Gesprächskreis
Nachrichtendienste in Deutschland e. V.

Technische Aufklärung

Zur Bedeutung und Zukunftsfähigkeit einer zentralen nachrichtendienstlichen Befähigung

Hintergrundinformation

(19. April 2021)

Im Rahmen der staatlichen Sicherheitsgewährleistung nehmen die Wahrung der außen- und sicherheitspolitischen Interessen sowie die Identifizierung und Analyse gravierender internationaler Risiken und Bedrohungspotentiale eine hohe Bedeutung ein. Der Bundesnachrichtendienst als einziger Auslandsnachrichtendienst des Bundes steht hier in besonderer Weise in der Pflicht[1], zusammen mit den Diensten und Behörden aus den Geschäftsbereichen von BMI und BMVg in der Wahrnehmung ihrer jeweiligen zentralen Aufgaben der nationalen Sicherheitsgewährleistung in den Dimensionen des Cyber- und Informationsraumes.

Das Bundesverfassungsgericht hat das überragende öffentliche Interesse an einer wirksamen Auslandsaufklärung zur Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen sowie zur Früherkennung von Gefahrenlagen, die aus dem Ausland drohen, in unmissverständlicher Weise bekräftigt[2].

„Nach dem Willen des Gesetzgebers soll die strategische Überwachung Erkenntnisse über das Ausland verschaffen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Sie soll damit dazu beitragen, frühzeitig Gefahren zu erkennen, die Handlungsfähigkeit der Bundesregierung zu wahren und die Bundesregierung in außen- und sicherheitspolitischen Fragen mit Informationen zu versorgen. Hierin liegt ein legitimes Ziel[3]“.

---

[1] Vgl. grundsätzlich: Eine Agenda für den Bundesnachrichtendienst - Sicherheitsgewährleistung für Deutschland im europäischen und transatlantischen Verbund. Stellungnahme des GKND e.V. 22. März 2021

[2] Vgl. zusammenfassend: Kernaussagen des Bundesverfassungsgerichts zur Auslandsaufklärung des Bundesnachrichtendienstes. Hintergrundinformation des GKND e.V. vom 15. März 2021

[3] BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -Rn. 144 Satz 2 und 3

Das breite Aufgabenspektrum der technischen Aufklärung ist bereits im Zusammenhang mit der strategischen Ausland-Ausland-Fernmeldeaufklärung erläutert worden[4]. Im Folgenden wird nunmehr das Augenmerk auf die wichtigsten Elemente der Technischen Aufklärung (im Sinne der Erfassung und Auswertung elektronischer Information) zu richten sein. Betrachtet werden sollen bestehende Befähigungen, auch im internationalen Vergleich, und die Bedingungen wie Notwendigkeiten ihrer weiteren Entwicklung angesichts dynamischer globaler Entwicklungen in Wissenschaft und Technik und der damit einhergehenden neuen Dimensionen sicherheitlicher Herausforderungen und Bedrohungen.

Erfassungstechnik

Nach national wie international geteilter fachlicher Bewertung und hiesigen Erfahrungswerten befinden sich nationale Befähigungen in der Erfassung von Kommunikationsdaten mit den heutigen Schwerpunkten der Satelliten- und Kabelerfassung hinsichtlich der Qualität der erforderlichen Sensorik auf der Höhe der Zeit.

Das größere Problem gegenüber der reinen technischen Erfassung besteht hingegen stets in der Selektion ND-relevanter Information **in Echtzeit** aus ständig wachsenden Informationsmengen bei kontinuierlich anwachsenden Übertragungsraten, da eine auch nur temporäre vollständige Aufbewahrung („Pufferung“) aufgrund des hierzu benötigten Speichervolumens unmöglich wäre. Hier besteht für alle Dienste die Notwendigkeit einer stetigen Erhöhung der eingesetzten Rechenleistung[5].

Ferner müssen die eingesetzten logischen Selektionsmechanismen („Filter“) immer weiter verfeinert werden, um die Balance zwischen der unvermeidlichen Datenverdichtung und der erhofften Nachrichtengewinnung zu wahren. Ebenso stellt die adäquate technische Umsetzung einschränkender juristischer und politischer Vorgaben angesichts des permanenten Fortschritts in der Kommunikationstechnik die Methodik der Filtrierung vor ständig neue Herausforderungen.

In Deutschland wird sich diese Problematik in besonderem Maße mit der Neufassung des BND-Gesetzes zum 31.12.2021 zeigen.[6] Das Selektionsproblem steht überdies in engem Zusammenhang mit dem weiter unten zu beschreibenden neuen Paradigma einer „sensorübergreifenden Aufklärung“. Vor dem Hintergrund der zunehmenden rechtlichen Einschränkung internationaler Kooperationsmöglichkeiten wird es nun für den Bundesnachrichtendienst mehr denn je erforderlich sein, die bisherige Abhängigkeit in der Technischen Aufklärung von den Erfassungsergebnissen anderer Nachrichtendienste deutlich zu verringern. Dem kann nur durch Ausweitung der vorhandenen eigenen Kapazitäten entsprochen werden, dies vor allem auf dem Gebiet der Kabelerfassung, die gegenüber der Satellitenerfassung (dem heuti-

---

[4] Zielsetzung und Aufgaben der strategischen Ausland-Ausland-Fernmeldeaufklärung (FmA) im Lichte des BVerfG-Urteils vom 19. Mai 2020. Hintergrundinformation GKND (Oktober 2020)

[5] Zur Problematik im US-Kontext: National Research Council (ed.), Bulk Collection of Signals Intelligence: Technical Options. 2015 (https://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options)

[6] Vgl. zum aktuellen zusätzlichen Mittelansatz von insgesamt über 450 Millionen Euro: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts, 16.Dezember 2020, Kapitel VI, Gesetzesfolgen, Abschnitte 2 und 3 (S. 56-57) (https://www.bundesregierung.de/resource/blob/976020/1829370/3299c2a2c74446424413b4363d6fb035/2020-12-16-rege-ge-bnd-data.pdf?download=1)

gen „Brot-und-Butter-Geschäft“) immer größere Bedeutung erlangt. Hier sind umfangreiche Investitionen in die notwendige technische Ausstattung erforderlich, begleitet von angemessenem personellem Aufwuchs.

Metadatenanalyse

Bei der Aufklärung eines Kommunikationsnetzes ist angesichts der Fülle erfasster Daten und der inhärenten Schwierigkeit der maschinellen Inhaltsanalyse, insbesondere auch im Falle gesprochener Sprache, eine erfolgreiche Metadatenanalyse die Voraussetzung jeder ertragreichen Informationsgewinnung. Hierunter versteht man die Analyse erfasster Kommunikation hinsichtlich der dabei zusätzlich gewonnenen Signalisierungsinformationen, d.h. „wer mit wem?“, „wann?“, von welcher Dauer?“, „wie häufig?“ usf.; dabei bleiben die eigentlichen Inhalte der Kommunikation zunächst außer Betracht.

Eine Metadatenanalyse erlaubt die Erkennung von Strukturen innerhalb eines Netzwerkes (Untergruppen, Hierarchien, neu hinzutretende oder wieder wegfallende technische Teilnehmer usw.), die Beobachtung etwaiger Abweichungen vom Normverhalten technischer Teilnehmer im Sinne von Frühwarnung, und damit die Konzentration auf herausragende oder anderweitig auffällige Teilnehmergruppen, auf die dann bereits die Erfassung beschränkt werden kann und bei denen im Weiteren die – stets aufwändige – Inhaltsanalyse ansetzen kann.

Da Signalisierungsdaten im Gegensatz zu inhaltstragenden Daten weitgehend standardisiert und klar strukturiert sind, erlauben sie eine nahezu vollständige maschinelle Analyse, die den Einsatz der – immer knappen – personellen Ressourcen ganz ans Ende verschiebt. Auch ist der schiere Datenumfang ohne die Inhalte naturgemäß erheblich geringer, so dass Signalisierungsinformation zunächst gespeichert und erst dann einer eingehenden Analyse zugeführt werden kann. Selbst im Falle unangreifbar verschlüsselter Kommunikationsinhalte, mit denen künftig in verstärktem Maße zu rechnen sein wird, verspricht Metadatenanalyse im Sinne der oben genannten Strukturinformationen einen beachtlichen Erkenntnisgewinn. Sie zählt mithin zum Kernbereich einer zukunftsfähigen auftragsgerechten technischen Aufklärung.[7]

Die technische Umsetzung von Metadatenanalyse jedoch erfordert die Entwicklung und den Einsatz geeigneter hochspezialisierter Software bis hin zu KI-basierten Methodiken (wie etwa der Mustererkennung) sowie die Bereitstellung von bedienungsfreundlichen Mensch-Maschine-Schnittstellen, dies alles selbstverständlich auf der Basis hinreichend leistungsfähiger Hardware. Dieser Bereich erfordert ganz erhebliche Investitionen, die zudem mit der hochdynamischen Entwicklung von Informations- und Kommunikationstechnologie Schritt halten müssen. Die amerikanische NSA und das britische GCHQ nehmen hier seit Jahrzehnten eine Spitzenposition mit Milliardenprogrammen ein.[8] Angesichts der traditionellen Unterfinanzierung des Bundesnachrichtendienstes[9] besteht hier zwangsläufig erheblicher dringlicher, auf mittlere Sicht zu dimensionierender Nachholbedarf zur Herstellung der erforderli-

[7] Zur rechtlichen Perspektive vgl. §26 Abs. 1 BNDG-Entwurf; Kritisch Stellungnahme Stiftung Neue Verantwortung, S. 20-22 (https://www.stiftung-nv.de/sites/default/files/stellungnahme_refe_bndg_wetzling_vieth.pdf)
[8] Vgl. hierzu Stellungnahme des GKND „Eine Agenda für den BND“ (n. 1)
[9] Ebenda

chen eigenen Befähigung, die ihrerseits erst eine valide Grundlage für relevante Kooperation und Burden- Sharing mit Partnern bilden kann[10].

Der hierzu erforderliche Entwicklungsaufwand bewegt sich in hohem Maße auf IT-Neuland im Bereich des Softwareengineering. Daher führt hier kein Weg an umfangreichen Vergaben an wissenschaftliche Einrichtungen und die einschlägige Industrie vorbei.[11]

Analyse von Spracherfassung

Die wohl größte Herausforderung an Informationsgewinnung aus erfasster Kommunikation stellt die Analyse gesprochener Sprache dar: selbst die traditionelle Auswertung (der sprachkundige Mitarbeiter) ist ja mit den Problemen von Dialekt, Jargon, Abkürzungen usf. bis hin zu störenden Umgebungsgeräuschen oder gar bewusster Verschleierung konfrontiert.

Da andererseits der Umfang verfügbaren Personals, das diese Schwierigkeiten meistern kann, stets überaus begrenzt sein wird, erfordert Sprachauswertung künftig den Einsatz von Analysetools, die zumindest eine Vorauswahl derjenigen Kommunikation („Telefonate“) treffen können, die dann der weiteren Bearbeitung durch eine Person zuzuführen ist. Eine ganz ohne den menschlichen Bearbeiter auskommende, hinreichend fehlerfreie inhaltliche Auswertung ist nach heutiger Beurteilung wohl noch Zukunftsmusik; keine Kommunikationsform ist eben so wenig strukturiert wie gesprochene Sprache.

Neben zunächst erfolgter Metadatenanalyse bedeutet dies den Einsatz von Software, die in der Lage ist, gesprochene Texte auf vorweg festgelegte, jedoch anpassbare Muster hin abzusuchen. Angesichts der oben genannten Komplikationen sind hier nur lernfähige KI-Lösungen vorstellbar, die laufend von einem menschlichen Bearbeiter trainiert und überwacht werden. Auch hier unternimmt das britische GCHQ seit Jahren ganz erhebliche Anstrengungen[12],;von ungleich umfangreicheren Ansätzen ist bei den USA auszugehen. Entsprechende Zielsetzungen und Programme werden auch für den BND im Interesse seiner Zukunftsfähigkeit zwingend erforderlich sein. Mangelnde Befähigungen in diesem Bereich können unmittelbare Folgen für Leib und Leben des eingesetzten zivilen wie möglicherweise auch militärischen Personals haben, wie jahrelange Erfahrungen der Force Protection in Afghanistan bereits gezeigt haben.

Aufsetzend auf kommerzielle lernfähige Spracherkennungssysteme, die – zumindest rudimentär – heute bereits Derartiges leisten, sind somit in großem Stil national und in Kooperation mit Partnern Entwicklungen zu beauftragen, die den besonderen nachrichtendienstlichen Anforderungen Rechnung tragen.

---

[10] Die Befähigung zur internationalen Kooperation wird auch vom Bundesverfassungsgericht als essentiell angesehen (1 BvR 2835/17 -Rn. 160)

[11] Zur Praxis in USA und Großbritannien und ihrer technischen wie sicherheitlichen Problematik vgl. Crampton, Jeremy, Collect it all: National Security, Big Data and Governance, GeoJournal 2015 (https://www.researchgate.net/publication/265950222_Collect_it_all_National_Security_Big_Data_and_Governance)

[12] Britain's GCHQ cyber spies embrace the AI revolution, (https://www.reuters.com/article/uk-britain-security-ai-idUSKBN2AO2W8)

Mobile Erfassungssysteme

Nicht jede Erfassung elektronischer Kommunikation kann von einer festen Installation (Antennenstandort, Internetknoten u. ä,) aus erfolgen; dies gilt z.B. dann, wenn das Signal aus Gründen der Reichweite nur in einer bestimmten räumlichen Nähe zum Sender erfasst werden kann oder wenn kurzfristig, etwa in einer Krisensituation, eine Erfassung aufgebaut werden soll.

Solche Situationen können im Rahmen von Force Protection, aber keineswegs nur dann, eintreten; in diesen Fällen müssen kurzfristig verlegbare und/oder bewegliche Erfassungssysteme zur Verfügung stehen. Dabei kommen land-, see- oder luftgestützte Systeme in Betracht, wobei insbesondere im Falle landgestützter Systeme das Erfordernis ihrer getarnten, jedenfalls aber geschützten Installation bestehen kann.

Unter anderem im Rahmen von Auslandseinsätzen deutscher Streitkräfte haben derartige Befähigungen bereits eine Rolle spielen können.

Die Übernahme größerer internationaler Verantwortung wird hier allerdings in der Zukunft Aufklärungsanforderungen an den Bundesnachrichtendienst richten , die den vermehrten Einsatz solcher, im beschriebenen Sinne mobiler Erfassungssysteme notwendig machen, und dies nicht nur im Rahmen von Auslandseinsätzen der Bundeswehr, wo deren Logistik und Infrastruktur zur Verfügung stünde.

Ein diesbezüglicher, erneut zeitnah einzuleitender Aufwuchs eigenständiger Kapazitäten bei Material und Personal wird demnach gerade auch im Interesse einer angemessenen eigenen Reaktions- und Handlungsfähigkeit in Krisensituationen erforderlich sein, auch hinsichtlich der luft- oder seegestützten Trägerplattformen.

Penetration von Rechnersystemen

Technische Aufklärung bedeutet neben der Informationsbeschaffung aus elektronischer Kommunikation auch den Abzug von Informationen aus Rechnersystemen, d.h. mittels der Gewinnung gewissermaßen „ruhender“ Daten. Diese Methodik genießt den Vorzug eines fokussierten Ansatzes auf ein aufzuklärendes Ziel, in Abgrenzung zur klassischen Fernmeldeaufklärung, wo die Aufgabe eher in der Selektion relevanter Information aus einer Fülle von Daten besteht.

Auf diesem Feld der *Computer Network Operations* (CNO) macht es die rasche Entwicklung der Informationstechnik, und damit einhergehend auch die ständige Weiterentwicklung defensiver Maßnahmen wie Firewalls, Virensuchprogramme, Authentisierungsmechanismen, Verschlüsselung und dergleichen erforderlich, ständig neue Penetrationstechniken zu entwickeln und vor ihrem Einsatz in gesicherter Umgebung zu erproben.

Der Einsatz dieser Methodik wird aufgrund des immanenten Entdeckungsrisikos und des beträchtlichen Aufwandes (insbesondere bei der Gewährleistung der operativen Sicherheit) stets auf besonders ausgewählte Ziele beschränkt bleiben; dennoch besteht hier ein beträchtliches, weiter zu pflegendes und auszubauendes Potential. Nicht zuletzt bietet dieser Ansatz vor dem Hintergrund sich ausbreitender unüberwindbarer Kommunikationsverschlüsselung eine verbleibende Chance.

Dabei genügt es nicht, sich auf die Findigkeit der eigenen „Hacker“ zu verlassen; vielmehr muss angesichts des immer begrenzten Personalumfangs und der Fülle sich überdies laufend verändernder Systemsoftware mit einhergehender begrenzter Überlebensdauer von Schwachstellen erneut fremdes *Knowhow* zu hohen Kosten beschafft werden.

Es ist offenkundig, dass auf diesem Sektor US-amerikanische Dienste mit Blick auf die nahezu ausschließlich auf ihrem Staatsgebiet ansässigen einschlägigen Unternehmen über einen uneinholbaren Vorsprung verfügen. Gleichwohl zählen leistungsfähige nationale Befähigungen im Bereich der *Computer Network Operations* zum Kernbereich sowohl für die Wahrung der erforderlichen, letztlich überlebenswichtigen Cyber-Abwehrkapazitäten als auch für die Umsetzung strategisch bedeutsamer Aufklärungsinteressen. Erhebliche, breit angelegte und nachhaltige Anstrengungen zur Wahrung und Weiterentwicklung derartiger Fähigkeiten werden mithin, nach Maßgabe der rechtlichen Rahmenbedingungen, auch in diesem Feld zu unternehmen sein[13].

Sensorübergreifende Technische Aufklärung

Die herkömmliche technische Aufklärung ist in den meisten Diensten „sensororientiert“: das heißt, dass die aus einem Erfassungsansatz („Sensor“) gewonnenen Daten zunächst für sich genommen selektiert und aufbereitet werden, bevor sie dann einem menschlichen Auswerter zugeleitet werden, dem seinerseits auch weitere, das Aufklärungsziel betreffende Erkenntnisse zur Verfügung stehen.

Diese Vorgehensweise ist wohletabliert; sie wird jedoch bereits den heutigen Anforderungen, viel weniger jedoch denen der Zukunft, nicht mehr gerecht: die technische Entwicklung der vergangenen zwei Dekaden hat dazu geführt, dass sich ein Aufklärungsziel (eine Person oder Organisation) mehr oder weniger gleichzeitig einer ganzen Reihe technisch unterschiedlicher Kommunikationsmittel bedient, die von den verschiedensten Medien getragen sind, während der einzelne Sensor naturgemäß nur seinen Ausschnitt sieht.

Um jedoch zeitnah zu relevanten Erkenntnissen zu gelangen, müssen die Informationspartikel aus möglichst vielen, am besten allen, Sensoren auf maschinellem Wege zusammengeführt und zu einem momentanen Gesamtbild geformt werden, das erst dann einem menschlichen Beurteiler zugeführt wird. Auf diese Weise kann die Fülle für sich genommen irrelevanter Informationen in einen verwertbaren aussagefähigen Kontext gebracht oder auch als insignifikant verworfen werden.

Diese Vision zeichnet aktuell noch ein Idealbild, das allenfalls schrittweise mit einem ganz erheblichen technologischen Aufwand erreicht werden kann: Auch hier müssen erst einmal intelligente Softwaresysteme entwickelt und zum Einsatz gebracht werden, die in der Lage sind, Daten verschiedenartigster Struktur (von Sprach- bis zu Bilddateien) thematisch und zielorientiert zu vergleichen sowie einer groben Relevanzprüfung zu unterwerfen, die dann möglichst rasch in ein für einen menschlichen Auswerter verständliches und überschaubares Format überführt werden müssen. Die sachliche Herausforderung ist jedoch international unbestritten, wenngleich auch in ihrer Dimension unterschiedlich beurteilt[14]. Potente Nachrich-

[13] Das neue BND-Gesetz regelt in § 34 derartige Eingriffe.

[14] Integrationserfordernisse neuer Qualität und Quantität stellen bereits heute ein zentrales Element der technischen Entwicklung dar, vgl. z.B. All-Source Intelligence Collection & Analysis. Transforming raw data into ac-

tendienste nähern sich diesem neuen Paradigma der Technischen Aufklärung daher derzeit wohl höchstens in Ansätzen. In jedem Falle sind auch hier vorausschauend enorme Entwicklungsanstrengungen erforderlich, die zum weit überwiegenden Anteil in Fremdvergabe geleistet werden müssen.

Technikverfolgung und -prognose

Im Interesse elementarer Zukunftsfähigkeit im Cyber-Zeitalter muss dem dramatischen technischen Fortschritt durch adäquate eigene Entwicklungsanstrengungen begegnet werden. Diese gesamtgesellschaftliche und gesamtwirtschaftliche Forderung gilt mehr denn je auch für die Nachrichtendienste. Nur wer die Dimension der Cyber-Welt begreift und beherrscht, wird die Zukunft bestehen können.

Wenn auch in der Mehrzahl der Fälle Entwicklungen im Wege der Fremdvergabe umgesetzt werden müssen, muss der Bundesnachrichtendienst, zusammen mit anderen kompetenten Stellen des Bundes[15], fachlich und personell in der Lage sein, die Tendenzen im Fortgang der Kommunikations- und Informationstechnik genauestens zu verfolgen und ihre Entwicklung perspektivisch im Blick zu behalten, um das *Knowhow* des Dienstes auf diesem Felde zukunftsfähig zu halten. Dies gilt auch für die Beobachtung der Standardisierung auf diesem Gebiet. Davon abgesehen bedürfen auch die angesprochenen anspruchsvollen und aufwändigen Projektvergaben an Dritte einer inhaltlich kompetenten Konzipierung, Ausplanung, Begleitung, Erfolgskontrolle und Einführung in den Regelbetrieb.

Eine Organisationseinheit „Zukunft der Technischen Aufklärung“ ist an dieser Stelle erforderlich, die – befreit von den Zwängen des Tagesgeschäfts – dieser Aufgabe in Form von Kontakten zu Industrie und Forschung, eigenen und vergebenen Studien, Informationsaustausch mit den Nachrichtendiensten Verbündeter, aber auch durch Mitwirkung in Standardisierungsgremien, nachgehen kann.

---

tionable intelligence (https://www.sosi.com/services/intelligence/all-source-intelligence-collection-analysis/); Ebenso die seit 2005 in Entwicklung befindliche Dimension von Geospatial Intelligence (GEOINT) (einführend: https://www.omnisci.com/technical-glossary/geoint), grundsätzlich auch: Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community, 2019 (https://www.researchgate.net/ publication/ 340647256 Intelligence Sources in the Process of Collection of Information by the US Intelligence Community)

[15] Unter anderem: Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), BMVg Abteilung CIT, Organisationsbereich Cyber und Informationsraum (CIR) der Bundeswehr, Bundesamt für Sicherheit in der Informationstechnik (BSI), BfV – Bereich Cyberabwehr, Bundesministerium für Forschung und Technologie (BMFT).