der Spiegel, 74/2008, S. 144.
[140] Vgl. Gunaratna, Rohan: Inside Al Qaeda. New York 2003, S. 109.

derer Form – finden sich zunehmend bei staatlichen Sicherheitskräften vor Friedensmissionseinsätzen.

Dem in Pakistan festgenommenen Anführer der Lashkar e-Taiba Gruppierung, Zakiur Rehman Lakhvi, wurde nachgewiesen, dass er die Anschläge aus Pakistan mittels Mobil- und Satellitentelefonen leitete. Offensichtlich sind größere Anschläge kaum ohne modernste Technologien plan- und durchführbar. Dennoch zeigen die Anschläge von Nairobi und Dar es Salaam, dass Taktiken, wie sie zur Zeit des Kalten Krieges vorherrschten (Infiltration oder der Einsatz von Schläfern), noch durchaus effektiv sind.[141]

Es hat den Anschein, dass sich die internationale Presse eher mit Fehlschlägen der Nachrichtendienste als mit positiven Aktionen auseinander setzt. Erfolge von Nachrichtendiensten beziehen sich lediglich auf länger zurückliegende historische Ereignisse. Negative Pressemeldungen mit einem offensichtlich einhergehenden Misstrauensverlust seitens Intelligencebediensteten gegenüber staatlichen Institutionen haben[142] zweifelsohne direkte Auswirkungen auf Nachrichtendienste. Keine Informationen gibt es über mögliche Auswirkungen von medial negativer Berichterstattung über Nachrichtendienste auf die Motivation ihrer Bediensteten. Anders geartet ist die Lage bei Angehörigen von Terrororganisationen. Für sie sind „Erfolgskriterien“ ihrer Arbeit leicht zu erkennen – in Form ausgeführter Anschläge und deren medialer Präsenz.

Ziel von Anschlägen

Terrororganisationen wollen Angst und Schrecken verbreiten. Vor allem der gegenwärtig am Stärksten in Erscheinung tretende islamistische Terrorismus treibt die staatlichen Kosten für die Terrorismusbekämpfung in noch nie da gewesene Höhen. Der internationale Terrorismus versucht

[141] Vgl. ebd., S. 103.

[142] Seit den späten 1990er-Jahren schließen CIA-Mitarbeiter vermehrt Rechtsschutzversicherungen ab, weil sie befürchten, dass sie für gesetzte Handlungen im Rahmen eines staatlichen Auftrages vor Gericht kommen könnten. Vgl. hierzu Gentry, John A.: Intelligence Failure Reframed. In: Political Science Quarterly. Summer 2008, S. 259.

zudem, westliche Gesellschaftssysteme und deren Politik durch gezielte Anschläge ins Wanken zu bringen. Entscheidend für einen erfolgreichen Antiterrorkampf ist es, profunde Kenntnisse über den jeweiligen Gegner zu erlangen: Wann ist der Feind wo und wie verletzbar? Welche Gegenreaktionen sind zu erwarten? Terroristen solche und ähnliche Fragestellungen nicht zuzutrauen bedeutet, sie in gröbster Weise zu unterschätzen. Fragestellungen dieser Art bedingen aber auch die Notwendigkeit eines Nachrichtenwesens in Terrororganisationen.

Organisationsformen

Versucht man, intelligenceähnliche Strukturen des Feindes zu analysieren, stößt man unweigerlich auch auf Organisationsformen außerhalb „normaler“ staatlicher Nachrichtendienste, die sich ebenfalls mit Intelligence beschäftigen. Unklare Vorgänge rund um die deutsche Telekom im Jahre 2008 (für die eine kleine Recherchedienstfirma tätig war) geben einen Vorgeschmack auf zukünftige Problematiken. Daher könnten für Staaten Verstöße gegen die Bürgerrechte seitens „privater“ Organisationen aufgrund von Datenklau und Datenmissbrauch zu einer großen Herausforderung werden.

Im deutschen Sprachgebrauch hört man immer wieder, wenn man über Intelligence oder Nachrichtendienste spricht, die Bezeichnung „Geheimdienste“. In wissenschaftlichem Sinne ist die Bezeichnung Nachrichtendienste zutreffender, da diese Organisationen aufgrund gesetzlicher Bestimmungen existieren, agieren, einer gesetzlichen Aufsicht unterliegen und daher nicht „geheim“ sein können. Der Begriff „Geheimdienst“ trifft daher eher für Terrororganisationen zu, da diese weder legal existieren noch agieren.

Die zuletzt besonders durch die Anschläge von Mumbai im November 2008 in Verdacht geratene und 1989 gegründete Organisation Lashkar e-Taiba ist ein Beispiel für eine gut organisierte Gruppierung. Haifz Mohammed Saeed wurde unter dem Verdacht, Oberhaupt und ideologischer Direktor von Lashkar e-Taiba zu sein, festgenommen. Saeed behauptete jedoch, nur noch Anführer der Wohlfahrtsorganisation Jamaat-

du-Dawa – einem „charity wing of the militant group“[143] – zu sein. Saeed wurde bereits kurz nach seiner Verhaftung wieder freigelassen. Jamaat-du-Dawa ist eine in Pakistan anerkannte und beliebte Hilfsorganisation und unterstützt in Not geratene Menschen (z. B. beim Erdbeben 2005). Ein Vorgehen gegen diese Organisation durch Sicherheitskräfte würde bei der Bevölkerung auf völliges Unverständnis stoßen und ist daher politisch kaum möglich. Geheimdienstliche Planung ist aber für Anschläge in diesen Dimensionen eine Grundvoraussetzung, denn derartige Anschläge benötigen erhebliche finanzielle Mittel und Koordination, was nur durch straffe Organisationen zu bewerkstelligen ist.

Zarrar Shah, ein Kommandant von Lashkar-e-Taiba und „communication specialist“,[144] wird als ISI-Verbindungsmann verdächtigt. Intensive Aufklärungsarbeit seitens einer Terrororganisation zur Vorbereitung von Anschlägen ist ebenso notwendig wie logistische Hilfe. Die Abstützung auf größere Strukturen ist unerlässlich, ausgeklügelte Planung notwendig und nur unter größter Geheimhaltung oder Verschleierung zu bewerkstelligen.

Lashkar-e-Taiba wurde in der Vergangenheit immer wieder vorgeworfen, von al-Qaida finanziell unterstützt worden zu sein. Gegenwärtige Verbindungen zu al-Qaida sind allerdings kaum festzumachen. Der Einfluss von al-Qaida – zumindest in ideologischer Hinsicht – ist jedoch unverkennbar.

Geheimdienstliche Strukturen in Terrororganisationen

Als Grundstein für den organisatorischen Aufbau von al-Qaida kann das durch Osama bin Laden und Abdullah Jussuf Mustafa Azzam ins Leben gerufene „Dienstleistungsbüro“ in Peschawar, Pakistan angesehen wer-

[143] Vgl. Pakistan Arrests Suspects in Mumbai Attacks. In: The New York Times. Online-Dokument: <http://www.nytimes.com/2008/12/09/world/asia/09pstan.html?hp=&pagewanted=print>, abgerufen am 8.12.2008.

[144] Vgl. Pakistan’s Spies Aided Group Tied to Mumbai Siege. In: The New York Times. Online-Dokument: <http://www.nytimes.com/2008/12/08/world/asia/08terror.html?_r=1&hp>, abgerufen am 8.12.2008.

den. Dieses hatte bereits eine Organisationsstruktur militärischen Charakters mit jeweils einer Unterabteilung für Ausbildung, militärische Angelegenheiten, Gesundheit und Logistik.[145] Weltweite „Außenstellen" des „Dienstleistungsbüros" kamen hinzu. Diese, wie auch das im Oktober 1986 durch Osama bin Laden gegründete und als „Die Höhle der Gefährten" (Ausbildungslager von und für arabische Freiwillige) bezeichnete Ausbildungslager, waren letztendlich für die Ausbreitung des transnationalen Terrorismus von großer Bedeutung.

Rohan Gunaratna erkennt in den meisten Anschlägen von al-Qaida drei wesentliche Grundelemente:[146]

- Intelligence Teams,
- Unterstützungsteams,
- Attentäterteams.

Wie andere große Organisationen besitzt auch al-Qaida ein Verbindungsmittel in die „Außenwelt" – in Form ihrer Medienstelle „Al Shahab". Indiz dafür, wie intensiv diese Medien arbeiten, ist eine Meldung in der US-amerikanischen Tageszeitung „US Today": „The U.S. military says it has captured at least six al-Qaeda media centers in Iraq and arrested 20 suspected propaganda leaders since June."[147]

Terroranschläge von der Dimension des 11. September 2001 führen die Notwendigkeit einer dementsprechenden Organisationsstruktur besonders deutlich vor Augen. Der Aufbau und die Führung derartiger Organisationen sind nur unter Verwendung nachrichtendienstlicher Methoden denkbar.

Der ägyptische Filmemacher Issam Diras beschrieb in einem Buch seine in einem afghanischen Ausbildungslager (welches Osama bin Laden gegründet hatte) gemachten Erfahrungen. Darin beschrieb er auch den or-

---

[145] Vgl. Kepel, Gilles, Milelli, Jean-Pierre: Al-Qaida Texte des Terrors. München 2006, S. 159.
[146] Vgl. Gunaratna, Rohan: Inside Al Qaeda. New York 2003, S. 103.
[147] Vgl. US Today: Online-Dokument: <http://www.usatoday.com/news/world/iraq/2007-10-04-Mediacenter_N.htm>, abgerufen am 5.10.2007.

ganisatorischen Aufbau des damaligen Dienstleistungsbüros (der späteren al-Qaida) der späten 80er-Jahre. Nach Informationen von Diras bestand die Verwaltung aus einer Militärabteilung, einer Verwaltungsabteilung, der Ausbildungs- und der Abteilung für Abreisen.[148]

Dass Terrorgruppierungen durchaus nach Management-Grundsätzen agieren, zeigt sich bei Khalid Sheikh Muhammad, dem Leiter der operationellen Abteilung al-Qaidas.[149] Dieser war für die Umsetzung des Schlüsselprinzips des Agierens der Zielorientiertheit zuständig.[150] Für die Anschläge von 9/11 war auch eine Logistikabteilung eingesetzt. Leiter dieser Abteilung war Ramzi bin al-Shibhwar.[151]

Geheimdienstliche Beschaffungsmethoden von Terrororganisationen

Westliche Texte trotzen von „Lessons Learned" in der Terrorismusbekämpfung. Kleine, aber für den Erfolg terroristischer Anschläge folgenschwere Fehler in der Ausführung seitens der Attentäter werden aufgezeigt. Oder es wird sogar beschrieben, wie und mit welchen Mitteln erfolgreiche Anschläge durchzuführen wären. Ein Leitsatz lautet z. B.: „Gehe mit Vorsicht und List, ja Verschlagenheit ans Werk".[152] Das Internet vervielfacht die Möglichkeiten von Terroristen um ein Vielfaches. Anleitungen für einen Erfolg versprechenden Terroranschlag oder Guerillakrieg sind leicht zugänglich und kaum zu verhindern.

Die von Terrororganisationen angewandten Grundsätze bei der Technik der Nachrichtenbeschaffung sowie der Rekrutierung von zuverlässigen Gruppenmitgliedern ähneln frappierend im Westen erschienen „Fachbuch"-Inhalten. Bauanleitungen für behelfsmäßige Sprengsätze und de-

---

[148] Vgl. Kepel, Gilles, Milelli, Jean-Pierre: Al-Qaida Texte des Terrors. München 2006, S. 56.
[149] Gunaratna, Rohan: Inside Al Qaeda. New York 2003, S. XX.
[150] Ebd., S. XXV.
[151] Ebd., S. XXVI.
[152] Aufgrund der Problematik derartiger Texte verzichtet der Autor dieses Beitrages bewusst auf die Nennung dieser „Fachbücher" in den Fußnoten.

ren effizienter Einsatz (wo und wie anzubringen) sowie detaillierte Beschreibungen über Kampftaktiken vervollständigen diese „Lehrbücher".

Auch aktive Unterstützungsmaßnahmen durch Trainingsmethoden, Waffentransporte sowie Wissenstransfer an unterschiedliche Widerstandsgruppierungen seitens westlicher Nachrichtendienste verstärkten das Problem von „Lessons Learned". So unterstützte die CIA über den pakistanischen ISI die Mudschaheddin in Afghanistan mit Waffen. Der ISI bevorzugte dabei die radikalen islamischen Parteien für einen antisowjetischen Dschihad.[153]

Diese Beispiele zeigen, dass Geheimdienste – wenn auch mit ehrbarem Ziel – bei der Unterstützung von radikalen Gruppierungen beteiligt waren. Ausbildungshilfen, die in operativer und taktischer Hinsicht für derartige Gruppierungen geleistet wurden/werden, können sich letztendlich als kontraproduktiv herausstellen. Ist Wissen einmal in fremden Händen, ist es nicht mehr kontrollierbar.

Während Nachrichtendienste in Demokratien einer staatlichen Kontrolle unterliegen, können Terrororganisationen uneingeschränkt Intelligenceaktivitäten anwenden, was ihnen Vorteile verschafft.

Eine wesentliche Methode zur Beeinflussung von Meinungen und Verhalten ist Desinformation. Sie wird nicht nur in westlichen Ländern angewandt, sondern auch bei radikalen Organisationen. Im Juli 2008 berichtet die Science-Abteilung von ORF.at über die „École de Guerre Économique" (EGE). Das in Paris ansässige Institut lehrt seinen Absolventen geopolitische Strategien zur Markteroberung, Militärtechniken und Vernebelungstaktiken. Der Direktor der 300 Studenten umfassenden EGE, Christian Harbulot, ist davon überzeugt, dass man, um „Kriege zu verhindern, man die anderen vor allem dazu bringen muss, einen zu fürchten".[154]

---

[153] Vgl. Rashid, Ahmed: Heiliger Krieg am Hindukusch. München 2002, S. 258.
[154] Vgl. ORF Online. Online-Dokument: <http://science.orf.at/science/news/151925>, abgerufen am 24.10.2008.

Es verwundert daher nicht, dass Ayman al-Zawahiri, Nummer zwei von al-Qaida, schon sehr früh mit Desinformation arbeitete. Damals allerdings noch, um Osama bin Laden dem Einfluss seines Mentors Abdullah Azzam zu entziehen. Ziel war es, sich die finanzielle Unterstützung von Bin Laden zu sichern. Um dieses Ziel zu erreichen, versuchte al-Zawahiri, Azzam bei Bin Laden mittels Desinformation zu diskreditieren. Al-Zawahiri verbreitete das Gerücht, dass Azzam ein Spion der Amerikaner sei.[155]

Mit Information – ob es sich dabei um Desinformation handelt, sei dahingestellt – spielt auch die Hamas. Der in einem Interview als „Ali" bezeichnete Imam aus dem Westjordanland erklärt, dass auch die (jüdische) Mafia in der israelischen Armee Waffen an die Hamas verkaufe.[156] Imam Ali wirft einen dunklen Schatten auf Angehörige der israelischen Streitkräfte: „Es passiert öfter, dass sie ihre Waffen verloren haben. In Wahrheit verkaufen sie sie an die Hamas."[157] Sollte es sich bei dieser Information um eine Desinformation handeln, so wurde sie psychologisch professionell von einer religiös anerkannten Autorität über Medien lanciert. Dies müsste von langer Hand geplant worden sein. Einerseits mit dem Ziel, Unsicherheit in der Führungsebene gegenüber den Untergebenen zu schüren und andererseits, um die schlechte Moral der Streitkräfte in der Öffentlichkeit anzuprangern und so die Bevölkerung gegen die eigene Armee aufzubringen und um dadurch auch Sympathisanten zu gewinnen.

Unterstützungsmaßnahmen durch westliche Nachrichtendienste

Oftmals zitierte Verbindungen zwischen dem pakistanischen Nachrichtendienst (ISI) und radikalen Terrorgruppierungen lassen sich in letzter Konsequenz nur „am Leben erhalten", wenn sich beide Seiten nachrich-

[155] Vgl. Kepel, Gilles, Milelli, Jean-Pierre: Al-Qaida Texte des Terrors. München 2006, S. 280.
[156] Vgl. Ertl, Sarah: „Israel verkauft uns bis heute Waffen". In: Die Presse, 30.12.2008, S. 4.
[157] Vgl. a.a.O.

tendienstlicher Methoden bedienen. Denn offizielle Verbindungen sind politisch und diplomatisch nicht „tragfähig“. Existieren sie dennoch, so erfordert dies von staatlichen Nachrichtendiensten, dass sie unterstützten Gruppierungen zumindest Grundkenntnisse von nachrichtendienstlicher Arbeitsweise vermitteln. Nur so kann eine Kooperation der beiden Akteure vor der Weltöffentlichkeit möglichst geheimgehalten werden. Die Zusammenarbeit der Taliban mit westlichen Geheimdiensten gegen die russischen Invasoren dürfte in den 80er-Jahren auf diese Art lange im Verborgenen durchgeführt worden sein.

Private Intelligencesektoren

Anlässlich der Ereignisse der letzten ein bis zwei Jahre in verschiedenen Industriebereichen zeigt sich die Berechtigung der Frage: „Wer ist eigentlich der Feind?“. Insbesondere Abhöraffären, Datenspionage und für politische Zwecke missbrauchte Informationen sowie unrechtmäßige Datenerhebungen lassen eine Abgrenzung von Feind/Freund bei Bürgerrechten kaum noch zu. Firmen arbeiten in rechtlichen Grauzonen für ihre Auftraggeber. Eine immer weiter fortschreitende Technik erlaubt immer öfter zu immer günstigeren Konditionen eine Nachrichtenaufbringung. Die bereits angeführten Vorfälle bei der deutschen Telekom dienen als Beispiel.

Wirtschaftliche Felder bedienen sich immer öfter nachrichtendienstähnlicher Mittel, wie das Beispiel der Pariser EGE mit seinen Lehrinhalten zu Fehlinformationskampagnen, digitalem Datenklau und Cyber-Sabotage zeigt.[158] Der Direktor der EGE, Christian Harbulot, gibt zu bedenken, dass das Image eines Konkurrenten gegenwärtig schneller angegriffen, sein Aktienkurs leichter zum Straucheln gebracht und dadurch in den Köpfen der Menschen Zweifel gesät werden kann[159] – was es zu verhindern gilt. Als Beispiel wird die in China vertretene französische

[158] Vgl. ORF. Online-Dokument: <http://science.orf.at/science/news/151925>, abgerufen am 24.10.2008. EGE bietet Angriffs- und Verteidigungsmethoden für Wirtschaftsakteure im Globalisierungskontext an.
[159] Vgl. ORF. Online-Dokument: <http://science.orf.at/science/news/151925>, abgerufen am 24.10.2008.

Supermarktkette Carrefour genannt. Boykottaufrufe über Mobiltelefon- und Internetnachrichten nach Attacken auf die olympische Fackel in Paris wurden nicht – wie fälschlicherweise kolportiert – aus China, sondern durch die Konkurrenz in Frankreich gesteuert. Dies verweist wiederum auf die Problematik des Internets, mit dem Desinformation erleichtert wird. Besondere Bedeutung könnte dadurch die Desinformationstaktik erlangen, die zukünftig als eine neue Strategie für Terrororganisationen dienen könnte.

Damit ergibt sich – wenn möglicherweise auch nicht beabsichtigt –, dass sich Intelligenceverhalten in staatlichen und bei Terrororganisationen gegenseitig bedingt. Allerdings sind dabei nicht nur Aktivitäten von „legalen“ Nachrichtendiensten äußerst bedenklich, sondern auch Literatur- und Medienmeldungen. Aufgezeigte „Lessons Learned“ können für Terrororganisationen einen Fundus für deren Ausbildungseinheiten darstellen.

Wenn Nachrichtendienste – wie Experten und politische Mandatare zusehends betonen – immer wichtiger werden, dann finden in einigen Jahren Kriege, Auseinandersetzungen und internationales Krisenmanagement ohne Intelligence kein Auslangen mehr. Ob dies im Umkehrschluss eine Kriegsführung ohne Intelligence ausschließt, bleibt unbeantwortet.

Konkrete Ableitung im Transformationskontext

Welche konkreten Ableitungen ergeben sich nun auf der Grundlage der aktuellen Studie für moderne Nachrichtendienste in Bezug auf eine effektive Terrorismusbekämpfung?[160] Dabei können konkrete Ableitungen für das staatliche „Eigenintelligence" benannt werden, die durch die Resultate aus dem (terroristischen) „Fremdintelligence" ergänzt werden.

Ableitungen Eigenintelligence:

- Nachrichtendienste dürfen im Transformationskontext keine zu starre institutionelle, funktionelle und personelle Struktur aufweisen. Sie müssen sich den sicherheitspolitischen Gegebenheiten und möglichen zukünftigen Herausforderungen (potentielle Bedrohungen) anpassen können (hohe strukturelle Adaptionsfähigkeit).
- Transformation ist als ein zeitlich offener Prozess zu verstehen, d. h. es gibt keinen endgültigen Endstatus.
- Die Formulierung eines nationalen Aufklärungsauftrages kann mittels Sicherheitsdialog zwischen dem sozialen System Politik und Intelligence erfolgen. Je detaillierter die Bedarfsformulierung erfolgt, desto gezielter können Intelligenceorganisationen arbeiten. Durch die Bedarfsformulierung kann auch eine perspektivistische Intelligence-Policy ermöglicht werden.
- Im Beschaffungswesen sind die beiden großen Beschaffungsansätze TECHINT und HUMINT komplementär zu betrachten, um ein Maximum an nachrichtendienstlichen Erkenntnissen zu erreichen.
- Vor dem Hintergrund verfassungsrechtlicher Bestimmungen und der gesetzlichen Mandatierung von Intelligenceorganisationen stellt die Terrorismusbekämpfung „die Quadratur des Kreises" dar. Diese Problematik ist von Experten im Intelligencebereich

[160] Vgl. hierzu auch Netanyahu, Benjamin: Fighting Terrorism – How Democracies Can Defeat the International Terrorist Network. New York 2001 (Erstveröffentlichung 1995).

zwischen der Politik, den gesetzgebenden und gesetzsprechenden Institutionen zu kommunizieren. Eine qualifizierte und fachliche öffentliche Debatte wäre in diesem Zusammenhang anzudenken.

- Die Intelligenceanalyse könnte verstärkt auf dem Klassifikationsprinzip von „need to share“ basieren, um so den Stellenwert und Gebrauchswert im Politischen zu stärken.
- Als Träger von Wissen sind in erster Linie Analysten anzusehen, sie können internationale Kooperationen initiieren, gestalten und thematisch vertiefen.
- Regionale Analyseeinheiten könnten mittels eines interdisziplinären und holistischen Ansatzes verstärkt tätig werden.
- Akkurate Analyseprodukte verbessern den Stellenwert von Intelligence im politischen Entscheidungsfindungsprozess; daher sollte das Unmittelbarkeitsprinzip einen besonderen Stellenwert einnehmen.
- Innerhalb der Gesamtstruktur Intelligence wäre es sinnvoll, die Handlungsfreiheit sowie thematische Selbstverantwortung der Analyse zu fördern.
- Bekannte Indikatoren in der Terrorismusbekämpfung sollten auf ihre praktische Tauglichkeit hin geprüft werden. Ergänzungen und Anpassungen sind in diesem Zusammenhang wünschenswert.
- Private Intelligencedienstleistungen in der Terrorismusbekämpfung könnten dort angefordert werden, wo sie mit den verfassungsrechtlichen Bestimmungen und den gesetzlichen Grundlagen von Nachrichtendiensten nicht kollidieren.
- Eine Überprüfung von PIF-Analysen durch den Nachrichtendienst ist unumgänglich (Vermeidung der politischen Instrumentalisierung im Sinne gewinnorientierter Interessen).
- Ein sich veränderndes Bedrohungsbild bedingt proaktive Führungsqualitäten und eine perspektivistische Intelligence-Policy.
- OSINT kann im Kontext der Analysefähigkeit im Bereich der Terrorismusbekämpfung noch verstärken werden.
- OSINT kann informationstechnisch rasch erweitert werden und mittels intelligenter Auswerteverfahren dem Analysebereich wertvolle Inputs liefern.

- Ein Großteil der beschafften Informationen im Intelligencebereich entstammt dem OSINT-Bereich, allerdings erhöht sich dadurch der Druck zur Schaffung eines qualifizierten Selektionsprozesses.
- Sicherheitspolitische Herausforderungen verlangen nach netzwerkzentrierten und integrierten Beschaffungs- und Analyseansätzen.
- Die Interaktionsebene zwischen Politik und Intelligence ist für eine qualitative Politikberatung grundlegend, daher sollten alle Nachrichtendienste eine institutionalisierte Schnittstelle einführen.
- Traditionelle Interpretationsformen von Intelligence legen nahe, dass es sich um ein politisches Instrument handelt, das nicht nur analysiert, sondern auch Handlungsoptionen für den sicherheitspolitischen Bereich erarbeitet.
- Intelligence ist in den Grundvoraussetzungen politischer Arbeit durch die Politikberatung verankert.
- Nachrichtendienste sollten sich vor medialen Anfeindungen schützen und ihren positiven Wert für die Sicherheit eines Landes mittels ausgewogener politischer Bildungsmaßnahme verdeutlichen.
- Besonders wichtig für die erfolgreiche Bekämpfung von Terrorismus ist ein integrierter Beschaffungsansatz, der neben den technischen Möglichkeiten vor allem HUMINT-Ansätze heranzieht. HUMINT-Fähigkeiten sind besonders wertvoll im Kampf gegen den internationalen Terrorismus. Eine Ausweitung dieser Fähigkeiten – insbesondere im Rahmen internationaler Einsätze – könnte angestrebt werden. HUMINT ist für den Truppenschutz im Rahmen von internationalen Friedensmissionen von zentraler Bedeutung.
- Geheime Aktionen gegen Ziele im Ausland werden nur von bestimmten Ländern angewendet. Vielfach fürchten Regierungen negative Schlagzeilen und politische Irritationen. Für Großmächte sind verdeckte Operationen zur gezielten Bekämpfung von Terroristen ein legitimes Mittel. In welchem Umfang allerdings diese Methode eingesetzt wird, darüber kann nur spekuliert wer-

den. Verdeckte Operationen sind unter demokratiepolitischen und rechtsstaatlichen Gesichtspunkten als problematisch einzustufen. Der Rückgriff auf bzw. die Entscheidung für eine geheime Aktion, sollten daher immer einer sehr kritischen Kosten-Nutzen-Kalkulation im Politischen folgen. Für Mittel- und Kleinstaaten ist diese Option nicht empfehlenswert.

Im Kontext der oben genannten Ableitungen im Zuge der Transformation nachrichtendienstlicher Strukturen unter den Voraussetzungen moderner Staatlichkeit werden von Benjamin Netanyahu zehn Möglichkeiten für eine erfolgreiche Terrorismusbekämpfung genannt.[161] Sie können als konkrete Ableitungen verstanden werden und sollten daher an dieser Stelle nicht unerwähnt bleiben:

1) *Impose sanctions on suppliers of nuclear technology to terrorist states.*
2) *Impose diplomatic, economic, and military sanctions on the terrorist states themselves.*
3) *Neutralize terrorist enclaves.*
4) *Freeze financial assets in the West of terrorist regimes and organizations.*
5) *Share intelligence.*
6) *Revise legislation to enable greater surveillance and action against organisations inciting to violence, subject to periodic renewal.*
7) *Actively pursue terrorists.*
8) *Do not release jailed terrorists.*
9) *Train special forces to fight terrorism.*
10) *Educate the public.*

Diese Möglichkeiten unterliegen jedoch individuellen nationalstaatlichen Voraussetzungen. Ihr tatsächlicher Mehrwert ergibt sich aus der jeweiligen rechtlichen und gesellschaftspolitischen Verfassung eines

[161] Vgl. Netanyahu, Benjamin: Fighting Terrorism – How Democracies Can Defeat the International Terrorist Network. New York 2001, S. 129-148.

Landes. Eine Implementierung dieser Optionen bedarf in erster Linie des politischen Konsenses, um wirksam werden zu können.

Ableitungen Fremdintelligence:

- Terrorgruppierungen benutzen eindeutig nachrichtendienstähnliche Verfahren und Elemente.
- Je größer Terrororganisationen sind, desto eher benötigt die Organisation einen „Intelligence-Anteil".
- Kompliziert auszuführende Anschläge setzen nicht nur äußerste Geheimhaltung, sondern zusätzlich langwierige und somit kostenintensive nachrichtendienstliche Vorarbeit voraus.
- Geheimhaltung bedeutet, verlässliche „Mitarbeiter" innerhalb der Gruppierung zu haben. Dies hat Rückwirkungen auf die genaue Auswahl von Mitgliedern aus den Reihen ihrer Sympathisanten. Loyalität steht an oberster Stelle jedes Nachrichtendienstes.
- Indoktrination besitzt im Zeitalter der weltweiten Kommunikation insbesondere bei radikalen Organisationen oberste Priorität. Ein Einschleusen von Agenten in Terrororganisationen ist somit kaum möglich und äußerst zeitintensiv.
- Ein finanzielles Erstarken von Terrororganisationen muss mit allen Mitteln unterbunden werden.
- Eine Zusammenarbeit zwischen einzelnen Intelligenceorganisationen stellt die Basis für den Antiterrorkampf dar. Westliche Nachrichtendienste sind ein zentraler Bestandteil im Kampf gegen den internationalen Terrorismus.
- Vor Beginn von Unterstützungsmaßnahmen für politische Oppositionsgruppierungen sollten deren mittel- als auch langfristige – möglicherweise ebenso globale – Auswirkungen in einer internationalen Zusammenarbeit analysiert werden.
- Mit einer Verbreitung über Medien von „Lessons Learned" in der Terrorbekämpfung sollte restriktiv umgegangen werden.
- Je heroischer sich eine Organisation gibt, desto attraktiver ist sie für Sympathisanten. Das bedeutet, dass in der Terrorismusbekämpfung eine „Entheroisierung" terroristischer Gruppierungen anzustreben ist. Inhumane Behandlungsweisen von Terrororgani-

sationen bei ihren „Auswahlverfahren“ gegenüber Bewerbern könnte z. B. publik gemacht werden. Aufklärungsarbeit an Schulen und Universitäten kann hierbei einen wichtigen Beitrag zur Terrorismusbekämpfung leisten.

- Nachrichtendienste müssen sich auch im Sinne der Terrorismusbekämpfung vor Infiltration schützen.
- Medien stehen vor dem Dilemma zwischen Info-Pflicht und verantwortungsvollem Umgang in Bezug auf die Preisgabe von Intelligence. Je mehr interne Abläufe preisgegeben werden, desto größer sind die „Lessons Learned“ bei den Terrororganisationen. Medien würden in diesem Fall Wissensmultiplikator für den Terrorismus sein.
- Erfolge von Intelligence in der Terrorismusbekämpfung müssen bekannt gemacht werden. Zum Erfolg führende nachrichtendienstliche Methoden sind dabei auszuklammern.
- Terrororganisationen und ihre Möglichkeiten sind nicht zu unterschätzen. Jedoch führt eine ständige mediale Überreizung zu einer Abstumpfung bei der Bevölkerung. Warnungen werden schließlich nicht mehr ernst genommen.
- Desinformationen durch Institutionen sind langfristig kontraproduktiv. Bei Entlarvung derartig bewusst gestreuter Desinformation wird den jeweiligen Institutionen kein Glauben mehr geschenkt.
- Datensicherheit wird zunehmend bedeutsamer, auch bei privaten Organisationen – wie zuletzt bei deutschen Firmen und Institutionen aufgedeckte Vorfälle beweisen. Generelle Kontrollen sind bei Vergehen gegen gesetzliche Bestimmungen des Datenschutzes zwar problematisch, müssen aber überprüft und geahndet werden.

Konklusion

Moderne westliche Demokratien haben beständige und gefestigte Institutionen herausgebildet, die auch in Zeiten der Krise das Funktionieren des Staates sicherstellen. Aufgrund ihres Grundauftrages lassen sich gewachsene institutionelle Strukturen oft nur langfristig verändern, was jedoch nicht notwendigerweise als negative Eigenschaft zu beurteilen ist. Nur so lassen sich tagespolitische Irrtümer und fehlgeleitete gesellschaftspolitische Trends abfedern. Nachrichtendienste stellen in diesem Zusammenhang eine punktuelle Ausnahme dar, weil sie im direkten Kontakt mit dem Gegner gefordert sind. Sie unterliegen daher einem besonderen Konkurrenzverhältnis, das den strukturellen Adaptionsbedarf besonders hervorhebt. Dieser Adaptionsbedarf ergibt sich nicht nur aus den vieldimensionalen Zusammenhängen in Bezug auf islamistische Gewaltaktivitäten gegen westliche Demokratien, sondern auch auf ideologischer Ebene, die als zentraler Motivationsfaktor angesehen wird. Um die ideologischen Implikationen islamistischer Gewaltgruppierungen verstehen zu können, bedarf es hier eines spezifischen Vorwissens. Nur eine qualifizierte Analyse auf der Grundlage wissenschaftlicher Erkenntnisse „entzaubert“ den weltweiten Dschihadismus.

Ein wenig erforschtes Gebiet im Intelligencebereich ist der wissenschaftliche Austauschprozess zwischen Nachrichtendiensten auf der einen Seite und Think Tanks, Forschungsinstitutionen sowie Universitäten auf der anderen Seite. Eine enge Kooperation zwischen beiden Akteuren ist als Zusatzmaßnahme geeignet, um potentielle Sicherheitsrisiken eingrenzen zu können. Es sind Intellektuelle, Wissenschafter und Kommentatoren, die über alternative Wissenszugänge verfügen, auf die auch die nachrichtendienstliche Analyseebene bereits verstärkt zugreift. Die Umsetzung dieses Adaptionsaspektes bedarf jedoch einer Institutionalisierung, um tragfähig zu werden. Fred Schreier, ein Schweizer Experte des Intelligencewesens, schlägt in diesem Kontext forschungstechnische Kooperationen zwischen offenen und geschlossenen Wissenseinrichtungen vor. Ob westliche Demokratien entsprechende offene Forschungsinstitutionen dem Intelligencesektor beistellen, ist eine Frage des politischen Willens und der Ressourcen. Schreier, Treverton, Steele u. a. favorisieren in

der Intelligenceanalyse eine verstärkte Einbindung von wissenschaftlichem Personal, das über eine human- und sozialwissenschaftliche Ausbildung verfügt. Dadurch könnten festgefahrene, strukturbedingte Denkweisen überwunden werden, die zu monokausalen Ableitungen in Bezug auf den islamistischen Feind führen.

Eine wirksame umfassende Sicherheitskonzeption setzt in vielen Fällen eine Vernetzung wissensbasierter Einrichtungen in einer Demokratie voraus, um alle Aspekte der politischen, ideologischen und religiösen Handlungsebenen von Staatsfeinden rasch aufklären zu können. Dadurch können bspw. islamistische Gewaltgruppierungen oder Proponenten der Radikalisierung klassifiziert sowie ihre tatsächliche Relevanz für die nationale Sicherheit bestimmt werden. Diese Vorgehensweise kann die weiterführende Analyse und die Herausarbeitung sicherheitspolitischer Gegenmaßnahmen vereinfachen.

Diese sozialwissenschaftliche Kernkompetenz nachrichtendienstlicher Analysearbeit ist aber auch noch aus einem anderen Grund wünschenswert. Wie wir in der vorliegenden Kurzstudie gesehen haben, besteht eine Kommunikationsbarriere zwischen der Politik und dem Intelligencebereich. Diese Kommunikationsbarriere beruht auf einem personen- und institutionsbezogenen Sozialisationsmuster. Diese Wissens- und Informationsvermittlung an die Politik ist jedoch die Grundlage, um intelligencebasierte Maßnahmen gegen islamistische Terrorgruppierungen demokratiepolitisch sowie rechtsstaatlich aufeinander abzustimmen. Dieser legitimatorische Aspekt verschärft aber auch das „Konkurrenzverhältnis“ zwischen den intelligencerelevanten Parallelitäten, die zwischen staatlichen Intelligenceorganisationen und Terrororganisationen bestehen (z.B. Problematik des raschen Handelns).

Der Feind studiert und lernt von modernen Demokratien die Möglichkeiten und Methoden der Terrorismusbekämpfung reziprok anzuwenden („Counter-Counter-Terrorism“). Terrororganisationen betreiben nicht nur systematische Aufklärung und auch Gegenaufklärung, sondern modifizieren ihre taktischen Vorgehensweisen gegenüber den Methoden staatlicher Nachrichtendienste. Das Verhalten subversiv agierender Terrorgruppierungen verdeutlicht die Verwertung von wissenschaftlichen

Erkenntnissen und Erfahrungswerten aus der Terrorismusforschung. Daraus geht hervor, dass Terrorgruppierungen unabhängig von ihrer Größe OSINT als Teil ihrer Struktur bzw. Planungsarbeit verwenden. Medien spielen mit ihrer Berichterstattung, bei der oftmals Details an die Öffentlichkeit und damit auch in die Hände von Terroristen gelangen, eine wichtige Rolle. Erschwerend ist, dass in den vergangenen Jahren Terrorgruppierungen zu einer durchaus effektiven Kleinstgruppen-Operationstaktik übergegangen sind, die von den Intelligenceorganisationen eingehend studiert wird.

Terrororganisationen gehen systematisch und pragmatisch vor, d. h. Auswahl eines lohnenden Zieles, anschließende Aufklärung und Auswertung des potentiellen Anschlagszieles. Erst danach erfolgt die Erstellung eines detaillierten Planes der Durchführung. Auf feindliche Strategiewechsel wird äußerst flexibel reagiert. Nicht nur staatliche Einrichtungen verwenden sogenannte Richtlinien und Handbücher, in denen Taktik, Methoden und Arbeitsabläufe vereinheitlicht sind, sondern auch Terrororganisationen. Teilweise übernehmen diese sogar Handbücher militärischer Einheiten für bestimmte Operationen, um diese entweder selber anzuwenden oder gezielte Gegenmaßnahmen durchzuführen. Diese subversiv-terroristische Anschlagsystematik des Feindes kann als „technische“ Ebene bezeichnet werden, während es daneben noch die „ideologische“ Ebene des Kampfes gegen den Westen gibt. Die Ideologiekomponente wird von den westlichen Nachrichtendiensten seit einiger Zeit vollinhaltlich erfasst. Vor allem die Ideologiekomponente radikal-islamistischer Terrororganisationen fungiert als vereinendes und systematisierendes Element. Sie ist die etablierte Kommunikationsbasis, die den bewaffneten Kampf gegen die „Ungläubigen“ nicht nur rechtfertigt, sondern auch als „Energiequelle“ für einen generationenübergreifenden Kampf nutzt. Die Ideologie radikal-islamistischer Kampfgefährten ist daher als die „Waffe“ zu bezeichnen. Sie soll mit aktuellen Maßnahmen gegen Radikalisierung, Rekrutierung und Terrorismus entschärft werden.

Moderne Staatlichkeit bedeutet in diesem sehr speziellen Bedrohungskontext die Fähigkeit zur umfassenden Sicherheitsgewährleistung für die eigenen Staatsbürger. Dabei wurde in den USA – aber auch in europäischen Demokratien – die Notwendigkeit der Adaption an die neuen si-

cherheitspolitischen Herausforderungen erkannt. In jenen Segmenten, in denen westliche Intelligenceorganisationen aufgrund gewachsener Tradition analytische Handlungsfreiheit begrenzen müssen, werden alternative institutionelle Ausweichmöglichkeiten gesucht, um die vieldimensionalen Bedrohungsinhalte qualitativ abdecken zu können. Insbesondere die Terrorismusbekämpfung setzt – wie bereits weiter oben erwähnt – eine interdisziplinäre Terrorismusforschung voraus. Daher werden in den Intelligenceorganisationen stets nach neuen Adaptionsoptionen gesucht, um eben alle Ebenen für eine effektive Terrorismusbekämpfung zu erfassen. Transformationsprozesse beinhalten in den europäischen Institutionen auch eine durchwegs selbstkritische Bestandsaufnahme der aktuellen Fähigkeiten, ohne die eine effektive Terrorismusbekämpfung kaum möglich wäre.

Ob die privaten Intelligencefirmen in diesem Adaptionsprozess die erforderlichen Innovationen mitbringen, bleibt abzuwarten. Erfahrungen der USA mit PIF in der Terrorismusbekämpfung müssten vor diesem Hintergrund separat evaluiert werden. Derartige Firmen sind zwar bereits als etablierte Einheiten im US-Intelligencewesen verankert, ihre tatsächliche Relevanz bleibt in letzter Konsequenz umstritten. Nicht zuletzt auch aufgrund ihrer immanenten wirtschaftlichen und gewinnorientierten Ausrichtung, die mit dem Staatlichkeitsgedanken im Sicherheitsbereich kollidiert.

Europäische Bestrebungen in Bezug auf die Terrorismusbekämpfung könnten vom Transformationsgedanken profitieren, wenn der Austausch von relevanten Informationen systematisiert werden würde. Allerdings sind hierfür einheitliche technische Standards für die Informationssicherheit unumgänglich. Im Kampf gegen den Terrorismus und vor dem Hintergrund seiner ideologischen Grundmotivation ist es für westliche Demokratien erforderlich, auf Veränderungen (strategischer, operativer wie auch taktischer Natur) sofort reagieren zu können. Der intelligencerelevante Informationsaustausch auf EU-Ebene ermöglicht ein rasches internationales Reagieren auf sicherheitsrelevante Veränderungen. Es geht dabei darum, Terroranschläge zu verhindern, aber auch darum, die eigenen kulturellen Identitäten vor Radikalisierung und Extremismus zu bewahren, weil damit demokratiepolitische Errungenschaften verbunden

sind, auf die in westlichen Demokratien nicht verzichtet werden kann. Gefestigte demokratische und rechtsstaatliche Prinzipien in Verbindung mit einer aufgeklärten Gesellschaft sind der beste Schutz vor Radikalisierung, Extremismus und Terrorismus. Österreich verfügt damit im Sinne von Machiavelli über ein „schützendes Dach“, das gestärkt werden sollte, um Sicherheit, Stabilität und Prosperität für die Zukunft garantieren zu können.

Anhang

Abkürzungen

AFCEA	Armed Forces Communications and Electronics Association
CIA	Central Intelligence Agency
CIA-NCS	CIA-National Clandestine Service
DCAF	Geneva Center for the Democratic Control of Armed Forces
DIA	Defense Intelligence Agency
DoD	Department of Defense
EADS	European Aeronautic Defence and Space Company
EU	Europäische Union
GAO	Government Accountability Office
GFC	Global Fusion Center
HUMINT	Human Intelligence
IC	Intelligence Community
IMINT	Imagery Intelligence
INSA	Intelligence and National Security Alliance
IO	Information Operations
IPOA	International Peace Operations Association
ISI	Inter-Services Intelligence
IKT	Informations- und Kommunikationstechnologie
IT	Information Technology
KGB	Komitet Gossudarstwennoy Besopasnosti (Komitee für Staatssicherheit)
MASINT	Measurement Intelligence
MAST	Maritime Asset Security and Training
NCTC	National Counterterrorism Center
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OSINT	Open Source Intelligence
PDB	President’s Daily Brief
PIF	Private Intelligencefirma

PMF	Private Militärfirmen
RADINT	Radar Intelligence
SAIC	Science Applications International Corporation
SIGINT	Signals Intelligence
SMO	Support for Military Operations
SOF	Special Operation Forces
TAC	The Analysis Corporation
TECHINT	Technical Intelligence (technische Aufklärung)
TIS	Total Intelligence Solution
UdSSR	Union der Sozialistischen Sowjetrepubliken
US-D	US-Dollar

Autoren

Dr. Wolfgang Braumandl-Dujardin ist wissenschaftlicher Mitarbeiter an der Landesverteidigungsakademie Wien des Bundesministeriums für Landesverteidigung und Sport (BMLVS). Zu seinen Forschungsfeldern gehören: Intelligence Studies, Terrorismusforschung, Comprehensive Approach und Privatisierung von Sicherheit. Er ist Co-Autor der Studie „Nachrichtendienstliche Kooperation der EU im Kampf gegen den Terrorismus“ (gemeinsam mit Christian Desbalmes, 2007), Mitherausgeber des Buches „Private Sicherheits- und Militärfirmen – Partner – Konkurrenten – Totengräber?“ (2008), Co-Autor der Informationsbroschüre *IFK aktuell* mit dem Titel „Private Militärfirmen – Geschäft mit dem Krieg“ (II/2008) sowie Mitarbeiter an zahlreichen internen Fachpublikationen. Vorträge zu den oben genannten Themenbereichen an unterschiedlichen Forschungsinstituten und Bildungseinrichtungen in Österreich und im Ausland. Absolvent von Kursen der NATO School in Oberammergau, Deutschland. Auslandseinsatz im Rahmen von KFOR 19.

Oberst Mag. Anton Dengg: Nach einem Auslandseinsatz bei UNDOF im Rahmen der Vereinten Nationen erfolgt die Aufnahme an der Theresianischen Militärakademie in Wiener Neustadt; Ausmusterung als Infanterieoffizier im Raum Wien; seit 1996 in verschiedenen Funktionen des BMLVS. 1999-2002 Studium der Politikwissenschaft in Verbindung mit Publizistik und Geschichte an der Universität Wien. Seit Sommer 2004 Leiter Referat Bedrohungs- und Konfliktbild am Institut für Friedenssicherung und Konfliktmanagement an der Landesverteidigungsakademie. Zu den Forschungsschwerpunkten gehören: Terrorismusforschung, Radikalisierung und Erforschung zukünftiger Konfliktbilder. Mitherausgeber (gemeinsam mit Walter Feichtinger): „Kein Feind in Sicht – Konfliktbilder und Bedrohungen der Zukunft.“ Wien 2010.

Abstract

Die vorliegende Kurzstudie verdeutlicht die Bedeutung von Intelligence im Bereich der internationalen Terrorismusbekämpfung. Die Arbeit gliedert sich in zwei Abschnitte: Im ersten Abschnitt werden Intelligencestrukturen in Bezug auf das staatliche Intelligencewesen analysiert, um strukturelle und institutionelle Stärken und Schwächen näher zu beleuchten. Die Autoren stellen die Frage, ob und in welchem Ausmaß strukturelle Adaptionen in den westlichen Intelligenceorganisationen erforderlich sind, um den internationalen Terrorismus noch besser bekämpfen zu können. Damit wird auf die zunehmende Komplexität der Bedrohungen und des Intelligencebereiches hingewiesen, und die Transformationsfelder benannt: Bedarfsformulierung, Beschaffung und Analyse. Zusätzliche Faktoren der modernen Informationstechnologien, wie beispielsweise Open Source Intelligence, bleiben nicht unerwähnt. Ein wesentlicher Mehrwert der Studie liegt in der Betrachtung von sogenannten privaten Intelligencefirmen, die bereits in den USA eine bedeutende Rolle in der Terrorismusbekämpfung spielen. Daher wird über ihren Nutzen aber auch über mögliche Risiken dieser Akteure vor dem Hintergrund demokratischer Standards referiert. Der zweite Abschnitt widmet sich den Terrorismusorganisationen und ihren inneren nachrichtendienstlichen Strukturen zur Anschlagsplanung. Dabei wird deutlich, dass auch terroristische Gruppierungen ähnlich wie staatliche Nachrichtendienste eine gezielt Beschaffung und Analyse durchführen. Die daraus gewonnen Erkenntnisse werden für die Anschlagsplanung verwendet. Die Studie schließt mit Ableitungen für einen erfolgreichen nachrichtendienstlichen Transformationsprozess. In der Schlussfolgerung wird auf der Grundlage der Analyse auch darauf hingewiesen, dass die Bekämpfung des internationalen Terrorismus mit demokratiepolitischen und rechtsstaatlichen Prinzipien vereinbar ist.