DATENSICHERHEIT IM SPANNUNGSFELD

Der Aufklärungsanspruch des Staates und das informationelle Selbstbestimmungsrecht des Bürgers

ANSGAR HEUSER || In der durch die „Enthüllungen" eines Edward Snowden ausgelösten „NSA-Abhöraffäre" versucht der Autor, der von 2009 bis 2012 für die Technische Aufklärung des Bundesnachrichtendienstes verantwortlich war, durch einige Anmerkungen aus der Sicht der Praxis nachrichtendienstlicher Arbeit zur Versachlichung der Debatte beizutragen, ohne dabei der Versuchung zur Verharmlosung der grundsätzlichen Problematik zu erliegen.

EINFÜHRUNG

Technische Aufklärung im Sinne der Informationsgewinnung aus der Überwachung elektronischer Kommunikation in jedweder Form, aber auch durch Eindringen in fremde Rechnersysteme ist ein tragender Pfeiler moderner nachrichtendienstlicher Arbeit, die ihrerseits der Versorgung der Bundesregierung mit nur so zu erlangenden Erkenntnissen auf politischen, militärischen, wirtschaftlichen und anderen Feldern dient. Sie stellt somit ein Element nationaler wie internationaler Sicherheit dar.

Angesichts der ständig wachsenden Masse der heute auf elektronischem Wege verbreiteten und verarbeiteten Informationen erklärt sich die Bedeutung der Technischen Aufklärung für einen Auslandsnachrichtendienst wie den Bundesnachrichtendienst von selbst. Ihren besonderen Stellenwert jedoch erlangt Technische Aufklärung aufgrund der Authentizität der so gewonnenen Informationen, die nicht durch Zwischenträger irgendwelcher Art verfälscht werden kann, aber auch aufgrund ihrer Fähigkeit, sich vergleichsweise rasch auf sich verändernde Aufklärungsforderungen einstellen zu können. Nicht gering zu achten ist dabei das gegenüber eher klassischen Formen nachrichtendienstlicher Tätigkeit in der Regel zu vernachlässigende Gefährdungsrisiko für die damit befassten Mitarbeiter.

Allerdings bedeuten die Erfassung von Kommunikation oder der (unbefugte!) Einblick in gespeicherte Daten von Personen, seien sie nun natürliche oder juristische, regelmäßig einen schwerwiegenden Eingriff in deren Rechte, heute schlagwortartig unter dem Begriff des „Rechtes auf informationelle Selbstbestimmung" gefasst. Dabei gewährt Art. 10 GG zunächst nur dem deutschen Staatsbürger (sowie allen sich auf deutschem Staatsgebiet befindlichen Personen) einen besonderen Schutz von Grundrechtsrang. In jedem Falle kollidiert jedoch Technische Aufklärung mit allgemeinen Persönlichkeitsrechten.

Diese inhärente Spannung ist nicht in Gänze auflösbar – es gilt vielmehr, sie bei der Erfüllung des nachrichtendienstlichen Auftrags durch Wahrung des vom Gesetzgeber vorgegebenen Rahmens sowie Beachtung des Gebotes der Verhältnismäßigkeit der eingesetzten Aufklärungsmittel auszuhalten.

Die nachfolgenden Ausführungen sollen nun einzelne Aspekte dieser Spannung illustrieren.

DIE SCHRANKEN DES AUFKLÄRUNGSANSPRUCHS

Da an anderer Stelle dieses Bandes auf die in der Bundesrepublik Deutschland geltenden rechtlichen Einschränkungen für die Technische Aufklärung näher eingegangen wird, beschränke ich mich hier auf einige ergänzende Anmerkungen.

Das „G10-Gesetz" sowie die einschlägige Rechtsprechung des Bundesverfassungsgerichtes setzen der Aufklärungstätigkeit des Bundesnachrichtendienstes auch im Vergleich zu ähnlichen Regelungen in anderen, parlamentarisch verfassten westlichen Demokratien recht enge Grenzen.

Auch die sogenannten „Metadaten", d. h. die technischen Umstände einer Kommunikation (Datum, Uhrzeit, Dauer, Kommunikationspartner u. ä.), unterliegen dem Schutz des Grundgesetzes, also keineswegs nur die Inhalte z. B. eines Telefonates oder einer Email. Nach meiner Kenntnis ist dies eine deutsche Besonderheit. Ferner existiert eine weitgehende Verpflichtung zur Unterrichtung eines Betroffenen (nach Abschluss einer sog. „Beschränkungsmaßnahme"), für die es ebenfalls anderswo kein Pendant gibt.

Festzuhalten ist jedoch: Die Problematik der deutschen G10-Regelungen liegt nicht darin, sie zu beklagen, vielmehr besteht die eigentliche Schwierigkeit in ihrer adäquaten Umsetzung, d. h. der Gestaltung technischer Lösungen, die den Rechtsrahmen wahren, ohne dabei durch untragbaren Aufwand die Erfüllung des Auftrages zu torpedieren. Diese Herausforderung stellt sich angesichts der rasanten Entwicklung von Kommunikations- und Informationstechnik ständig neu.

Soweit Technische Aufklärung den Versuch des Eindringens in Rechnersysteme (landläufig: „Hacking") bedeutet, sind die für den BND geltenden Dienstvorschriften recht eng. Da dies als ein besonders schwerwiegender Eingriff zu betrachten ist, bedarf jede einzelne solcher Maßnahmen der Genehmigung durch die Führungsebene, in Einzelfällen außerordentlicher politischer Brisanz sogar der des Bundeskanzleramtes. Im Sinne der Verhältnismäßigkeit des Mitteleinsatzes sind solche Aktivitäten (im Jargon: „Operationen") also Situationen vorbehalten, wo die eventuell zu gewinnenden Informationen dies auch rechtfertigen.

Ganz allgemein besteht das Problem, dass rechtliche Regelungen der technischen Entwicklung immer hinterherhinken, so dass unvermeidlich Interpretationsspielräume entstehen; einige „Pannen" der Vergangenheit finden so ihre Erklärung.

Ebenso wenig kann Datenverarbeitung eine 100%-Sicherheit gewährleisten. Diese Feststellung kann nur den überraschen, dessen Weltbild juristisch und nicht technisch geprägt ist.

MASSENHAFTE ÜBERWACHUNG ODER GEZIELTE SUCHE?

In der breiten Öffentlichkeit ist aufgrund der Snowden-„Enthüllungen" der Eindruck entstanden, als sei weltweit jedwede private Kommunikation, also jedes Telefonat, jede Email, jede SMS, jeder Mausklick auf Google oder jedes Gezwitscher auf Twitter der Überwachung durch finstere Mächte, vornehmlich des US-Aufklärungsdienstes National Security Agency (NSA), ausgesetzt.

Zwar kann ich nur aufgrund eigener Erfahrungen (die auch einen gewissen Einblick in die Absichten und Möglichkeiten von NSA, GCHQ und anderer einschließen) urteilen, es scheint mir jedoch festzustehen, dass diese Vorstellung, da jede technische Phantasie übersteigend, eine groteske Dämonisierung darstellt. Angesichts der ungeheuren Datenmengen, von denen hier die Rede ist, wäre eine solche flächendeckende Überwachung ein Ding der Unmöglichkeit. (Das Beispiel Telefonie mag dies erläutern: Bis heute erfordert eine Auswertung *gesprochener* Sprache aufgrund von Dialektfärbung, Jargon, Anspielungen, störenden Umweltgeräuschen usw. am Ende den menschlichen Übersetzer – nicht alle Zielpersonen bedienen sich schließlich des Englischen.)

Mehr noch, man unterstellt hier ein Aufklärungsinteresse, das in dieser Form schlichtweg nicht besteht. Vielmehr versuchen die genannten Dienste – wie im Übrigen alle westlichen Nachrichtendienste – im Auftrag ihrer Regierungen Informationen über die politischen Absichten bestimmter Staaten, ihr militärisches Potenzial oder ihre wirtschaftlichen Möglichkeiten zu gewinnen. Sie versuchen Einblicke zu

bekommen in terroristische Strukturen und solche der organisierten Kriminalität, in Ströme von Geldwäsche und Mechanismen der Proliferation von Massenvernichtungswaffen usw. Die private Kommunikation von Herrn Fritzchen und Frau Lieschen Müller ist hier ohne jeden Belang.

In der Tat handelt es sich hier um die sprichwörtliche Suche im Heuhaufen, allerdings findet man die Nadel nur, wenn man den Heuhaufen auch systematisch durchwühlt. Das heißt: Es ist zu unterscheiden zwischen einer gewissermaßen rein physikalischen Erfassung von Kommunikationskanälen durch einen Sensor, bei der tatsächlich zunächst alles durchläuft, und einer Überwachung im eigentlichen Sinne, die sich nach geeigneter Filtrierung auf das tatsächlich Gesuchte beschränkt, dieses aufzeichnet und einer eventuellen weiteren Bearbeitung zuführt. Die Güte der Filtrierung entscheidet dabei über den Erfolg von Technischer Aufklärung, und sie stellt heute die grundlegende Schwierigkeit in diesem Geschäft dar, nicht die Erfassung als solche.

An dieser Stelle kommt die Bedeutung von intelligenter Metadatenanalyse ins Spiel (zum Begriff der Metadaten vgl. den vorherigen Abschnitt): Die hoch aufwändige und anspruchsvolle Untersuchung nur der Metadaten allein erlaubt bereits die Erkennung von Kommunikationsstrukturen, von Gruppenbildungen und Hierarchien, einer etwaigen Abweichung vom Normverhalten als Indikation usw., bevor überhaupt eine inhaltliche Auswertung möglich und sinnvoll ist.

Hier will ich nicht ausschließen, dass durch die oben genannten Mächte, zumindest in bestimmten Weltregionen, eine flächendeckende Metadatenerfassung und -analyse erfolgt, auf deren Basis dann eine gezielte Suche im Sinne der oben genannten Aufklärungsaufträge, die dann auch auf Inhalte gerichtet ist, durchführbar erscheint.

Natürlich würde eine derartige, wahrhaft beeindruckende Fähigkeit Missbrauchsmöglichkeiten eröffnen, die Unbehagen bereiten. Hier setzt dann die Frage nach einer wirksamen politischen Kontrolle durch die jeweiligen Regierungen ein. Wem dies nicht genügt, der sei auf den letzten Abschnitt verwiesen.

INTERNATIONALE ZUSAMMENARBEIT – WILLFÄHRIGKEIT ODER NOTWENDIGKEIT

Gerade im Bereich der Technischen Aufklärung ist die internationale Zusammenarbeit ohne Alternative. Das liegt einmal in dem gigantischen Kommunikationsaufkommen begründet, das im Einzelfall nur noch arbeitsteilig bewältigt werden kann, sie eröffnet zum anderen große Chancen im Sinne der Kooperation auf technischem Gebiet im engeren Sinne, d. h. etwa durch Vermeidung teurer Mehrfachentwicklungen bei Hard- oder Software.

Ein hervorragendes Beispiel für überaus erfolgreiche Zusammenarbeit ist das gemeinsame Wirken der technischen Aufklärungsdienste der Staaten, die im Rahmen der Afghanistan-Mission dort Streitkräfte einsetzen, zum Schutz von Leib und Leben ihrer Soldaten. Hinsichtlich ihres Umfangs, aber auch mit Blick auf das Niveau des erlangten gegenseitigen Vertrauens ist diese Kooperation nach meinem Urteil historisch einmalig.

Gerade in Zeiten der „NSA-Affäre“ ist vielfach der Vorwurf erhoben worden, dass von deutscher Seite geradezu Bütteldienste für unzulässige Schnüffeleien durch fremde Dienste geleistet worden seien. Selbstverständlich ist die Zusammenarbeit von Nachrichtendiensten immer interessengesteuert und vom Prinzip des „do ut des“ (lat.: „ich gebe, damit du gibst“, die Red.) geleitet. Dennoch darf man den deutschen Diensten doch wohl so viel Professionalität zutrauen, dass sie in der Lage sind, die Vorteile einer Kooperation zu nutzen, ohne dabei gegen deutsche Staatsbürger oder Institutionen gerichteten Interessen Vorschub zu leisten.

Mehr als bedauerlich wäre es, wenn als Konsequenz dieser Affäre die großen Möglichkeiten, die internationale Zusammenarbeit bietet, künftig ungenutzt blieben. Erhöhte Wachsamkeit allerdings kann nicht schaden.

DAS PROBLEM DER VERSCHLÜSSELUNG

In zunehmendem Maße sieht sich die Technische Aufklärung mit kryptierten Nachrichten oder Daten konfrontiert (z.T. gilt dies im Einzelfall bereits für Teile von Metadaten). Dieses Thema verdiente eine eigene Erörterung. An dieser Stelle sei dazu nur so viel angemerkt: Trotz immer noch bemerkenswerter Erfolge stößt auf-

grund der Verbreitung leistungsfähiger Chiffrierverfahren die klassische Methode der Entzifferung an ihre Grenzen, die etwa die begrenzte Rechenkapazität trotz aller mathematischen Ingeniosität der Analytiker setzt.

Diese Entwicklung stellt nicht allein die Technische Aufklärung durch Nachrichtendienste vor ein Problem, sie lässt auch die Telekommunikationsüberwachung im Rahmen von Strafverfolgung ins Leere laufen, wenn diese trotz Vorliegens aller rechtlichen Voraussetzungen als Ergebnis lediglich ein unverständliches Chiffrat gewinnt. Hier wird also der Wille des Gesetzgebers durch den technischen Fortschritt schlicht ausgehebelt.

So berechtigt die Forderung nach mehr Informationssicherheit – und hier ist wirksame Verschlüsselung ein ganz wesentliches Element – auch im privaten Bereich (vgl. hierzu auch den letzten Abschnitt) ist, so sei dennoch an dieser Stelle auf jene hässliche Nebenwirkung hingewiesen. Trotz langwieriger Debatten im Bereich der Bundesverwaltung während der 1990er-Jahre besteht dieser im Grunde unauflösbare Widerspruch fort. Hier wird die Überschrift dieses Beitrages geradezu manifest.

POLITISCHE KONTROLLE ODER SCHLAGZEILEN?

Für die Technische Aufklärung gilt in noch stärkerem Maße als für nachrichtendienstliche Tätigkeit allgemein die Notwendigkeit striktester Geheimhaltung. Dies begründet sich nicht im Hang zu übertriebener Geheimniskrämerei der Beteiligten, sie ist vielmehr eine Voraussetzung ihres Erfolges. Denn jedes Bekanntwerden von Aufklärungsfähigkeiten sensibilisiert die Ziele eines solchen Aufklärungsansatzes, löst Gegenmaßnahmen aus und verschüttet somit die Informationsquelle.

Diese Forderung nach Geheimhaltung richtet sich nicht gegen die Instanzen von Legislative und Exekutive, denen in der Bundesrepublik Deutschland die Kontrolle über die Nachrichtendienste obliegt. In einem freiheitlich verfassten Staatswesen ist politische Aufsicht über die Nachrichtendienste eine unbestrittene Notwendigkeit. Eine Stärkung dieser Einrichtungen wäre unter Umständen dem Vertrauen der Öffentlichkeit in die Dienste sogar förderlich.

Entschieden bestreite ich jedoch ein legitimes Interesse des breiten Publikums an Unterrichtung über jedwede Operation von Nachrichtendiensten. Sensationslüsterne Berichterstattung in den Medien, häufig von rein kommerziellen Interessen geleitet, verunsichert lediglich den fachlich nicht vorbereiteten Leser, löst Profilierungsversuche dazu nicht Berufener aus und zerschlägt im Ergebnis mehr Porzellan, als an demokratischer Kultur gewonnen werden mag.

Hingegen ist gegen eine seriöse, sachlich fundierte und zwischen Geheimhaltungsnotwendigkeit und begründetem Informationsbedürfnis der Öffentlichkeit wohlabgewogene Darstellung, auch in den Medien, nichts einzuwenden. Hier kann ich mir durchaus mehr vorstellen, als seitens der Politik heute erfolgt.

WIDER DAS GROßE UNBEHAGEN: HANDELN STATT KLAGEN

Wen angesichts der zum Teil angedeuteten, zum Teil aber auch konkret benannten Möglichkeiten nachrichtendienstlicher Aufklärung das große Unbehagen beschleicht, dem mögen die nachstehenden Thesen einen Weg weisen:

- Klagen über nachrichtendienstliche Aktivitäten anderer sind nichts weiter als naiv,
- Forderungen nach Selbstbeschränkung („no-spy-Abkommen“ u. ä.) sind irgendwo zwischen Unwirksamkeit und Lächerlichkeit angesiedelt,
- das Gebot der Stunde ist vielmehr die Gewährleistung von Informationssicherheit durch Umsetzung geeigneter technischer Maßnahmen.

Als zu beackernde Felder sind hier zu benennen: die sensiblen Bereiche der öffentlichen Verwaltung, die spionagebedrohten Sektoren der deutschen Privatwirtschaft, die sabotagegefährdeten kritischen Infrastrukturen und, nur wo notwendig und sinnvoll, das private Umfeld. Angesichts immer knapper personeller und materieller Ressourcen sind diese hier zu konzentrieren, die Forderung nach allumfassender Informationssicherheit ist nicht erfüllbar.

Sichere Verschlüsselungsverfahren, verlässliche Authentisierungsmechanismen, aktuell gehaltener Virenschutz und Firewalls, vertrauenswürdige Hard- und Software, nicht zu vergessen

personelle Sicherheit, mögen für sich genommen das Problem nicht in Gänze lösen; in ihrer Summe kumulieren sie sich zu einer beträchtlichen Hürde für einen Angreifer, dessen Ressourcen natürlich auch stets begrenzt bleiben, wie ich aus eigener leidvoller Erfahrung berichten kann.

Wäre all dies geleistet, brauchte man sich über die befürchteten oder gar unterstellten Absichten anderer nicht mehr so viele Gedanken zu machen.

DR. ANSGAR HEUSER

Abteilungsleiter „Technische Aufklärung“
im BND a.D., Euskirchen