

human *FORWARD*

INTELLIGENCE

What Europe Needs To Know

Illustration itbusca/stock





Dr. Rebekka Reinhard,
Chefredakteurin

Editorial

Liebe Leserin, lieber Leser,

Europa befindet sich im Umbruch. 2026 ist das Jahr, in dem die Regierungen unseres Kontinents die Hoffnung auf eine baldige Entspannung der transatlantischen Beziehungen verabschiedeten – zugunsten größerer strategischer Autonomie und Souveränität. Dabei geht es nicht nur um KI-getriebene digitale, sondern auch um militärische, wirtschaftliche und gesellschaftliche Resilienz. Eine der wichtigsten Voraussetzungen ist der Zugang zu verlässlichen Informationen. „Unsere freiheitlich-demokratische Grundordnung schützen wir gegen ihre Feinde im Inneren und Äußeren“, so Bundeskanzler Friedrich Merz bei der Münchner Sicherheitskonferenz, und weiter: „Unter anderem werden wir unsere Nachrichtendienste stärken.“

Wir glauben: Europa steht im Übergang zu einer Ära, die nur durch eine präzedenzlose, über den Geheimdienst-Kontext hinausgehende „Intelligence“-Kultur verstanden werden kann. Die originalen, teils exklusiven internationalen Beiträge und -Interviews dieser digitalen Sonderedition lassen „Intelligence“ daher erstmals ganzheitlich als dringliche gesellschaftliche, politische, wirtschaftliche und technologische Zukunftsaufgabe Europas begreifen. Das Whitepaper **Intelligence: What Europe Needs to Know** verbindet Bereiche, die bisher in Forschung, Politik und Praxis strikt getrennt diskutiert wurden – und schafft damit einen neuartigen Referenzrahmen mit hoher Praxisrelevanz für das 21. Jahrhundert. Unser Ziel ist es, einen humanistischen Zugang zur strategischen Aufklärung zu leisten. Denn „Intelligence“ darf nicht nur als Instrument nationaler Sicherheit oder wirtschaftlicher Risikominimierung gelten. Wir müssen sie als Infrastruktur für eine freie demokratische Gesellschaft sehen.

Ob es um Cybersicherheit oder OSINT, Datenschutz oder dringend nötige Public-Private-Partnerships geht – überall ist eine tragfähige Balance zwischen Sicherheitsinteressen, Transparenz, Grundrechten und kollektiver Selbstaufklärung entscheidend. Wir danken unseren Top-Contributors aus Deutschland, Großbritannien, Italien, Belgien, der Schweiz sowie den USA für Ihre Insights und Learnings!

Übrigens: Die **Mona Lisa** auf dem Cover ist eine Fälschung – ebenso wie die auf den Innenseiten dieser Publikation. Hätten Sie das erkannt? Was wir unter den Bedingungen von Unsicherheit mehr denn brauchen, sind gründliche Quellenkritik und sorgfältige Rekonstruktion von Kontext. Das gilt für Beispiele aus der Kunstgeschichte so wie für politische und soziale, wirtschaftliche und technologische Sachverhalte.

München, März 2026.

Let's rethink intelligence. Let's reclaim humanity – and move human forward.

Schreiben Sie uns – wir freuen uns auf Ihr Feedback!

Herzlichst Ihre

rebekka.reinhard@human-magazin.de

thomas.vasek@human-magazin.de

human-magazin.de

human Magazin, Dr. Rebekka Reinhard, Thomas Vašek

human_magazin, rebekkareinhard

Inhalt

Editorial.....	2
----------------	---

01_Intelligence Matters

Wissen ist Macht.....	5
-----------------------	---

Thomas Vašek_ What Europe Needs to Know	6
--	---

Niccolo Petrelli (*Universität Roma Tre, Italien*)_

Hybrider Krieg	13
-----------------------------	----

Wolfgang Krieger (*Universität Marburg*)_

Neue Weltordnung	17
-------------------------------	----

Interview: Loch K. Johnson (*Universität Georgia, USA*)_

Internationale Zusammenarbeit	22
--	----

Christoph Meyer und Daniel Rainer Neumann (*King's College, UK*)_ **Reform der Nachrichtendienste**.....

Interview: Klaus Schmidt (<i>Oberst a. D., BND</i>)_	28
--	----

Bundesnachrichtendienst	32
--------------------------------------	----

Beatrice Heuser (*Brussels School of Governance, VUB, Belgien*)_ **Offene Gesellschaften**.....

02_Insight

Vorsprung durch Erkenntnis.....	46
---------------------------------	----

Interview: Jennifer E. Sims (*Stuart Street Atelier, USA*)_

Decision Advantage	47
---------------------------------	----

Interview: Alana Gramm (*IBM iX*)_ **OSINT**.....

Simon Wunder (*Volkswagen AG*)_

Geopolitical Risk Intelligence	59
---	----

Interview: Daniela Richterova (*King's College, UK*)_

Sabotage	62
-----------------------	----

Interview: Christopher Radler-Moric (*Berater*)_

Corporate Security	67
---------------------------------	----

Interview: Ole Donner (*Berater, Strukturierte Analyse*

<i>Deutschland</i>)_ Strukturierte Analyse	71
--	----

03_Technology

Fähigkeiten statt Abhängigkeiten.....	74
---------------------------------------	----

Interview: Marcus Willett (*IISS, Ex-GCHQ, UK*)_

Cyber Operations	75
-------------------------------	----

Armin Müller (*Central Europe Veeam Software*)_

Advertorial KI-Sicherheit	83
--	----

Timo Blenk und Christina Schäfer (*Agora Strategy*)_

Weltraum	84
-----------------------	----

Jeff Watkins (*Founder North Star Alliance, UK*)_

KI Persuasion	89
----------------------------	----

Interview: Frank Sauer (*Metis Institut für Strategie*

<i>und Vorausschau</i>)_ KI & Krieg	96
---	----

Richard Weiss (*Berater, u. a. NATO Centre of Excellence COE*) und Marc Mahlke (*Cybersecurity*

<i>Experte</i>)_ Cyber Threat Intelligence	100
--	-----

Interview: Krista Marija Läbe (*Quantum Systems*)_

Luftaufklärung	104
-----------------------------	-----

Interview: Julian Werner (*Center for Intelligence and Security Studies, Universität der Bundeswehr*

<i>München</i>)_ Urban Warfare	108
--	-----

Aviva Guttman (*Universität Aberystwyth, UK*)_

Signals Intelligence	111
-----------------------------------	-----

Interview: Ralf Schneider und Lars König

(<i>NetWatch</i>)_ Advertorial: Threat Intelligence	114 >
--	-------

04_Governance

Macht kontrollieren, Vertrauen schaffen.....	119
--	-----

Interview: Konstantin von Notz (<i>Deutscher Bundestag</i>)_	
Parlamentarisches Kontrollgremium	120
Interview: Luca Manns (<i>Universität Köln</i>)_	
BND-Reform	126
Interview: Jan-Hendrik Dietrich (<i>Hochschule des Bundes, Berlin</i>)_	
Wehrhafte Demokratie	129
Eva Herschinger (<i>Universität der Bundeswehr, München</i>)_	
Proteste	133
Interview: Anna Daun (<i>Hochschule für Wirtschaft und Recht, Berlin</i>)_	
Intelligence Culture	137
Interview: Holger Janusch (<i>Hochschule des Bundes, Berlin</i>)_	
Strategic Intelligence	141
Interview: Esther Omlin (<i>Ostschweizer Fachhochschule OST, CH</i>)_	
Europäische Kooperation	145

05_Ecosystem

Europas Kräfte bündeln.....	148
-----------------------------	-----

Brendan Kotze (<i>Performanta, UK</i>)_	
Intelligence-Architektur	149
Interview: Rafaela Kraus (<i>Universität der Bundeswehr, München</i>)_	
Cognitive Warfare	155
Raluca Csernatonu (<i>Carnegie Europe, Belgien</i>)_	
Kognitive Sicherheit	159
Jim Sengl und Felix Rieger (<i>KI.M KI Kompetenzzentrum Medien</i>)_	
Advertorial Souveräne Medien	164
Interview: Larysa Visengereyeva (<i>Women in Defense Tech WiDT</i>)_	
Preparedness	166
Irina Rosensaft (<i>Expertin für Digitale Transformation und Cybersicherheit</i>)_	
Collective Intelligence	171
Interview: Dennis-Kenji Kipker (<i>Cyber Intelligence Institute, Frankfurt a. Main</i>)_	
Cyberresilienz	176
Birger P. Priddat (<i>Universität Witten/Herdecke</i>)_	
Demokratische Intelligenz	179



Interview mit Krista-Marija Läbe,
Kommunikationsstrategin bei Quantum
Systems und Mitbegründerin der
Deutsch-Ukrainischen Gesellschaft DUG

Fakten

Contributors & Interviewpartner.....	185
Partner.....	189
Impressum.....	189

01_ Intelligence Matters

Wissen ist Macht

„The strategy employed by European countries to counter Russia’s escalating hostile intelligence activities has demonstrated moderate effectiveness.“

Niccolò Petrelli, Italien.

Illustration FierceAbin/iStock



*„Haben wir einen
Punkt erreicht, an
dem wir aktive
Gegenmaßnahmen
ergreifen müssen?“*

Martin Jäger, Präsident des Bundesnachrichtendienstes,
13. Februar 2026

Im Dienst der Demokratie

Demokratien brauchen verlässliches Wissen, um handlungsfähig zu bleiben. In einer Welt digitaler Datenfluten, hybrider Angriffe und Desinformation wird Intelligence zu einer zentralen Infrastruktur der offenen Gesellschaft.

Der Ernst der Lage war Martin Jäger anzumerken. Der Präsident des Bundesnachrichtendienstes (BND) sprach über russische Cyberangriffe, Desinformation, Sabotage, Drohnenüberflüge, Auftragsmorde. Und er wählte deutliche Worte: Es sei Russlands Führung, die destabilisierende Kampagnen in unseren Gesellschaften orchestriert. Sie verfolge damit das Ziel, die Nato zu spalten, pro-russische Regierungen zu installieren, die EU zu delegitimieren: „Wenn Russland Erfolg hätte, wären die Folgen überall spürbar“.

Der BND-Präsident stellte eine Frage in den Raum: „Wollen wir diese Entwicklungen einfach weiterhin nur beobachten und dokumentieren, oder haben wir einen Punkt erreicht, an dem wir aktive Gegenmaßnahmen ergreifen müssen?“ Die Frage beziehe sich auch auf den BND, ergänzte Jäger – und gab sich die Antwort gleich selbst: „Meiner Meinung nach muss und wird der Dienst operativer werden.“

Der Auftritt Jägers am 13. Februar 2026 auf der Münchner Sicherheitskonferenz war in mehrfacher Hinsicht bemerkenswert. Es ist schon nicht alltäglich, dass Nachrichtendienstler überhaupt auf öffentlichen Veranstaltungen sprechen. Noch ungewöhnlicher ist es, dass ein deutscher Nachrichtendienst-Chef der russischen Führung kaum verklausuliert mit Vergeltung droht. Schon das zeigt, wie dramatisch sich die Welt verändert hat.

BND-Präsident Martin Jäger, seit September 2025 im Amt, gilt als außenpolitisch erfahrener Krisendiplomat, als Mann für schwierige Aufgaben, den man überall hinschicken kann, wo es gerade brennt. Unter anderem war er deutscher Botschafter in >

TEXT_ Thomas Vašek

Thomas Vašek ist Co-Chefredakteur von „human“. Zuvor war der gelernte Investigativjournalist unter anderem Gründungschefredakteur der Philosophiezeitschrift „Hohe Luft“ sowie der deutschen Ausgabe von „MIT Technology Review“.

KEY MESSAGES

- **Epochenbruch der Weltordnung:** Regeln verlieren an Bedeutung, strategische Unsicherheit wächst – damit steigt der Bedarf an Intelligence.
- **Transformation der Intelligence:** In einer Welt der Datenfülle werden Analyse und strategische Deutung von Informationen immer wichtiger.
- **Rolle von KI und OSINT:** KI und offene Quellen erweitern Analysefähigkeiten, schaffen aber auch Risiken durch Desinformation und Datenmanipulation.
- **Epistemische Funktion:** Nachrichtendienste werden zu institutionellen Wahrnehmungs- und Analyseapparaten.
- **Europäische Perspektive:** Europa sollte Intelligence stärker koordinieren, z.B. durch europäische OSINT-Agentur.

„Gute Intelligence hilft, bessere Entscheidungen zu treffen.“

Afghanistan, später im Irak und zuletzt in Kiew. In den zwei Jahren seiner Dienstzeit hat er nach eigenen Angaben über 1000 Luftalarme erlebt.

Jäger ist nicht der typische Verwaltungsjurist, wie man ihn beim BND so häufig findet. Er hat Ethnologie, Philosophie und Politikwissenschaft studiert. Mit seiner vielfältigen Erfahrung – er war zeitweilig auch für den Autokonzern Daimler tätig – soll er den Dienst auf „allerhöchstes Niveau“ führen, wie es Bundeskanzler Friedrich Merz als Ziel formuliert hat.

ZEITENWENDE DER DIENSTE

Bei der öffentlichen Anhörung durch das Parlamentarische Kontrollgremium im Oktober 2025 deutete Jäger an, in welche Richtung er den BND verändern will. Der deutsche Auslandsnachrichtendienst müsse auch mal Risiken eingehen, um an „wertige Informationen“ heranzukommen. Nur so werde man anschlussfähig für europäische und internationale Partnerdienste, für das »harte Geschäft« der nachrichtendienstlichen Kooperation, das auf dem Geben und Nehmen von Informationen beruht.

Was Jäger vorschwebt, das ist nichts weniger als ein Kulturwandel beim BND. Der Dienst soll schneller, proaktiver, wagemutiger werden. Den Gegner auch mal konfrontieren, ihm Widerstand entgegensetzen, ja sogar Schmerzen zufügen, wenn es nötig ist. Das setze natürlich voraus, dass man dem Dienst auch die entsprechenden „Mittel und Befugnisse“ an die Hand gebe.

Die Stoßrichtung ist klar: Weg vom Berichtswesen, hin zum „echten“ Geheimdienst, der auch aktive Operationen durchführt. Der womöglich in Wohnungen einbricht, Computernetzwerke hackt oder gegnerische Infrastrukturen sabotiert, wenn es der rechtliche Rahmen erlaubt. Alle diese Fragen sind für die Handlungsmöglichkeiten der Dienste von großer Bedeutung.

Doch es wäre ein Fehler, die Debatte über die anstehende Reform der deutschen Nachrichtendienste auf Fragen von „Mitteln und Befugnissen“ zu beschränken. Entscheidend ist, was wir von den Diensten überhaupt erwarten, welche Ziele wir mit ihnen verfolgen, in Deutschland ebenso wie im europäischen Kontext.

Mit anderen Worten: Es geht um Strategie.

In der Disruption der Weltordnung liegt zugleich eine Chance für die Nachrichtendienste, sich neu zu erfinden. Dabei geht es um weit mehr als die Fähigkeit, hybride Angriffe wirksamer ab-

zuwehren. Auch die Frage, wie europäische Dienste unabhängiger von ihren US-Partnern werden können, greift zu kurz. Entscheidend ist vielmehr, wie wir strategisches Wissen in der neuen „Weltunordnung“ organisieren müssen, um unsere Werte und Interessen zu wahren.

Nachrichtendienste sind nicht einfach nur ein skandalanfälliges, notwendiges Übel, als das sie gerade in Deutschland oft gesehen werden. Wir brauchen sie schlicht, um in einer immer gefährlicheren, immer schnelleren und komplexeren Welt handlungsfähig zu bleiben.

Die internationale Ordnung der Nachkriegszeit beruhte in wesentlichen Teilen auf Regeln, Normen und Institutionen. Staaten konnten zumindest in groben Zügen antizipieren, wie andere Akteure reagieren würden. Regeln reduzierten damit Unsicherheit. Sie strukturierten das Handeln, begrenzten Eskalation und garantierten eine gewisse Verlässlichkeit in einem ansonsten anarchischen System.

Wenn Regeln nicht mehr zählen, wird Verhalten schwerer vorhersehbar. Verträge können gebrochen, institutionelle Verfahren umgangen werden. In einer solchen Umgebung brauchen wir mehr Wissen. Wer sich nicht mehr auf andere Akteure verlassen kann, muss besser verstehen, welche Ziele und Absichten sie verfolgen. Das gilt nicht nur für die Politik.

Es ist diese Art Wissensvorsprung, um den es bei „Intelligence“ geht. Wenn man den Begriff eng fasst, dann meint er schlicht das Sammeln und Auswerten von Informationen für Regierungen. Gute Intelligence ist Wissen, das hilft, bessere Entscheidungen zu treffen. Über die genaue Definition wird unter den Fachleuten gestritten, etwa um die Frage, ob Intelligence grundsätzlich „geheim“ ist – und ob es sich um eine staatliche Tätigkeit handelt.

Weitgehende Einigkeit herrscht darüber, dass Intelligence mehr ist als nur Information. Eine Information kann alles sein, was man erfährt. Unter Intelligence hingegen versteht man verarbeitete, geprüfte und entsprechend aufbereitete Information, die den Anforderungen des jeweiligen Entscheiders entspricht. Bei Intelligence gehe es nicht um absolute Wahrheit, schreibt der US-amerikanische Intelligence-Experte Mark M. Lowenthal, sondern um eine «Annäherung an die Realität».

Intelligence befindet sich heute mitten in einem strukturellen Wandel. Während im Kalten Krieg Informationen knapp wa- >

ren und die Dienste enorme Ressourcen aufwenden und hohe Risiken eingehen mussten, um an geheime Informationen heranzukommen, ist heute das Gegenteil der Fall: Informationen sind im Überfluss vorhanden, von kommerziellen Satellitenbildern über Social-Media-Inhalte bis zu geleakten Mobilfunkdaten, die im Dark Web zum Verkauf angeboten werden. Viele Entwicklungen – etwa militärische Bewegungen, wirtschaftliche Trends oder gesellschaftliche Dynamiken – lassen sich heute zumindest teilweise aus offenen Quellen rekonstruieren.

Die zunehmende Verfügbarkeit offen zugänglicher Informationen verändert die nachrichtendienstliche Arbeit. Die entscheidende Fähigkeit besteht nicht mehr primär im Sammeln, sondern im Verarbeiten, Einordnen und Interpretieren von Informationen. Open Source Intelligence (OSINT) und künstliche Intelligenz (KI) stehen im Zentrum dieses Wandels.

In mancher Hinsicht ist das nachrichtendienstliche Handwerk einfacher geworden, weil Daten leichter zu beschaffen sind. Zugleich aber ist es heute auch viel schwieriger, in der Datenflut das wirklich Relevante zu erkennen. „Information ist billig. Ihre Verarbeitung ist teuer – und ihre Deutung eine Kunst,“ schreibt Emily Harding, Intelligence-Expertin beim Center for Strategic and International Studies (CSIS), in ihrem Beitrag „Intelligence in a Transparent World“.

Die digitale Datenflut hat mehrere Konsequenzen für klassische Formen der nachrichtendienstlichen Arbeit. Erstens verschiebt sich ihre Funktion: Verdeckte Methoden dienen weniger der generellen Informationsbeschaffung als der Klärung spezifischer Fragen, die offene Quellen nicht beantworten können, etwa politische Absichten oder interne Entscheidungsprozesse.

Zweitens erhöht die digitale Transparenz moderner Gesellschaften auch die Risiken für operative Tätigkeit. Individuen hinterlassen heute umfangreiche digitale Spuren – etwa durch biometrische Daten, Reisebewegungen oder Onlineaktivitäten –, die verdeckte Identitäten und operative Kontakte leichter erkennbar machen können.

Drittens verändert die Offenheit des Informationsraums die Beziehung zwischen staatlicher Intelligence und anderen Akteuren. Journalisten, Forschungsgruppen, private Analysefirmen oder zivilgesellschaftliche Netzwerke betreiben heute teilweise selbst komplexe OSINT-Analysen und veröffentlichen ihre Ergebnisse öffentlich. Nachrichtendienste verlieren damit teilweise ihr Monopol auf bestimmte Formen strategischer Analyse.

Der Krieg in der Ukraine gilt als erster „Open-Source-Krieg“ der Geschichte. Kommerzielle Satellitenbilder, Social-Media-Daten und öffentlich zugängliche Sensorinformationen ermög-

Deutschlands Nachrichtendienste

Bundesnachrichtendienst (BND)

Der BND ist der Auslandsnachrichtendienst Deutschlands. Er sammelt und analysiert Informationen über politische, militärische, wirtschaftliche und technologische Entwicklungen im Ausland, die für die Sicherheit und Außenpolitik Deutschlands relevant sind. Seine Erkenntnisse unterstützen die Bundesregierung bei sicherheitspolitischen Entscheidungen.

Bundesamt für Verfassungsschutz (BfV)

Das BfV ist der Inlandsnachrichtendienst. Es beobachtet extremistische Bestrebungen, Terrorismus sowie Spionageaktivitäten fremder Dienste in Deutschland. Ziel ist der Schutz der freiheitlichen demokratischen Grundordnung. Der Verfassungsschutz arbeitet föderal mit den Landesämtern für Verfassungsschutz zusammen.

Militärischer Abschirmdienst (MAD)

Der MAD ist der Nachrichtendienst der Bundeswehr. Seine Aufgabe ist es, Spionage, Extremismus und sicherheitsgefährdende Aktivitäten gegen die Streitkräfte aufzudecken und abzuwehren. Er schützt damit Personal, Einrichtungen und Einsatzfähigkeit der Bundeswehr.

lichten es auch zivilen Akteuren, militärische Entwicklungen nahezu in Echtzeit zu beobachten.

Bereits vor der russischen Invasion 2022 machten öffentlich verfügbare Daten russische Truppenbewegungen sichtbar. Gleichzeitig wurde die ukrainische Bevölkerung selbst zu einem Teil des Intelligence-Systems: Smartphones, soziale Medien und zivile Satellitendaten verwandelten die Gesellschaft faktisch in ein verteiltes Sensornetzwerk. Hinzu kamen kommerzielle Unternehmen, die Satellitenbilder oder Cyberanalysen bereitstellten. Intelligence wurde damit zu einer Gemeinschaftsleistung von Staat, Gesellschaft und Privatwirtschaft.

Die enormen Datenmengen, die bei Nachrichtendiensten anfallen, sind ohne algorithmische Unterstützung schlicht nicht mehr zu bewältigen. Schon heute integrieren die Dienste KI in ihre Analyse- und Auswertungsprozesse. Was früher enorme personelle Ressourcen erforderten, etwa die Auswertung globaler Medienströme oder großer Bildbestände, lässt sich heute teilweise automatisieren. KI kann zudem Informationen aus unterschiedlichen Quellen zusammenführen und so schneller Lagebilder erzeugen oder Veränderungen in komplexen Systeme- ➤

men sichtbar machen. Intelligence wird durch KI schneller, skalierbarer und in manchen Bereichen auch präziser. Beim BND soll etwa eine Arbeitseinheit für KI-gestützte Analyse bei der Erstellung eines Echtzeitlagebildes helfen. Gleichzeitig entstehen durch KI aber auch neue Risiken. Fehlerhafte Daten oder algorithmische Verzerrungen können sich durch automatisierte Analyseprozesse verstärken und ganze Entscheidungsketten beeinflussen. Kritisch wird dies in sicherheitsrelevanten Anwendungen, in denen KI-Systeme Informationen nicht nur analysieren, sondern operative Prozesse unterstützen. Mit agentischer KI kündigt sich bereits die nächste Stufe der KI-Revolution an.

KI-Agenten können eigenständig Aufgaben planen, Informationen beschaffen und digitale Werkzeuge einsetzen. Damit verschiebt sich der Einsatz von KI von der reinen Analyseunterstützung hin zu automatisierten Handlungssystemen – mit unabsehbaren Folgen für die Cybersicherheit.

Agentische Systeme können bereits heute große Teile eines Cyberangriffs autonom durchführen, von der Zielauswahl über Schwachstellenanalyse bis zur Exploit-Kette. Zugleich werden KI-Systeme aber auch selbst zu strategischen Angriffszielen, etwa durch Prompt-Injection oder manipulierte Trainingsdaten. Nachrichtendienste müssen daher lernen, nicht nur menschliche Akteure zu beobachten, sondern auch künstliche Systeme, die im Informationsraum eigenständig operieren.

Für Intelligence bedeutet dies eine doppelte Transformation. Erstens wird KI zur zentralen analytischen Plattform, mit der große Datenräume ausgewertet, Cyberoperationen unterstützt und Entscheidungsprozesse beschleunigt werden können. Zweitens entsteht eine neue Abhängigkeit von den Big Techs, die die leistungsfähigsten Modelle entwickeln und kontrollieren. Intelligence-Fähigkeiten werden damit teilweise privatisiert.

Der Konflikt zwischen dem Pentagon und dem KI-Unternehmen Anthropic zeigt, dass fortgeschrittene KI-Modelle zunehmend als strategische Infrastruktur betrachtet werden. Die US-Regierung forderte umfassenden Zugang zu den Modellen der Firma für militärische Anwendungen, während Anthropic dies mit Verweis auf Risiken wie autonome Waffensysteme oder massenhafte Überwachung ablehnte. Zugleich verfolgt auch China das Ziel, KI militärisch nutzbar zu machen.

Staaten sehen KI heute als entscheidenden Faktor geopolitischer Macht und wollen ihre Entwicklung beschleunigen. Gleichzeitig warnen viele Experten, dass die Technologie noch unausgereift und gefährlich ist. Intelligence wird sich in Zukunft daher immer mehr darum drehen, wer den Zugang zu solchen hochriskanten Systemen hat.

Demokratien beruhen nicht nur auf Wahlen, Institutionen und Rechtsstaatlichkeit, sondern auch auf einer gemeinsamen epistemischen Grundlage, also auf einem Mindestmaß an geteiltem Wissen über die Realität, über Risiken und politische Optionen. Intelligence kann zu diesem Wissen beitragen. Diese Funktion gewinnt auch deshalb an Bedeutung, weil der Informationsraum selbst zum strategischen Konfliktfeld geworden ist. Autoritäre Akteure versuchen gezielt, demokratische Gesellschaften durch Desinformation, Informationsüberflutung und manipulative Narrative zu destabilisieren. Solche Operationen zielen letztlich darauf ab, Vertrauen in jede Form verlässlicher Information zu untergraben.

Intelligence kann in diesem Kontext als Teil der epistemischen Infrastruktur demokratischer Staaten verstanden werden. Staatliche Analysefähigkeiten tragen dazu bei, dass politische Institutionen unter Bedingungen wachsender Unsicherheit handlungsfähig bleiben.

Medien, Wissenschaft und zivilgesellschaftliche Akteure leisten wichtige Beiträge zur öffentlichen Wissensproduktion, verfügen jedoch weder über denselben Zugang zu sensiblen Informationen noch über die Verantwortung für kollektive Sicherheit.

In einer zunehmend komplexen Informationsumgebung wirken Nachrichtendienste als institutionalisierter Wahrnehmungs- und Analyseapparat des Staates. Sie sammeln, prüfen und kontextualisieren Informationen, um belastbares Wissen für politische Entscheidungen bereitzustellen. Es geht um die systematische Produktion von Erkenntnissen über Risiken, Absichten und Entwicklungen im internationalen Umfeld.

Intelligence hat nicht nur die Aufgabe, Bedrohungen frühzeitig zu erkennen. Sie kann auch helfen, strategische Chancen sichtbar zu machen, Handlungsspielräume zu identifizieren, Situationspotenziale zu nutzen. Sollten unsere Nachrichtendienste nicht die Ambition entwickeln, solche Chancen im geopolitischen oder technologischen Wettbewerb aufzuspüren? Und sollen sie dafür nicht auch in einem gewissen Rahmen Spionage betreiben dürfen, um einen Wissensvorsprung zu erlangen?

Wenn Intelligence als Wahrnehmungs- und Analyseapparat des Staates verstanden wird, kann sie auch eine wichtige Rolle für das Vertrauen in staatliche Handlungsfähigkeit spielen. Denn Vertrauen in den Staat entsteht nicht nur aus normativer Legitimität oder demokratischen Verfahren, sondern auch aus der Annahme, dass staatliche Institutionen die Realität angemessen erkennen und auf dieser Grundlage handeln können, und zwar über Wahlperioden hinweg. Das setzt allerdings voraus, dass staatliche Intelligence tatsächlich zu besserer Erkenntnis der >

„Ein gemeinsames Lagebild würde die außen- und sicherheitspolitische Koordination in Europa verbessern.“

Realität führt. In der Praxis neigen Nachrichtendienste auch zu Verzerrungen, die zu Fehlwahrnehmungen führen können. Historische Beispiele – etwa Fehleinschätzungen zur Existenz von Massenvernichtungswaffen im Irak – zeigen, dass Intelligence keineswegs automatisch überlegenes Wissen garantiert. Wenn staatliche Analyseinstitutionen irren, kann dies Vertrauen sogar massiv untergraben.

Demokratische Wissensordnungen leben von Pluralität und Offenheit: Wissenschaft, Medien, Zivilgesellschaft und unabhängige Forschung tragen gemeinsam zur Interpretation von Realität bei. Wenn Intelligence zur privilegierten epistemischen Instanz wird, kann das diese pluralen Erkenntnisprozesse verdrängen oder delegitimieren.

Nachrichtendienste arbeiten zumindest teilweise im Geheimen. Gerade diese Geheimhaltung kann jedoch das Vertrauen in ihre Erkenntnisse begrenzen. Wenn zentrale Wissensgrundlagen politischer Entscheidungen nicht öffentlich überprüfbar sind, kann dies Skepsis und Verschwörungstheorien sogar verstärken. Auch deshalb müssen wir die Rolle der Dienste in der Demokratie immer wieder neu überdenken. Die Frage ist, wie sie sich strukturell verändern müssen, um in der heutigen Informationsumgebung handlungsfähig zu bleiben, ohne sich von der demokratischen Gesellschaft abzukoppeln.

Die Idee eines europäischen Nachrichtendienstes wird seit Jahren diskutiert, stößt jedoch auf erhebliche politische und institutionelle Hürden. Geheimdienste gehören traditionell zum Kern staatlicher Souveränität; Mitgliedstaaten sind daher zurückhaltend, sensible Quellen, Methoden und operative Fähigkeiten preiszugeben. Unterschiede in Bedrohungswahrnehmungen, rechtlichen Rahmenbedingungen und Vertrauensniveaus erschweren zusätzlich eine unmittelbare Integration.

Vor diesem Hintergrund könnte eine europäische OSINT-Analyseagentur als realistischer Zwischenschritt dienen. Eine solche Einrichtung würde sich ausschließlich auf Open Source Intelligence konzentrieren, also auf die Sammlung und Analyse öffentlich verfügbarer Informationen. Anders als klassische Nachrichtendienste hätte sie keine verdeckten Operationen und keine geheimen Quellen. Ihr Auftrag bestünde darin, offene Da-

ten systematisch auszuwerten und daraus europäische Lagebilder zu erstellen und zugleich professionelle Analysestandards zu sichern. Gerade in einer digitalisierten Welt, in der große Teile strategisch relevanter Informationen öffentlich zugänglich sind, gewinnt diese Form der Analyse stark an Bedeutung. Eine solche Einrichtung wäre politisch leichter realisierbar als ein europäischer Nachrichtendienst und könnte langfristig Vertrauen, gemeinsame Methoden und ein europäisches Bedrohungsverständnis entwickeln. Offene Informationen lassen sich deutlich leichter teilen als sensible Geheimdienstquellen.

Eine OSINT-Agentur könnte so Vertrauen aufbauen und eine gemeinsame europäische Analyseplattform schaffen, ohne nationale Souveränität unmittelbar zu berühren. Gleichzeitig entstünden Skaleneffekte: Aufwendige Dateninfrastrukturen, KI-gestützte Analyseplattformen oder satellitengestützte Geodaten müssten nicht von jedem Staat separat aufgebaut werden.

Zudem könnte eine europäische OSINT-Agentur zur Entwicklung einer gemeinsamen Bedrohungswahrnehmung beitragen. Hybride Bedrohungen betreffen Europa als Ganzes, werden aber bislang überwiegend auf nationaler Ebene analysiert. Ein gemeinsames Lagebild würde die außen- und sicherheitspolitische Koordination verbessern. Damit hätte eine OSINT-Agentur auch eine institutionelle Lernfunktion.

Gemeinsame Analyseverfahren, Ausbildungsprogramme und technische Standards würden entstehen. Analysten aus verschiedenen europäischen Staaten könnten in gemeinsamen Strukturen arbeiten und Vertrauen aufbauen. Solche Netzwerke wären eine zentrale Voraussetzung für jede weitergehende Zusammenarbeit im Bereich Intelligence. In diesem Sinne wäre eine europäische OSINT-Agentur weniger ein Ersatz für nationale Nachrichtendienste als vielmehr ein evolutionärer Zwischenschritt. Sie würde gemeinsame Analysekapazitäten schaffen, ohne sofort operative Kompetenzen zu zentralisieren.

Wenn es gelingt, Vertrauen, gemeinsame Methoden und ein europäisches Lageverständnis zu etablieren, könnte daraus langfristig eine stärkere Integration entstehen – möglicherweise sogar die Grundlage für einen europäischen Nachrichtendienst. Eine europäische OSINT-Agentur würde auch von der Diver- ➤

sität in Europa profitieren. Die EU vereint 24 Amtssprachen und zahlreiche weitere Regional- und Minderheitensprachen. Eine Analystin aus Litauen liest russischsprachige Telegram-Kanäle vermutlich anders als jemand ohne historische und kulturelle Erfahrung im postsowjetischen Raum. Ein souveränes europäisches Sprachmodell könnte als zentrale analytische Infrastruktur dienen, die große Mengen offener Informationen aus verschiedenen Sprachen, Quellen und Beschaffungsarten integriert.

In einer Welt exponentiell wachsender Datenmengen wird Intelligence zunehmend zur Fähigkeit, die Analysekapazitäten der KI mit menschlicher Erfahrung und Urteilskraft zu verbinden. Darin liegt vielleicht die strategische Chance Europas, in einer immer gefährlicheren Welt den entscheidenden Wissensvorsprung zu gewinnen.

Europa wird Teile seiner Intelligence mit KI automatisieren müssen, um im heutigen Informationsraum handlungsfähig zu bleiben. Doch was nicht automatisierbar ist, das ist unsere menschliche Entschlossenheit, unsere Interessen und Werte in Zeiten der Unsicherheit zu verteidigen.

Wir befinden uns in einem „eisigen Frieden“, der punktuell

jederzeit in eine „heiße Konfrontation“ umschlagen könne, sagte BND-Präsident Martin Jäger im Oktober 2025 bei der Anhörung im Bundestag. Man sei konfrontiert mit einer „aggressiven Gegenmacht“, die wenig Zurückhaltung kenne. Und was für Russland gelte, das gelte zunehmend auch für andere internationale Akteure: „Diese Realität müssen wir anerkennen.“

Es ist weder militärische, noch wirtschaftliche oder technologische Macht allein, die in einer solchen Auseinandersetzung entscheidet, das weiß auch Jäger. Es kommt darauf an, resilienter zu sein, mehr zu wissen, schlauer zu sein als der Gegner. Man könne von der Widerstandskraft der Ukrainer in den letzten vier Jahren viel lernen, sagte der BND-Präsident im Bundestag – nicht zuletzt in mentaler Hinsicht.

Eine Auseinandersetzung werde „in den Köpfen gewonnen“, habe ihm ein ukrainischer Frontoffizier einmal gesagt. Auf das richtige Mindset, die entschlossene Einstellung komme es an. Dazu gehöre es, sich auf extreme Entwicklungen einzustellen und sich selbst in die Lage zu versetzen, unter extremen Bedingungen zu handeln: „Nur dadurch werden wir unsere Gegner abschrecken und den Ernstfall meistern können.“ ■

GLOSSAR

Intelligence

Systematische Gewinnung, Analyse und Bewertung von Informationen über Akteure, Risiken und Entwicklungen zur Unterstützung politischer und sicherheitspolitischer Entscheidungen.

Intelligence Cycle

Prozess von Planung, Sammlung, Auswertung und Weitergabe von Informationen. Beschreibt, wie Rohdaten in entscheidungsrelevante Erkenntnisse überführt werden.

HUMINT (Human Intelligence)

Gewinnung von Informationen durch menschliche Quellen, etwa Informanten, Überläufer oder verdeckte Kontakte.

SIGINT (Signals Intelligence)

Auswertung elektronischer Signale und Kommunikation, etwa Mobilfunk- oder Internetverkehr.

OSINT (Open Source Intelligence)

Analyse öffentlich verfügbarer Informationen, z. B. Medienberichte, Social Media, Satellitenbilder oder Datenbanken.

All-Source Analysis

Zusammenführung verschiedener Quellenarten (HUMINT, SIGINT, OSINT etc.), um ein umfassendes Lagebild zu erstellen.

Indications & Warning (I&W)

Frühwarnanalyse zur Identifikation von Hinweisen auf bevorstehende Krisen, Angriffe oder strategische Veränderungen.

Counterintelligence

Maßnahmen zum Schutz vor Spionage, Sabotage und Einflussoperationen fremder Dienste oder Akteure.

Covert Action

Verdeckte staatliche Operationen zur politischen Einflussnahme im Ausland, bei denen die wahre Urhebererschaft verborgen bleiben soll.

Intelligence Assessment

Analytische Bewertung von Entwicklungen und Szenarien, die Entscheidungsträgern mögliche Risiken und Handlungsoptionen aufzeigt.

Resilienz ohne Entschlossenheit

Russlands hybride Angriffe fordern Europas Sicherheitsarchitektur immer wieder heraus. Die Gegenmaßnahmen zeigen zwar Wirkung, es gibt aber auch anhaltende Schwächen.

Mit dem Eintritt ins Jahr 2026 steht Europa an einem kritischen Punkt seines Schattenkonflikts mit Russland – eines Krieges, der nicht mit konventionellen Schlachten geführt wird, sondern mit einer unablässigen Abfolge hybrider Taktiken, darunter Sabotage, Spionage, Cyberangriffe und Desinformationskampagnen. Diese Auseinandersetzung, die sich nach Russlands großangelegter Invasion der Ukraine im Februar 2022 dramatisch verschärfte, hat Moskau dazu veranlasst, Methoden einzusetzen, um die europäische Geschlossenheit zu untergraben, die öffentliche Unterstützung für Kyjiw zu schwächen und die Reaktionsschwellen der NATO zu testen, ohne einen offenen Krieg auszulösen.¹ Nach einem deutlichen Anstieg entdeckter russischer Operationen in ganz Europa – von Brandanschlägen auf militärische Lieferketten bis hin zu GPS-Störungen über der Ostsee –, die sich von 2023 auf 2024 nahezu verdreifachten, brachte das Jahr 2025 jedoch eine unerwartete Wende: Vorfälle klassischer Sabotage und Brandstiftung gingen auf etwa die Hälfte des Vorjahresniveaus zurück.²

Dieser Rückgang ist zwar ermutigend, wirft jedoch Fragen über Europas Umgang mit dem nachrichtendienstlichen Wettbewerb mit Russland auf. Welche Strategie spiegeln die ergriffenen Gegenmaßnahmen tatsächlich wider, und was sind – wenn überhaupt – ihre zentralen Elemente? Tragen sie Früchte? >

¹ Seth G. Jones, "Russia's Shadow War against the West", *Center for Strategic and International Studies Brief*, March 18, 2025, <https://www.csis.org/analysis/russias-shadow-war-against-west>.

² <https://www.france24.com/en/europe/20251228-russia-hybrid-warfare-attacks-europe-dropped-this-year-but-could-they-pick-up-2026>.

TEXT_ Niccolò Petrelli

Dr. Niccolò Petrelli ist Assistenzprofessor am Fachbereich Politikwissenschaften der Universität Roma Tre, wo er strategische Studien lehrt. 2025 veröffentlichte er das Buch *I servizi segreti italiani e l'Intelligence USA (Die italienischen Geheimdienste und der US-Geheimdienst)*, eine Geschichte der wechselseitigen Beziehungen von 1943 bis zu den 1970er Jahren.

KEY MESSAGES

- **Europa** hat Russlands feindliche nachrichtendienstliche Aktivitäten mit einer defensiven Strategie aus Resilienz und Disruption beantwortet.
- **Gemeinsame Bedrohungsanalysen** und der Austausch von Erkenntnissen haben Desinformations- und Einflussoperationen geschwächt.
- **Massenhafte Ausweisungen** haben russische Geheimdienstnetzwerke und deren operative Fähigkeiten erheblich beeinträchtigt.
- **Grenzbefestigungen und der Schutz kritischer Infrastrukturen** verringerten Sabotagemöglichkeiten und verhinderten „leichte Erfolge“.
- **Trotz dieser Erfolge** bleiben europäische Schwächen wie Fragmentierung, verzögerte Attribution und eine überwiegend defensive Grundhaltung.

Europa hat auf die Intensivierung dieses Wettbewerbs durch Russland mit der Umsetzung einer defensiven Strategie der Resilienz und Disruption reagiert. Diese Strategie verknüpft nachrichtendienstliche Erkenntnisse mit politischen Maßnahmen und gesellschaftlichem Handeln und stützt sich dabei auf vier Elemente.

Das erste Element ist die gemeinsame Bedrohungsanalyse und -bewertung mit dem Ziel, ein gemeinsames „strategisch-operatives Lagebild“ zu entwickeln, Bedrohungswahrnehmungen zu bündeln und das öffentliche Bewusstsein für die Gefahr zu schärfen. Die EU führt seit 2020 gemeinsame Bedrohungsanalysen durch; diese Praxis wurde nach Russlands Invasion der Ukraine im Februar 2022 im Rahmen der Single Intelligence Analysis Capacity (SIAC) deutlich intensiviert. Die SIAC ist eine EU-nachrichtendienstliche Struktur, die sich aus dem Intelligence and Situation Centre (INTCEN) beim Europäischen Auswärtigen Dienst (EAD) und dem Intelligence Directorate des EU-Militärstabs zusammensetzt.³

In der baltischen Region, wo die Verwundbarkeiten besonders ausgeprägt sind, haben Estland, Lettland, Litauen, Polen und Finnland die nachrichtendienstliche Zusammenarbeit weiter vertieft und robuste Mechanismen zum Informationsaustausch entwickelt. Dabei werden Nachrichtendienstlerkenntnisse häufig mit Open-Source-Daten (OSINT) und investigativem Journalismus kombiniert, um Desinformationsnetzwerke zu zerschlagen. Litauens „Elfen“, ein Graswurzelnetzwerk freiwilliger Factchecker zur Entlarvung von Kreml-Narrativen, stehen exemplarisch für dieses gesamtgesellschaftliche Engagement.⁴

Das zweite Element der Strategie sind umfangreiche Ausweisungen russischer Offizieller. In den vergangenen vier Jahren haben europäische Staaten beispiellose, koordinierte Ausweisungen russischen diplomatischen Personals vorgenommen, von denen viele ausdrücklich als Geheimdienstoffiziere identifiziert wurden (vor allem des Militärgeheimdienstes GRU, des Auslandsgeheimdienstes SVR und des Inlandsdienstes FSB), die unter diplomatischer Tarnung operierten. Ziel war es, die für hybride Kriegsführung genutzten Netzwerke zu stören. Schätzungen

zufolge wurden in den Jahren 2023 bis 2025 europaweit über 600 bis 750 russische Offizielle (von denen viele als Geheimdienstpersonal galten) ausgewiesen.

Diese Maßnahmen wurden explizit mit der Abwehr russischer hybrider Kriegsführung begründet – nicht nur klassischer Spionage, sondern auch aktiver Unterwanderung, Bedrohungen kritischer Infrastruktur und destabilisierender Aktivitäten im Zusammenhang mit dem Ukrainekrieg. In der Folge ist Russland zunehmend auf nicht-diplomatische Methoden angewiesen (etwa angeworbene Einheimische, Stellvertreter sowie Cyber- und Sabotageakte). Gleichwohl zählen die Ausweisungen zu den wirksamsten kollektiven Gegenmaßnahmen gegen Moskaus Geheimdienstnetzwerke in Europa seit dem Kalten Krieg.⁵

Das dritte Element ist der Ausbau der Grenzüberwachung und -befestigungen, mit dem Ziel, instrumentalisierte Migration (über Belarus), Drohnenüberflüge und Sabotagebedrohungen einzudämmen. Zentrale Maßnahmen in diesem Bereich umfassten die Verstärkung physischer Barrieren, Panzerabwehranlagen, Überwachungssysteme und Anti-Drohnen-Technologien. Die Investitionen beschleunigten sich in den Jahren 2024–2025 angesichts einer Zunahme entsprechender Vorfälle (u. a. 58 Drohnenüberflüge seit 2022, davon allein 36 im Jahr 2025). Staaten wie Polen, Estland, Lettland, Litauen und Finnland investierten Milliarden in physische Sperranlagen, Überwachungsnetze und Maßnahmen zur Bewegungshemmung. Polens Programm „East Shield“, die „Baltic Defense Line“ sowie die finnischen Grenzbefestigungen stehen exemplarisch für diesen Kurswechsel. Entlang von Hunderten Kilometern an den Grenzen zu Belarus, Russland und der Exklave Kaliningrad entstanden hohe Stahlzäune, tiefe Panzergräben, betonierte „Drachenzähne“, Bunker, hochentwickelte ISR-Systeme (Intelligence, Surveillance, Reconnaissance) sowie zunehmend leistungsfähige Anti-Drohnen-Abwehrsysteme.⁶

Das vierte und letzte Element besteht in der Stärkung des Schutzes kritischer Infrastrukturen, mit dem Ziel, einerseits die systemische Resilienz zu erhöhen und andererseits russischen

³ <https://www.euronews.com/my-europe/2025/05/23/we-know-what-russia-is-doing-and-how-it-does-it-eu-intelligence-centre-chief-tells-euron>; <https://www.politico.eu/article/europe-intelligence-spies-donald-trump-russia-security-politics/>.

⁴ <https://www.debunk.org/about-elves>.

⁵ Kevin P. Riehle, „Soviet and Russian Diplomatic Expulsions: How Many and Why?“, *International Journal of Intelligence and Counterintelligence*, 37/4 (2024), 1238–1263; <https://greynomics.com/the-silent-hand-russian-intelligence-activities-in-europe>; <https://tass.com/politics/1567203>.

⁶ <https://pism.pl/publications/eu-and-nato-states-investing-in-protection-of-borders-with-russia-and-belarus>; <https://valtioneuvosto.fi/en/situation-at-finlands-eastern-border>; <https://raja.fi/en/the-eastern-border-barrier-fence>.

Saboteuren leicht angreifbare Ziele zu entziehen. Die Sabotage der Nordstream-Pipelines im September 2022 wirkte dabei als Weckruf und machte die Verwundbarkeiten von Energienetzen, Unterseekabeln, Pipelines und Verkehrsnetzen deutlich sichtbar.

Darauf folgte rasch eine Vielzahl von Initiativen auf EU-, NATO- und nationaler Ebene, um den Schutz physischer Infrastrukturen zu verbessern. Hervorzuheben ist dabei die EU-Richtlinie zur Resilienz kritischer Einrichtungen (Critical Entities Resilience Directive) vom Dezember 2022, die die Mitgliedstaaten verpflichtet, innerhalb von zehn Monaten technische, sicherheitsbezogene und organisatorische Maßnahmen umzusetzen. Der Fokus liegt auf Prävention, Reaktion und Wiederherstellung gegenüber allen Gefährdungsarten, einschließlich Sabotage, und erstreckt sich auf elf Sektoren, darunter Energie, Verkehr, Bankenwesen, Gesundheitswesen und digitale Infrastrukturen.⁷ Ergänzt wurde dies durch die EU-NATO-Taskforce zur Resilienz kritischer Infrastrukturen von 2023, die gezielt Expertise aus dem privaten Sektor einbezog, um Schwachstellen in Energienetzen und Unterseekabeln zu identifizieren.⁸ Auch beim Schutz digitaler Infrastrukturen handelten die europäischen Staaten zügig.

Die Cyber Defence Policy von 2022 aktualisierte die Anforderungen der Richtlinie über Netz- und Informationssicherheit (NIS-2), insbesondere in Bezug auf Meldepflichten bei Vorfällen und die Sicherheit von Lieferketten. Zugleich verbesserte sie die Koordination zwischen zivilen und militärischen Cyberaktivitäten, stärkte die technologische Souveränität, förderte Investitionen in Fähigkeiten und festigte die europäische Verteidigungsindustrie.⁹ Darauf folgte der Cyber Solidarity Act, der im Februar 2025 in Kraft trat. Er schuf den European Cyber Shield – ein paneuropäisches Netzwerk nationaler und grenzüberschreitender Security Operations Centers, das mithilfe von KI und Datenanalyse Bedrohungen in Echtzeit erkennt und darauf reagiert.¹⁰

Die von den europäischen Staaten eingesetzte Strategie zur Abwehr der zunehmend feindlichen nachrichtendienstlichen Aktivitäten Russlands – ein defensiver Ansatz, der, wie gezeigt, auf Disruption und Resilienz ausgerichtet ist – hat moderate Wirksamkeit entfaltet. Bis Anfang 2026 trug sie spürbar zu einem

„Russland reagiert oft schneller, als Europa nachziehen kann.“

Niccolò Petrelli

Rückgang der Vorfälle bei, verhinderte zivile Todesopfer und minderte unmittelbare Eskalationsrisiken, ohne einen offenen Konflikt zu provozieren – ein bemerkenswerter Erfolg in einem hoch angespannten Umfeld.

ERFOLGE UND HERAUSFORDERUNGEN

Tatsächlich hat diese Strategie erstens Russlands Desinformations- und Unterwanderungsbemühungen geschwächt, indem sie europaweit eine größere Gemeinsamkeit in der Bedrohungswahrnehmung gefördert und damit die Wirksamkeit von Fragmentierungsstrategien reduziert hat. Durch die Verknüpfung unterschiedlicher nachrichtendienstlicher Quellen und Methoden sowie die engere Anbindung von Intelligence an politische und gesellschaftliche Maßnahmen gelang es häufig, Propagandnetzwerke und Einflusskampagnen frühzeitig offenzulegen und dadurch ihre Wirkung zu mindern.

Die Ausweisungen haben Russlands operative Fähigkeiten unmittelbar geschwächt, indem sie etablierte Netzwerke zerschlugen und die Führungs-, Kontroll- und Koordinationsmöglichkeiten vor Ort für Sabotage, Rekrutierung und Nachrichtengewinnung einschränkten. Die Grenzbefestigungen wiederum verringerten die Möglichkeiten für Grenzsondierungen und Sabotageeinsätze. Nicht zuletzt führte der verbesserte Schutz kritischer Infrastrukturen zu widerstandsfähigeren physischen und digitalen Systemen, die mehr Angriffe besser absorbieren und deren Folgen begrenzen können.

All dies erschwert Russlands Vorgehen, indem es „leichte Erfolge“ unterbindet und Moskau zugleich unter Druck setzt, zu innovieren: entweder durch qualitativ schwache Massenoperationen mit geringer Erfolgsaussicht oder durch komplexere, ressourcenintensive Maßnahmen, die jedoch leichter zu erkennen, zuzuordnen und zu bekämpfen sind. >

⁷<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557>.

⁸https://assets.kpmg.com/content/dam/kpmg/be/pdf/RR-Critical-Entities-Resilience-Directive-2025-EN-Brochure-A4_Final.pdf; https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

⁹<https://www.european-cyber-defence-policy.com>.

¹⁰<https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>.

Trotz dieser Erfolge bestehen weiterhin erhebliche Herausforderungen.¹¹ Russland hat sich als äußerst anpassungsfähig erwiesen und reagiert oft schneller, als Europa wirksam nachziehen kann. Dabei ist Moskau zu einer Art „Gig-Economy-Modell“ der Subversion übergegangen, das viele klassische Abwehrbarrieren umgeht und persistente Taktiken ermöglicht – etwa Desinformation über Doppelgänger-Websites oder Cyberangriffe (beispielsweise der Qilin-Ransomware-Angriff von 2025 auf spanische Systeme).¹²

Ein zentrales Problem bleibt die Fragmentierung: Die Reaktionen sind häufig national isoliert, geprägt von unzureichenden Budgets, unterschiedlichem politischem Commitment und Koordinationsdefiziten. Die Einordnung dieser Aktivitäten als „Grauzonen“-Handlungen verstärkt zudem die Ambiguität, verzögert Attribution und öffentliche Verurteilung.¹³

Rechtliche und diplomatische Zurückhaltung hat Naming-and-Shaming-Ansätze gebremst und dazu geführt, dass untererfasste Vorfälle über Jahre hinweg erhebliche wirtschaftliche Schäden in Höhe von Hunderten Millionen Euro verursachen konnten. Hinzu kommen übergeordnete strategische Defizite: So haben Europas Gegenmaßnahmen bislang die finanziellen Grundlagen russischer Operationen nicht umfassend adressiert.¹⁴

DEFENSIVE GRUNDHALTUNG

Europas Strategie hat zwar klare Stärken hervorgebracht – vereitelte Anschläge, erhöhte Resilienz und das Ausbleiben größerer Eskalationen –, zugleich aber auch anhaltende Schwächen offenlegt: Koordinationslücken, verzögerte Attribution und eine überwiegend defensive Grundhaltung, die es Russland erlaubt, Asymmetrien kostengünstig über Stellvertreter und neue Technologien wie KI-Deepfakes auszunutzen. Russland setzt diesen Schattenkrieg unbeirrt fort. Europa kann sich verteidigen – doch wie lange wird es jeden Schlag abwehren können? ■

¹¹ Lara Jakes, "Europe Wants to Get the Word Out: Russia Is to Blame for Sabotage", *the New York Times*, December 3 2025, <https://www.nytimes.com/2025/12/03/world/europe/europe-russia-hybrid-attacks.html>.

¹² Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* (London: International Institute for Strategic Studies, 2025), <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf>.

¹³ <https://apnews.com/article/russia-estonia-baltics-sabotage-spying-kallas-62835b00fdb31f648ebe2259908ca2a1>.

¹⁴ Tom Keatinge and Kinga Redłowska, „The Financial Dimension of EU Internal Security Threats“, *RUSI Insights Papers*, 21 November 2025 <https://www.rusi.org/explore-our-research/publications/insights-papers/financial-dimension-eu-internal-security-threats>.

Im Schatten der Zeitenwende

Geheimdienste stehen im Zentrum einer neuen Weltordnung. Terrorismus, Cyberkrieg und aggressive Großmachtpolitik fordern Europas Sicherheitsarchitektur heraus. Wie leistungsfähig sind die Dienste – und welche Reformen sind überfällig?

Gheimdienste haben prinzipiell drei Aufgaben. Sie sollen erstens für ihre Auftraggeber geheime Informationen beschaffen über deren Gegner oder Feinde, manchmal auch über Partner und Freunde. Im modernen souveränen Staat ist der Auftraggeber die Regierung. Die Informationen betreffen zumeist militärische, wirtschaftliche, technologische oder politische Sachverhalte, die geheim gehalten werden, um sich einen Vorteil zu verschaffen, der es erlaubt, den Gegner zu überraschen oder zu täuschen. Gelingt es, diese geheimen Informationen durch Spionage zu beschaffen, so nimmt man dem Gegner diesen Vorteil. Anders gewendet: Man erspart sich unangenehme Überraschungen.

Die zweite Aufgabe besteht darin, Spionageaktivitäten des Gegners abzuwehren. Dabei spricht man von Spionageabwehr und von Gegenspionage. Die dritte Aufgabe wird als verdeckte Operationen umschrieben. Sie umfasst viele Varianten, die von verdeckter Propaganda und Beeinflussung des Gegners, beispielsweise durch Bestechung oder heimliche Finanzierung von Aktivitäten, bis zu paramilitärischen Operationen wie Entführung, Sabotage oder gezielter Tötung reichen.

Alle drei Aufgaben können wir bis in die antike Welt zurückverfolgen, doch in modernen Demokratien dürfen sie nur auf gesetzlicher Grundlage und mit Überwachung durch unabhängige Staatsorgane, insbesondere durch Parlament und Justiz, erfolgen. Das Ziel ist der Schutz der Bevölkerung, der Staatsorgane und der Wirtschaft sowie der politischen und kulturellen Selbstbestimmung. In Diktaturen hingegen ist das primäre Ziel die Absicherung der Machthaber und ihres Herrschaftsapparates. Der Schutz der Bevölkerung spielt hier keine Rolle, wie wir tagtäglich >

TEXT_ Wolfgang Krieger

Prof. Dr. em. Wolfgang Krieger lehrte Neuere Geschichte an der Philipps-Universität Marburg und war Fellow der Universitäten Oxford und Harvard. Er ist Mitglied im „International Institute for Strategic Studies“ und des „Conseil scientifique de la recherche historique de la défense“ des französischen Verteidigungsministeriums sowie Mitbegründer der International Intelligence History Association. 2026 veröffentlichte er „Die Geschichte der Geheimdienste“.

KEY MESSAGES

- **Geheimdienste** erfüllen seit der Antike drei Kernaufgaben: Informationsgewinnung, Spionageabwehr und verdeckte Operationen.
- **Terrorismus, Cyberangriffe und hybride Kriegsführung** haben das klassische Bedrohungsbild grundlegend erweitert.
- **Die Illusion einer stabilen regelbasierten Ordnung** weicht einer konfliktreichen Welt rivalisierender Machtblöcke.
- **Europas Sicherheitsfähigkeit** leidet unter militärischen, geheimdienstlichen und politischen Defiziten – besonders in Deutschland.
- **Ohne Reformen, technologische Anpassung und strategische Klarheit** droht ein dauerhafter Verlust an Handlungsfähigkeit.

lich im Iran, in Russland, in China und in anderen Diktaturen sehen können.

Während die westlichen Geheimdienste im Ost-West-Konflikt in einem klar definierten politischen und internationalen Umfeld operierten, wurden sie nach 1990/1991 in rascher Folge mit neuen Aufgaben und Herausforderungen konfrontiert. Zunächst durch den islamistischen Terrorismus – man denke an die Terroranschläge in den USA, Frankreich, Israel, Großbritannien und Spanien, aber auch in der Türkei, in Russland, Kenia, Indien, Indonesien, Nigeria, im Irak und in vielen anderen Staaten. Manche Terroranschläge konnten verhindert, einige der Täter vor Gericht gebracht werden, doch die Erfolgsbilanz war insgesamt mager.

Innovationspartner dar, pflegt aber gleichzeitig mit den Kriegsmächten Russland und Iran eine enge Partnerschaft. Es kauft beispielsweise deren Erdöl, unter Umgehung internationaler Sanktionen, und liefert Waffen an sie. Somit ist klar, dass der islamistische Terrorismus nicht verschwunden ist. Er hat vielmehr unter der Führung des Iran eine neue Dimension angenommen.

Innenpolitisch ist in Europa die Sorge um die Bedrohung von Bürgerrechten durch Cyber-Angriffe und durch staatliche Überwachung von privater Kommunikation (Mobilfunk, Internet, Datenspeicher) keineswegs verschwunden. Zugleich fragt man sich, ob private Kommunikation überhaupt noch geschützt werden kann. Denn neben den Geheimdiensten sammeln auch Pri-

„Die regelbasierte Ordnung erweist sich als Illusion, weil sich die Großmächte dieser Logik nicht unterwerfen.“

Wolfgang Krieger

Dann, vor gut zehn Jahren, begann sich die Weltpolitik grundlegend zu wandeln. Man sprach nun von einer neuen „Weltunordnung“ (Carlo Masala) oder einer „Zeitenwende“ (Olaf Scholz). Seither geht es in den Geheimdiensten darum, die Absichten und Fähigkeiten von rivalisierenden Staaten sowie von kriegsbereiten feindlichen Staaten zu erkunden. Russland und China sind im UN-Sicherheitsrat nicht mehr um eine Verständigung mit der westlichen Seite bemüht, sondern bauen eine rivalisierende internationale Ordnung auf, der sich große Staaten wie Indien und Brasilien sowie zahlreiche kleinere bereits anschließen. Der russische Angriffskrieg in der Ukraine wird durch diese neue Koalition von Mächten unterstützt. Russland und China schließen Bündnisse mit Diktaturen wie dem Iran und Venezuela.

Es folgen zwei völlig unterschiedliche Kriege – in der Ukraine (seit 2022) und im Mittleren Osten (seit 2023). Aggressive Großmachtpolitik und islamistischer Terrorismus vermischen sich. Während Russland unter Wladimir Putin einen klassischen Eroberungskrieg führt, erfolgte der Überfall auf Israel durch die Hamas, eine nicht-staatliche Terrorgruppe. Hamas wird von Terrorgruppen wie der Hisbollah im Libanon und den jemenitischen Huthi unterstützt. Alle drei werden von der Islamischen Republik Iran finanziert, bewaffnet und gesteuert. China wiederum stellt für den Westen einen unverzichtbaren Handels- und

vatunternehmen in einem schwer vorstellbaren Umfang die Daten ihrer Kunden.

FÄHIGKEITSLÜCKEN

Angesichts dieser äußeren und inneren Bedrohungen, die hier nur stark verkürzt aufgeführt werden, ist deutlich, in welchem Ausmaß das Leben in unseren heutigen Wohlstandsgesellschaften vom Schutz durch staatliche Sicherheitsbehörden abhängt, also von Polizei, Militär und Geheimdiensten. Cyber-Angriffe können unsere «kritische Infrastruktur» lahmlegen, das heißt unsere Energieversorgung, Verkehrs- und Kommunikationssysteme, Fabriken, Banken, Krankenhäuser und vieles mehr.

Bei der Abwehr solcher Angriffe sind geheimdienstliche Fähigkeiten unerlässlich. Um die Gefahren rechtzeitig zu erkennen, braucht man geheimdienstliche Mittel, mit denen man global operieren kann und die weniger sichtbar sind als Polizei und Militär. Denn Angriffe aus dem Internet, Terrorangriffe, Waffen- und Menschenhandel werden im Geheimen vorbereitet oder ausgeführt. Sie müssen ohne Rücksicht auf Souveränitätsansprüche verbrecherischer Regime aufgeklärt werden.

Trotz dieser Umbrüche klammern sich europäische Regierungen an den Traum von einer „regelbasierten Ordnung“, in der Konflikte mit Hilfe von völkerrechtlichen Normen, Ver- ➤

trägen oder Institutionen geregelt werden. Doch das erweist sich als Illusion, weil sich China, Russland, Indien und andere Großmächte dieser Logik nicht unterwerfen. Die USA unter Präsident Donald Trump suchen neue Wege der Konfliktlösung und greifen dabei auf Praktiken der alten Großmachtpolitik zurück, mit denen militärische Gewalt angedroht oder eingesetzt wird, um regionale Interessenssphären abzusichern, vor allem in Lateinamerika und im Nordatlantik (beim Streit um Grönland). Sie initiieren jedoch auch neue Formen internationaler Kooperation, beispielsweise dem im Januar 2026 etablierten Board of Peace, das sich zunächst mit der Zukunft des Gaza-Territoriums befassen soll. Das Völkerrecht ist also nicht tot, aber es ist nur begrenzt wirksam.

Vom Niedergang der „regelbasierten Ordnung“ ist Deutschland in besonderer Weise betroffen, weil es nach 1990 seine Landesverteidigung nahezu aufgab und seine auswärtige Politik nur noch im Rahmen der Europäischen Union (EU) sowie der NATO definierte. Die deutsche Wirtschafts-, Finanz- und Technologiepolitik wurde an die EU delegiert, die Landesverteidigung an die nukleare Abschreckung der USA. Der Verteidigungshaushalt wurde auf ein Prozent der Wirtschaftsleistung heruntergefahren, von einstmalen fünf Prozent. Doch die EU wird in der neuen Weltordnung kaum ernst genommen, weil sie kein Drohpotential gegenüber Peking, Moskau oder Washington hat. Die USA verlangen eine selbständige konventionelle Verteidigungsfähigkeit der europäischen NATO-Mitglieder.

Auch die deutschen Nachrichtendienste weisen gravierende Fähigkeitslücken auf, die bis 2025 ignoriert wurden. Erst der Koalitionsvertrag vom 5. Mai 2025 enthielt eine offizielles Eingeständnis der politischen Versäumnisse und eine Festlegung auf eine Geheimdienstreform, die zumindest einige der juristischen Fesseln lockern und die Dienste schlagkräftiger machen soll. Ob es dazu kommt, bleibt ungewiss. Vor allem müssen sie sich an die Welt des Internets anpassen, denn es geht hier nicht nur um die

Übermittlung von Bild und Ton in alle Richtungen, sondern auch um die Kontrolle elektronisch gesteuerter Maschinen und technischer Systemen (Internet der Dinge). Was sich zunächst als ein großer Freiheitsgewinn und als technischer Fortschritt präsentierte, zeigte bald seine Schattenseiten. Kriminelle profitierten von den neuen Kommunikationsmöglichkeiten. Diktaturen wie China und der Iran manipulieren den Internetzugang.

HYBRIDER KRIEG

Heute verfügen viele Staaten über offensive Cyberfähigkeiten, allen voran die USA, Russland, China, Iran, Nordkorea, Großbritannien und Frankreich. Großbritannien veröffentlichte erstmals 2011 eine Cyber Security Strategy, Frankreichs Planungen begannen bereits mit dem Verteidigungsweißbuch von 2008. In Deutschland wurde erst 2017 eine Teilstreitkraft „Cyber und Informationsraum“ eingerichtet, jedoch ohne Befugnis für „offensive Operationen“.

Der gängige Begriff des «hybriden Krieges» beschreibt eine Vermischung militärischer Gewaltanwendung durch reguläre Streitkräfte mit Elementen einer verdeckten Aggression oder «irregulären Kriegführung», die von schwarzer Propaganda («fake news») bis zu Cyberangriffen auf die zivile Infrastruktur oder zum Einsatz irregulärer Kämpfer reichen. Dahinter stecken geheimdienstliche Apparate und ihre Methoden. Das Ziel ist, den Gegner wirtschaftlich, finanziell und vor allem psychologisch zu zermürben – durch gefälschte Bilder und Videos, oftmals perfektioniert durch Künstliche Intelligenz (KI).

Als eine weitere neuartige Form der Konfliktaustragung mit geheimdienstlichen Instrumenten gelten auch Wirtschafts- und Finanzsanktionen gegen Einzelpersonen im gegnerischen Staat. Diese Sanktionen erfordern eine präzise geheimdienstliche Ermittlung von Finanz- und Besitzstrukturen. Aus den USA ist bekannt, dass die Geheimdienst-Abteilung der Treasury (Finanzministerium) dafür zuständig ist. Dieses *Office of Intelligence* >

„Sanktionen gegen Einzelpersonen im gegnerischen Staat erfordern eine präzise geheimdienstliche Ermittlung von Finanz- und Besitzstrukturen.“

Wolfgang Krieger

and Analysis (OIA) wurde 2004 gegründet und gehört zu den 17 Geheimdiensten der U. S. Intelligence Community, ebenso wie das FBI im Justizministerium. Im Hintergrund arbeiten weitere US-Geheimdienste und mächtige Anwaltssozietäten («Law Firms») Hand in Hand, um möglichst hohe Geldstrafen auszuhandeln, an denen die Wirtschaftsanwälte prozentual und mit fetten Honoraren beteiligt sind.

Schuld auf die Regierungspolitik, die versucht habe, den Palästina-Konflikt «einzufrieren», bis er durch eine direkte Verständigung mit maßgeblichen arabischen Staaten an Bedeutung verlieren würde. Die bislang offengelegten Geheimdienstinformationen der israelischen Seite ergeben jedoch noch kein schlüssiges Bild.

Nicht zu bezweifeln ist, dass es sich beim 7. Oktober um eines der größten «intelligence failures» der Geschichte handelt – und

„Nicht zu bezweifeln ist, dass der 7. Oktober eines der größten Geheimdienstversagen der Geschichte war.“

Wolfgang Krieger

Am 7. Oktober 2023, dem jüdischen Feiertag Simchat Tora (Freude der Tora), stürmten 6000 Hamas-Kämpfer über die Grenze zwischen dem Gaza-Gebiet und Israel. Sie griffen eine große Zahl von jüdischen Siedlungen sowie die Teilnehmer eines Open-Air-Festivals an. Dabei ermordeten sie 1200 Männer, Frauen und Kinder. Zusätzlich gab es über 3400 Verwundete, weitere 250 Menschen wurden als Geiseln in das Gaza-Territorium verschleppt. Aus Gaza feuerten Hamas-Kämpfer gleichzeitig 4300 Raketen auf Israel.

Für die Geheimdienst-Interessierten lieferte der Hamas-Krieg zunächst ein großes Erstaunen, dass ein solcher Terrorangriff den Staat Israel völlig unvorbereitet treffen konnte. Dabei hatten die israelischen Geheimdienste immer wieder warnende Informationen erhalten. 2018 und 2022 erbeuteten sie Dokumente, die auf einen solchen Angriff explizit hindeuteten. Nach einem Untersuchungsbericht der IDF (Israel Defense Forces), veröffentlicht im Februar 2025, soll die Entscheidung zum Angriff im Mai 2023 gefallen sein.

INTELLIGENCE FAILURES

Hier sehen wir ein Erkenntnisproblem, das sich immer wieder findet, wenn wir ein geheimdienstliches Versagen zu analysieren haben. Zum einen wird dem Gegner die gleiche taktisch-strategische Logik zugesprochen, der man selbst in dessen Situation folgen würde; zum anderen nimmt man am liebsten Informationen zur Kenntnis, die in ein bereits existierendes Denkschema passen. Der Geheimdienstexperte Scott Ritter gab die Schuld einer KI-gestützten Methodik, unter Aufgabe traditioneller Wahrscheinlichkeitsanalysen. Israelische Militärexperten schoben die

zwar zugerechnet in Israel, das weltweit über die meiste Erfahrung im Kampf gegen den islamistischen Terrorismus verfügte, sowie unter Ministerpräsident Benjamin Netanyahu, der über weitaus mehr Erfahrung als Soldat und mit den Geheimdiensten verfügte als jeder andere westliche Regierungschef. Im verlustreichen Tunnelkrieg verlor Netanyahu keineswegs die größere Perspektive der vom Iran geführten Feinde aus den Augen. Schließlich kam es im September 2024 zu direkten Raketenangriffen der Huthi-Milizen im Jemen und im Oktober 2024 aus dem Iran selbst. Israel führte also einen Mehrfrontenkrieg, wobei die Geheimdienste eine wichtige Rolle spielten.

Am 17. und 18. September 2024 kam es im Libanon zu einem ebenso spektakulären wie neuartigen israelischen Angriff auf die Terrormiliz Hisbollah. Als Waffe diente eine große Zahl von Pagers, kleinen Funkgeräten und anderen elektronischen Geräten, die der Mossad gekauft, mit Sprengstoff präpariert sowie mit einer speziellen Software ausgestattet hatte, die es erlaubte, die Geräte per Funksignal zu zünden. Diese Pager wurden verdeckt an die Hisbollah verkauft. In einem einzigen Moment wurden sie zur Explosion gebracht, wobei etwa 2800 Hisbollah-Kämpfer verletzt und zwölf Personen getötet wurden. Am darauffolgenden Tag kam es zu einer ähnlichen Aktion mit Walkie-Talkies. Dabei gab es 450 Verletzte und 20 Tote.

Damit wurde die Hisbollah psychologisch gelähmt, weil ihr das große Ausmaß der feindlichen Unterwanderung vor Augen geführt wurde. Der Öffentlichkeit wurde zugleich die genaue Identität der Kämpfer bekannt, das heißt von Brüdern, Vätern und Söhnen, die oftmals ein vorgeblich braves Familienleben führten. >

Auf beiden Kriegsschauplätzen spielten Drohnen eine wichtige Rolle, insbesondere billige Modelle mit geringer Reichweite. Seit Beginn des Ukrainekrieges werden sie von beiden Seiten eingesetzt. Am 1. Juni 2025 kam mit der Operation «Spinnennetz» eine neue Variante dieser Drohneneinsätze ans Licht, als der ukrainische Militäргеheimdienst eine Anzahl von Lastwagen in das russische Staatsgebiet schmuggelte, einige davon mehrere Tausend Kilometer östlich der ukrainischen Grenze. Sie waren mit kleinen Drohnen beladen und konnten sich bis auf wenige Kilometer den Flughäfen der russischen Luftstreitkräfte nähern, um Duzende russischer Fernbomber zu zerstören.

Kurz darauf, in der Nacht vom 12. zum 13. Juni 2025, startete Israel im Iran einen massiven Luftangriff auf Atomanlagen, Produktionsstätten für Raketen und militärisch genutzte Gebäude. Es sollen 200 Militärmaschinen beteiligt gewesen sein. Hinzu kam eine Welle von Angriffen auf Einrichtungen der iranischen Luftverteidigung. Dabei gelang es den israelischen Geheimdiensten offensichtlich, diese Drohnen samt ihrem Bedienungspersonal vorab auf iranischem Boden zu positionieren und im gegebenen Moment zum Einsatz zu bringen. Nach diesen Vorbereitungen griffen am 21. / 22. Juni 2025 sieben amerikanische B-2-Tarnkappen-Bomber mehrere iranische Nuklearanlagen an. Insgesamt wurde im Iran eine Reihe hoher Militärs und führender Atomwissenschaftler getötet. Der am 24. Juni verkündete Waffenstillstand markierte eine Zeitenwende für die iranisch-geführten Stellvertreterkriege im Mittleren Osten.

Zweifellos beruhten diese israelisch-amerikanischen Angriffe auf intensiven, monatelangen, vermutlich sogar jahrelangen Vorbereitungen der Geheimdienste. In einem Fall gelang es, einen Besprechungstermin für Kommandeure zu fingieren, um dann mehrere von ihnen gezielt auszuschalten. Weiterhin sollen DNA-Proben, gefälschte Software, Cyberangriffe und KI-gestützte Überlistung von Gesichtserkennung zum Einsatz gekommen sein. Die iranische Justizbehörde nahm 2000 vermutete Spione

fest und schob massenhaft afghanische Flüchtlinge ab, die als illoyal betrachtet wurden. Schließlich ist die Geheimoperation gegen den venezolanischen Diktator Nicolás Maduro am 3. Dezember 2026 zu nennen, die ebenfalls auf umfangreichen Vorarbeiten der (amerikanischen) Geheimdienste beruhte.

Aufgrund der strengen Geheimhaltung lässt sich nicht genau sagen, wie die europäischen Geheimdienste auf diese spektakulären Operationen reagieren. Aber wir kennen ihre neuen Aufgaben und ihre Mittel. Es liegt nun an den europäischen Regierungen, ihre Geheimdienste bestmöglich auszustatten, um sie in ihrer Außen- und Sicherheitspolitik optimal einzusetzen. ■

Es liegt an den europäischen Regierungen, ihre Geheimdienste bestmöglich auszustatten, um sie in ihrer Außen– und Sicherheitspolitik optimal einzusetzen.

Wolfgang Krieger

„Vertrauen ist zentral“

Wenn Machtinteressen Wahrheit verdrängen und Kontrolle versagt, verliert Intelligence ihre demokratische Legitimität. Der US-Intelligence- und Sicherheitsexperte Loch K. Johnson über Donald Trump, Intelligence-Kooperation und die moralische Pflicht von Geheimdiensten, die Wahrheit zu verteidigen.

Loch Johnson, wie beurteilen Sie die jüngste US-Militäraktion in Venezuela aus nachrichtendienstlicher Perspektive?

Loch K. Johnson: Ich halte sie für eine absolute Schande. Wer hat die Vereinigten Staaten zum Rächer der Welt ernannt, der die Regierungen anderer Länder zurechtrückt? Das ist nicht ihre Aufgabe. Wenn ich auf Venezuela blicke, fühle ich mich sehr stark an frühere verdeckte Operationen erinnert, insbesondere an Chile unter Salvador Allende. Damals drängten Unternehmensinteressen auf Interventionen, um Vermögenswerte zu schützen – nicht die Demokratie. Meine Hypothese ist, dass es heute ähnlich ist: US-Ölinteressen haben Investitionen in Venezuela verloren und politischen Druck ausgeübt. Das wirkt weniger wie Außenpolitik und mehr wie unternehmerische Macht, die staatliches Handeln lenkt – genau wie damals in Chile.

Sie kritisieren auch den amtierenden Präsidenten sehr scharf.

Weil wir es mit einem Präsidenten zu

tun haben, der grundlegende verfassungsrechtliche Prinzipien ignoriert. Die zentrale Einsicht der US-Verfassung war, dass Macht gefährlich ist und daher durch Checks and Balances begrenzt werden muss. Versagen diese Schutzmechanismen, können Führungspersonen sehr schnell autoritär werden. Hier sehen wir einen Präsidenten, der Gesetze bricht, Fakten missachtet und rechtsstaatliche Verfahren verweigert – der falsche Behauptungen aufstellt und Tötungen zulässt.

Aus rein geheimdienstlicher Perspektive war die Operation ein Erfolg...

Ja – und genau darin liegt die Ironie. Militärisch war sie beeindruckend. Berichte deuten darauf hin, dass die CIA die Gewohnheiten des venezolanischen Präsidenten äußerst detailliert verfolgt hat, bis hin zu seinem Tagesablauf. Die Koordination von Schiffen, Flugzeugen und Truppen ohne US-Opfer zeugt von hoher operativer Kompetenz. Aber wie viele Zivilisten sind dabei ums Leben gekommen? Technisch „erfolgreiche“ >



INTERVIEW_ Loch K. Johnson

Loch K. Johnson ist emeritierter Regents Professor für Public and International Affairs an der School of Public and International Affairs (SPIA) der University of Georgia. Er ist Autor oder Herausgeber von mehr als vierzig Büchern, darunter zuletzt *The Oxford Handbook of National Security Intelligence* (Oxford University Press, 2025) sowie *National Security Intelligence*, 3. Auflage (Polity, 2024).

KEY MESSAGES

- **Die US-Maßnahmen in Venezuela** folgen der Logik verdeckter Interventionen des Kalten Krieges, weniger getrieben von demokratiepolitischen als von wirtschaftlichen Interessen.
- **Geheimdienstliche Operationen** können technisch erfolgreich sein und zugleich moralisch wie politisch zerstörerisch wirken.
- **Politisierung und Missachtung von Kontrolle** schwächen die Wirksamkeit von Intelligence und untergraben das Vertrauen von Partnern.
- **KI wird Sammlung und Analyse von Intelligence** grundlegend verändern, kann jedoch menschliches Urteilsvermögen, Ethik und Verantwortlichkeit nicht ersetzen.
- **In Demokratien** muss Intelligence nicht nur physische Sicherheit schützen, sondern auch Wahrheit, Vertrauen und eine gemeinsame Wirklichkeitsbasis.

Intelligence kann dennoch moralisch zutiefst verwerflich sein.

Über Venezuela hinausgehend: Wie beeinflussen die aktuellen geopolitischen Verschiebungen den Auftrag strategischer Intelligence?

Das größte Problem ist nicht die Geopolitik – es ist die Führung. Wir haben einen Präsidenten, der Intelligence nicht versteht, das President's Daily Brief nicht liest und Briefings auslässt. Das ist erschütternd. Die USA geben über 100 Milliarden Dollar jährlich für Intelligence aus, doch ihr Hauptadressat ignoriert sie. Berater filtern das Verbleibende ideologisch, wählen selektiv aus, was in ihre Agenda passt, und untergraben damit den Kernzweck von Intelligence.

Schadet die Trump-Administration der internationalen Intelligence-Kooperation?

Ja, leider tut sie das. Kontakte im Vereinigten Königreich, in Deutschland und anderen verbündeten Staaten nehmen die USA zunehmend als unberechenbar und weniger vertrauenswürdig wahr. Traditionell war Five Eyes eines der robustesten Intelligence-Kooperationsformate der Welt. Doch selbst innerhalb dieses Kreises wächst inzwischen das Misstrauen. Verbündete sind zunehmend unsicher, wie sicher gemeinsam geteilte Intelligence innerhalb der Vereinigten Staaten tatsächlich behandelt wird.

Welche Risiken entstehen daraus?

Enorme Risiken. Bei Human Intelligence (HUMINT) geht es um reale Menschen, deren Identitäten in streng geheimen Berichten auftauchen können; bei einer Weitergabe drohen ihnen Haft oder Hinrichtung. Sensible technische Details – Satellitenumlaufbahnen, Abhörmethoden – sind nach einer Offenlegung unwiederbringlich verloren. Meine britischen Kontakte berichten von gro-

ßer Sorge, dass die Rücksichtslosigkeit der US-Führung Schutzmechanismen geschwächt hat, die früher zuverlässig funktioniert haben.

Das Problem ist also nicht nur politisch, sondern strukturell?

Ganz genau. Die Welt ist groß. Kein einzelnes Land – nicht einmal die Vereinigten Staaten – kann alles allein abdecken. Intelligence-Kooperation ist unverzichtbar. Deutschland hat insbesondere aufgrund seiner Geschichte eine ausgeprägte Sensibilität für Bürgerrechte, die ich sehr respektiere. Diese Erfahrung macht deutsche Nachrichtendienste besonders sorgfältig im Umgang mit der Gewinnung und Weitergabe von Informationen. Wenn Zweifel entstehen, ob Intelligence in Washington ausreichend geschützt wird, werden deutsche Dienste zwangsläufig zögern. Und wenn Vertrauen erst einmal erodiert, ist es außerordentlich schwer, es wiederherzustellen.

Sie haben Deutschlands Ansatz in der nachrichtendienstlichen Zusammenarbeit erwähnt. Haben Sie dazu persönliche Anmerkungen?

Ja. Ich habe Angela Merkel immer sehr bewundert. Als bekannt wurde, dass die NSA sie ausspionierte, reagierte sie öffentlich mit den Worten: „Wenn sie wissen wollen, was ich denke, sollen sie mich einfach fragen.“ Ich fand das großartig – besonnen, würdevoll und prinzipientreu. Das brachte etwas Wesentliches demokratischer Führung und von Vertrauen auf den Punkt. Intelligence sollte der Demokratie dienen, nicht sie untergraben. Und derzeit ist dieses Gleichgewicht deutlich gestört.

Was bereitet Ihnen die größten Sorgen?

Die Normalisierung von Rechtsbruch. Wenn Aufsichtsgesetze ignoriert werden, wenn Verbündete nicht konsultiert

werden, wenn Intelligence politisiert oder fahrlässig behandelt wird, bleibt der Schaden nicht auf eine einzelne Operation oder ein einzelnes Land begrenzt. Er breitet sich aus. Und wenn Vertrauen – Vertrauen in die Verfassung, Vertrauen unter Verbündeten, menschliches Vertrauen – verloren geht, wird Intelligence selbst deutlich weniger wirksam.

Wie können westliche Verbündete auf diese Situation reagieren? Gibt es eine klare Strategie?

Ich glaube fest an Dialog und offene Zusammenarbeit. Nach Jahrzehnten gemeinsamer Arbeit kennen sich Nachrichtendienstler in Deutschland, den USA und anderen westlichen Staaten sehr gut. Gerade deshalb sind gegenseitige Versicherung und engere Kooperation entscheidend. Auf der operativen Ebene sind Vertrauen und persönliche Beziehungen wichtiger denn je – und diese Bemühungen werden ganz offensichtlich fortgesetzt.

Kann die Krise zu einer Erneuerung führen – etwa zu neuen Formen nachrichtendienstlicher Kooperation oder sogar zu einem europäischen Intelligence-Hub?

Das sind große Ideen und es lohnt sich, sie zu verfolgen. Aber wir müssen ehrlich über die menschliche Natur reden. Wir sind schlecht im Lernen, wir vermeiden Kriege nicht, und wir unterschätzen, wie entscheidend die Zusammenarbeit unter Demokratien ist. Demokratie ist fragil und selten – vielleicht erfüllen nur 25 von 200 Staaten diese Kriterien. Dennoch bleibt die Kooperation unzureichend. Five Eyes ist wichtig, aber nicht genug. Demokratien brauchen breitere und tiefere Intelligence-Partnerschaften, auch mit Ländern wie Deutschland, um dem wachsenden Druck standzuhalten. >

Was sehen Sie als die zentrale Aufgabe von Intelligence – insbesondere strategischer Intelligence – in demokratischen Gesellschaften?

Ich glaube, die Kernaufgabe von Intelligence ist Schutz: Frühwarnung, damit politische Entscheidungsträger nicht von Katastrophen wie Pearl Harbor oder 9/11 überrascht werden. Darüber hinaus leisten Dienste einen wichtigen Beitrag bei Themen wie Umweltzerstörung, Pandemien, wirtschaftlicher Instabilität und Migrationsbewegungen. COVID hat gezeigt, wie entscheidend Frühwarnung sein kann. Dennoch bleibt der zentrale Auftrag die Verhinderung nationaler Vernichtung – sicherzustellen, dass wir nicht plötzlich durch Nuklearraketen großer Mächte ausgelöscht werden.

Stimmen Sie zu, dass eine der Kernaufgaben von Intelligence in demokratischen Gesellschaften darin besteht, Wahrheit oder zumindest ein gemeinsames Wirklichkeitsverständnis zu schützen?

Ja, absolut. Diese Aufgabe ist beinahe ebenso wichtig wie der Schutz von Gesellschaften vor physischer Zerstörung. Nachrichtendienste – russische, chinesische, aber auch westliche – haben Informationen manipuliert. Russland ist dabei besonders aggressiv vorgegangen, etwa durch die Verbreitung falscher Behauptungen über AIDS, COVID und andere Themen. Solche Narrative gewinnen durch Wiederholung und Propaganda an Wirkung. Mit dem Fortschritt von KI wird sich dieses Problem weiter verschärfen.

Welche zentrale Rolle sollten Nachrichtendienste dabei spielen?

Idealerweise sollten amerikanische und westliche Nachrichtendienste genau das tun, was Sie eben angedeutet haben: Sie sollten helfen, demokratische

Gesellschaften darüber aufzuklären, was real ist und was nicht – und Bürgerinnen und Bürger dabei unterstützen, ein belastbares Wirklichkeitsverständnis zu entwickeln. Fairerweise muss man sagen, dass dies bereits teilweise geschieht. Nachrichtendienste warnen vor Desinformationskampagnen, ausländischer Einflussnahme und manipulierten Narrativen. Aber wir könnten das deutlich besser machen. Demokratie hängt von einer informierten Öffentlichkeit ab.

„Geheimdienste haben die moralische Pflicht, die Wahrheit zu verteidigen.“

Loch K. Johnson

Wenn Bürger Fakten nicht mehr von Fiktion unterscheiden können, geraten Wahlen, öffentliche Debatten und demokratische Verantwortlichkeit ins Wanken.

Das würde aber auch bedeuten, dass Nachrichtendienste selbst keine Manipulation betreiben sollten.

Ganz genau. Das ist die ethische Grenze. Es gibt jedoch Ausnahmen. Wenn man etwa eine Operation wie die Landung in der Normandie im Zweiten Weltkrieg plant, will man den Gegner unbedingt täuschen. Man möchte, dass er glaubt, man lande an Punkt A, während man tatsächlich bei Punkt B landet. In Kriegszeiten ist Täuschung nicht nur legitim, sondern notwendig. Das unterscheidet sich jedoch grundlegend von alltäglicher Informationsmanipulation, die sich gegen zivile Bevölkerungen richtet – insbesondere innerhalb von Demokratien. Der Öffentlichkeit

oder verbündeten Gesellschaften bewusst falsche Informationen zu liefern, untergräbt Vertrauen. Und wenn Vertrauen einmal verloren ist, lässt es sich nur sehr schwer wiederherstellen.

Die Gefahr ist also nicht nur extern, sondern auch intern?

Die größte langfristige Bedrohung für Demokratien ist möglicherweise nicht militärische Gewalt, sondern der Verlust eines gemeinsamen Wirklichkeitsverständnisses. Deshalb haben Geheim-

dienste eine moralische Pflicht, Wahrheit zu verteidigen – auch dann, wenn sie unbequem ist. Wird Intelligence zu Propaganda, hört sie auf, Demokratie zu schützen, und beginnt, sie zu untergraben – eine der gravierendsten Herausforderungen unserer Zeit.

Wie verändert KI das Intelligence-Geschäft, sowohl bei Sammlung und Analyse als auch hinsichtlich neuer Bedrohungen?

KI ist geradezu explodiert; Unternehmen und Nachrichtendienste investieren Milliarden. Im Intelligence-Zyklus kann sie Entscheidungsträgern helfen, Ressourcen rationaler zu verteilen und datenkompetenter zu werden. Doch Ideologie überlagert häufig Fakten. In hochrangigen Sitzungen bestimmen persönliche Obsessionen Prioritäten – unabhängig von der Evidenz. Selbst die besten KI-gestützten Analysen können ignoriert oder verzerrt werden.

Können Sie das näher erklären?

>

KI kann Entscheidungen informieren, aber menschliche Voreingenommenheit nicht ausgleichen. Ich habe an solchen Sitzungen teilgenommen. Menschen bringen ihre Ideologien und Fixierungen mit. Nehmen Sie etwa Marco Rubio: Er ist gleichzeitig Außenminister und Nationaler Sicherheitsberater – was absurd ist, niemand kann beide Aufgaben sinnvoll erfüllen. Und was bringt er in diesen Sitzungen ständig vor? Kuba, Kuba, Kuba. Russland, China, Kuba. Kuba ganz oben auf der Prioritätenliste. Kuba? Wirklich?

Welche Rolle spielt KI bei der Informationsgewinnung?

Hier hat KI ein enormes Potenzial. Denken Sie etwa an die Jagd auf Osama bin Laden. Wir wussten, dass er etwa zwei Meter groß war. Damals flogen Drohnen über Afghanistan und Pakistan. Heute könnte man diese Drohnen mit KI-Systemen ausstatten, die gezielt Personen dieser Größe identifizieren, Gesichtszüge abgleichen und Bewegungsmuster verfolgen. Solche automatisierten Erkennungssysteme könnten genutzt werden, um Zielpersonen festzunehmen – oder, deutlich bedrohlicher, um sie zu töten. KI kann die Fähigkeiten der Informationsgewinnung massiv erweitern, wirft aber auch tiefgreifende ethische Fragen auf.

Und die Analyse?

Hier könnte KI ihren größten Mehrwert entfalten. Sie kann riesige Informationsmengen sehr viel schneller durchsuchen als jedes menschliche Analysteam. Vor 9/11 waren Daten über zahlreiche Behörden verteilt, und niemand hatte das vollständige Lagebild – ein katastrophales Versagen der All-Source-Intelligence. KI könnte helfen, Daten behördenübergreifend zu integrieren. Doch das Risiko

bleibt: Wenn die Daten fehlerhaft, verzerrt oder unvollständig sind, verarbeitet KI diese Mängel lediglich schneller.

Was ist mit der Weitergabe von Intelligence an politische Entscheidungsträger?

Hier bin ich am pessimistischsten. KI mag Intelligence-Produkte verbessern, doch Entscheidungsträger befassen sich nur selten ernsthaft mit ihnen. Joe Nye (ehem. US-Präsidentenberater und Politikwissenschaftler, Anm.) sagte mir einmal, er habe täglich acht Minuten Zeit, um Intelligence zu lesen. Acht Minuten. Wenn Joe Nye acht Minuten hatte – was heißt das dann für Leute wie Marco Rubio oder Pete Hegseth? Wie viel Zeit investieren sie wirklich in eine ernsthafte Auseinandersetzung mit Intelligence? KI kann dieses Problem nicht lösen. Schlimmer noch: Ideologie wirkt wie Scheuklappen. Viele Führungspersonen wissen bereits, was sie tun wollen, und ignorieren Intelligence, ob menschlich oder KI-gestützt, sobald sie ihren Überzeugungen widerspricht.

KI wird also Intelligence-Versagen nicht einfach beheben.

Ganz genau. KI kann die Analyse erheblich verbessern, doch menschliche Triebe – Ego, Ideologie, politische Interessen – werden weiterhin viele Entscheidungen bestimmen. KI ist besonders stark in der Skalierung: Sie kann globale Medien in Minuten auswerten und Muster erkennen, die Menschen übersehen würden. Das ist ihr eigentlicher Wert. Aber sie unterstützt Urteilsbildung – sie ersetzt sie nicht.

Wird sich Intelligence zukünftig stärker auf offene Quellen stützen?

Absolut. Open-Source-Intelligence ist deutlich ausgereifter geworden und bildet heute den Ausgangspunkt jeder Analyse. Ich sehe Intelligence als eine Art Puzzle: Offene Quellen liefern viele

Teile, aber einige fehlen immer. Ein Beispiel: Präsident Clinton fragte mich einmal, ob China M-6-Raketen an Pakistan verkauft. Offene Quellen lieferten selbst nach Wochen kaum Hinweise. Erst klassifizierte Satellitenbilder – die zeigten, wie chinesische Frachter Raketenkomponenten in Karachi entladen – lieferten den entscheidenden Beweis. Ohne geheime Intelligence wäre meine Bewertung gescheitert.

Geheimhaltung wird also immer eine Rolle spielen?

Ja. Vor allem Human Intelligence. Stellen Sie sich vor, man rekrutiert einen Agenten innerhalb des russischen oder chinesischen Nachrichtendienstes – jemanden, der mit Putin oder Xi im selben Raum sitzt. Diese Person kann Fragen stellen, Absichten direkt hören. Ein Freund von mir sagte einmal: Technische Intelligence kann den Baum fotografieren. Human Intelligence kann den Baum schütteln, sodass der Apfel abfällt. Das ist der Unterschied. Solchen Zugang hat man selten – aber wenn man ihn hat, ist er unbezahlbar.

Wie wird das Gleichgewicht aussehen?

Open-Source-Intelligence wird weiter an Bedeutung gewinnen. KI wird helfen, sie schneller und besser auszuwerten. Doch Geheimhaltung – Satelliten, Signals Intelligence, menschliche Quellen – bleibt unverzichtbar. Intelligence wird immer eine Mischung aus Sichtbarem und Verborgenen, aus Automatisierung und menschlicher Arbeit sein. Und die größte Herausforderung wird nicht die Technologie sein, sondern politische Entscheidungsträger dazu zu bringen, zuzuhören.

Wenn wir auf KI, technologische Beschleunigung und das menschliche Unvermögen blicken, Wahrheit zu erfassen: Welche Rolle spielen Zeit und Geschwindigkeit? >

Diese Maschinen sind außerordentlich hochentwickelt. Ich spiele ständig Schach gegen Bots und habe großen Respekt vor ihnen. Sie sind schnell, und Geschwindigkeit ist eine ihrer größten Stärken. Doch was ihnen fehlt – zumindest bislang – sind Instinkte. Und Sie haben recht: Menschliche Instinkte können langsam sein. Aber genau sie unterscheiden uns von diesen beeindruckenden Maschinen. Wir können KI nutzen, um Daten zu sammeln, riesige Informationsmengen zu durchsuchen und Muster zu erkennen. Das ist enorm wertvoll. Wir wissen bereits, dass Maschinen Schachweltmeister schlagen, juristische Staatsexamina bestehen und Komplexität jenseits menschlicher Fähigkeiten verarbeiten können. In

Katastrophe geführt hat. Diese gelebte Erfahrung ist von enormer Bedeutung.

Geschwindigkeit muss kein Vorteil sein.

Ganz genau. Geschwindigkeit kann gefährlich sein. Demokratien sind bewusst langsam angelegt – sie diskutieren, wägen ab und zögern – und genau diese Langsamkeit ist ein Schutzmechanismus. Viele Systeme scheitern nicht an Verzögerung, sondern daran, zu schnell zu handeln, ohne Reflexion oder Ethik. KI beschleunigt Informationsflüsse und Entscheidungsdruck, doch menschliches Urteilsvermögen braucht Zeit. Wenn Technologie unsere Fähigkeit zur Reflexion überholt, geraten Demokratien in Gefahr.

Welche Rolle spielt Vertrauen im Zusammenhang mit Intelligence und KI?

„Wenn Technologie Reflexion überholt, geraten Demokratien in Gefahr.“

Loch K. Johnson

einem technischen Sinn sind sie „intelligent“. Aber sie haben kein Gewissen. Und das ist entscheidend. Manche glauben zwar, Maschinen könnten eines Tages moralisch autonom werden – und wenn das geschieht, haben wir ein ernstes Problem. Vorerst jedoch sind wir weiterhin auf menschliches Urteilsvermögen angewiesen. Das wirft eine zentrale Frage auf: Wem vertrauen Sie? Einem schnellen, aber undurchsichtigen Algorithmus – oder einer erfahrenen Amtsträgerin mit jahrzehntelanger Krisenerfahrung, Urteilsfähigkeit und Gewissen? Ich würde dem Menschen vertrauen. Sie erinnert sich an frühere Fehler, erkennt Muster und kann benennen, was funktioniert hat – oder in die

Vertrauen ist zentral. Ich habe erlebt, dass politische Entscheidungsträger fragen: „Woher wissen Sie das?“ Wenn die Antwort lautet, dass es sich um eine geschützte menschliche Quelle handelt, kann man die Belege nicht offenlegen – und das Vertrauen sinkt. Legt man hingegen Satellitenbilder auf den Tisch, die zeigen, wie Raketen in Karachi entladen werden, ist das konkret und überzeugend. Menschen vertrauen dem, was sie sehen und überprüfen können. Deshalb begegnet man KI-Ergebnissen oft mit Skepsis: Die Prozesse sind intransparent, die Schlussfolgerungen nicht leicht nachvollziehbar.

Gilt diese Skepsis speziell gegenüber KI?

Sehr sogar. Viele Geheimdienstler –

und noch mehr politische Entscheidungsträger – vertrauen KI-Systemen nicht vollständig. Und ehrlich gesagt haben sie allen Grund zur Vorsicht. KI kann ein mächtiges Werkzeug sein, hat bislang aber gravierende Schwächen. Sie macht Fehler. Manchmal macht sie sehr viele davon. Wenn eine Maschine falsch liegt, kann sie das sehr schnell und in enormem Maßstab tun. KI kann menschliches Urteilsvermögen also unterstützen, aber nicht ersetzen. Zumindest noch nicht – und vielleicht auch niemals in der Weise, wie manche Technologen es sich vorstellen.

Wie hängt das mit dem Aufstieg und Niedergang von Zivilisationen zusammen?

Zivilisationen steigen auf, wenn sie Innovation mit Weisheit in Einklang bringen. Sie fallen, wenn Geschwindigkeit das Urteilsvermögen überholt. Demokratie ist besonders fragil, weil sie auf Vertrauen, einem gemeinsamen Wirklichkeitsverständnis und moralischer Selbstbegrenzung beruht. All das lässt sich nicht automatisieren. Es braucht Zeit, Erinnerung und Gewissen. Wenn wir Systemen, die wir nicht verstehen – und die keine moralische Verantwortung tragen –, zu viel Autorität übertragen, riskieren wir, unseren eigenen Niedergang zu beschleunigen. Intelligence ist im tiefsten Sinne keine Frage von Geschwindigkeit oder Daten. Sie ist eine Frage des Urteils.

Bleibt Intelligence also in einem philosophischen Sinn menschlich?

Ja. Maschinen können uns helfen, mehr zu sehen, mehr zu wissen und mehr zu verarbeiten. Aber Weisheit – zu wissen, was mit diesem Wissen zu tun ist – bleibt eine menschliche Verantwortung. Und wenn Demokratien das vergessen, wird sie keine noch so fortgeschrittene künstliche Intelligenz retten. >

Wie beurteilen Sie die Macht von Big Tech im Bereich Daten und KI? Kann man Unternehmen wie Google oder Amazon als eine Art Geheimdienste begreifen?

Ja – und genau das bereitet mir große Sorgen. Deutsche verstehen aufgrund ihrer Geschichte die Gefahren einer Überwachungsgesellschaft sehr gut. Solche Technologien könnten eine Welt schaffen, in der es kein Entkommen mehr gibt, insbesondere für Andersdenkende. In entstehenden autoritären Systemen könnte KI-gestützte Überwachung Oppositionelle identifizieren, verfolgen und inhaftieren, noch bevor Widerstand entsteht. Intelligence war immer gefährlich, wenn sie missbraucht wurde; in Kombination mit KI und massenhafter Datensammlung vervielfacht sich dieses Risiko.

Die Bedrohung ist also nicht nur staatlich, sondern auch privatwirtschaftlich?

Unternehmen sind schon für sich genommen mächtig genug – doch nun gewinnen sie zusätzlich beispiellose Überwachungsfähigkeiten, wirtschaftlichen Einfluss und politische Macht, verpackt in die Sprache technologischen Fortschritts. Diese Konzentration von Macht sollte jeden beunruhigen, dem an Demokratie gelegen ist.

Was ist aus Ihrer jahrzehntelangen Erfahrung die wichtigste menschliche Fähigkeit für die geheimdienstliche Arbeit?

Wenn ich mit einem einzigen Wort beginnen müsste, wäre es Ehrlichkeit – ein tiefes, kompromissloses Bekenntnis zur Wahrheit, egal wie unbequem sie ist. Das ist Objektivität. Zweitens braucht man tiefgehende Fachkompetenz: gut ausgebildete Fachleute, die ihr Themengebiet wirklich verstehen. Drittens ist internationale Erfahrung entscheidend – Sprachen, Reisen, kulturelle Kompetenz. Mitarbeiter, die im Ausland echte Beziehungen aufbauen,

berichten präziser und können wesentlich effektiver kooperieren.

Und wenn Sie sich auf eine einzige Eigenschaft festlegen müssten?

Ehrlichkeit und Objektivität – vor allem anderen. Und das ist schwierig. Stellen Sie sich vor, Sie betreten das Oval Office und sagen zum Präsidenten: „Sie liegen völlig falsch. Das sind die Fakten.“ Das könnte das Ende Ihres Zugangs bedeuten. Es könnte Ihrer Karriere schaden oder sie sogar zerstören. Deshalb besteht ständig die Versuchung, zum Jasager zu werden – Führungspersonen das zu sagen, was sie hören wollen.

Gibt es diese Eigenschaften heute noch in den Nachrichtendiensten?

Ja, die gibt es. Ich kenne viele Nachrichtendienstmitarbeiter in den USA, in Deutschland und im Vereinigten Königreich, die genau diese Eigenschaften verkörpern: objektiv, hervorragend ausgebildet, kulturell versiert und der Wahrheit verpflichtet. Während politische Ernennungen an der Spitze dazu neigen können, Führungspersonen gefallen zu wollen, sind etwa 98 Prozent der Mitarbeitenden darunter hochprofessionell. Die eigentliche Herausforderung besteht darin, ihre Expertise durch politische Barrieren hindurch in Entscheidungen einfließen zu lassen.

Gibt es etwas, das Ihnen Hoffnung macht?

Ganz allgemein spüre ich ein Erwachen in den Vereinigten Staaten. Viele Menschen beginnen zu erkennen, dass die amerikanische Demokratie in ernsthaften Schwierigkeiten steckt. Es gab zuletzt Wahlen – in Virginia und anderswo –, bei denen Republikaner verloren haben. Das spiegelt wider, dass Menschen sagen: „Genug. Wir haben genug von MAGA und diesem Unsinn.“ Ironischerweise habe ich an Trump früher eine Sache bewundert: seine

Kritik an endlosen Kriegen. Er sagte, die USA seien in zu viele ausländische Konflikte verwickelt und müssten damit aufhören. Ich dachte damals: „Absolut richtig.“ Und jetzt sehen Sie ihn – unüberlegte militärische Aktionen, genau das, was er einst kritisiert hat.

Ihr abschließender Gedanke?

Vor allem Dankbarkeit. Ich fühle mich geehrt und freue mich sehr über dieses Gespräch. Dialoge wie dieser – offen, ehrlich und transnational – sind genau das, was mir Hoffnung gibt.

Dann bringen wir Sie einmal nach München...!

Sehr gerne. Bringen Sie mich nach München, wir trinken ein Bier, und dann sage ich Ihnen, was ich *wirklich* denke. ■

Architektur des Vertrauens

Deutschland steht unter wachsendem Druck hybrider Angriffe. Um handlungsfähig zu bleiben, braucht es leistungsfähige Nachrichtendienste und eine Entscheidungsarchitektur, die Erkenntnisse bündelt und nutzt.

Die Sicherheitslage Deutschlands ist prekär, und es gibt wenig Gründe, eine zukünftige Verbesserung zu erwarten – im Gegenteil. Deutschland steht im Fadenkreuz jener Mächte von innen und außen, die unsere Demokratie, unseren gesellschaftlichen Zusammenhalt und unseren Beitrag zu Verteidigung eines starken und eigenständigen Europas untergraben wollen.

Schon heute sind wir Cyberangriffen und Akten der Sabotage gegen kritische Infrastruktur ausgesetzt. Die Attacken staatlicher Akteure haben in den letzten Jahren stark zugenommen, sie sind komplexer geworden in ihrer Konzeption und Durchführung – und gefährlicher für Leib und Leben von Bürgern. Die Grenzen zwischen staatlichen Akteuren, terroristischen Gruppen und organisierten Verbrechen verschwimmen zunehmend, da insbesondere Russland nach der Ausweisung vieler seiner Agenten andere Handlanger rekrutiert hat.

Russland bedient sich aus der gesamten Werkzeugkiste je nach Kosten-Nutzenabwägung und unabhängig von völkerrechtlichen Verpflichtungen, um seine Ziele zu erreichen: von der Verbreitung gefälschter Videos über Friedrich Merz im Bundeswahlkampf über Drohnenflüge in der Nähe von Flughäfen und militärischen Einrichtungen bis zu Brandbomben in DHL-Flugzeugen oder gar nuklearen Drohungen. Dabei gilt es, zwischen den unmittelbaren Schäden und den intendierten Wirkungen zu unterscheiden. Russland geht es vor allem um die Schädigung des Vertrauens der Bürger in Staat und Regierung, um die Stärkung der Kräfte, die ein Ende von EU und NATO wollen, sowie um die Schwächung der Widerstands- und Mobilisierungsfähigkeit der Gesellschaft insgesamt. >

TEXT_ Christoph Meyer &

Daniel Neumann

Prof. Dr. Christoph Meyer ist Professor für Europäische und Internationale Politik am King's College London. Seit über 15 Jahren forscht er zu Frühwarnung, strategischer Überraschung und Lernen aus Krisen. Zu seinen Büchern zählen *Warning about War* (2020) sowie *Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise* (2023).

PhD Dr. Daniel Rainer Neumann ist Politikwissenschaftler mit Schwerpunkt Intelligence Studies und Assistenzprofessor am Institute for Security and Global Affairs der Universität Leiden. Er forschte zur Unterstützung der Gemeinsamen Außen- und Sicherheitspolitik der EU durch die Nachrichtendienste der Mitgliedsstaaten.

KEY MESSAGES

- **Deutschlands Sicherheitslage** verschlechtert sich durch hybride Angriffe
- **Leistungsfähige Nachrichtendienste** sind zentral für Prävention, Attribution und Abschreckung.
- **Das Potenzial der Dienste** wird bisher zuwenig genutzt.
- **Reformen** müssen Analyse, Koordination und Nutzung von Intelligence in politischen Entscheidungen stärken.
- **Neben Gesetzen** braucht es Investitionen, europäische Kooperation und einen kulturellen Wandel.

DER WERT DER NACHRICHTENDIENSTE

Während im kalten Krieg extremistische Gruppen und Parteien von KGB und der Stasi direkt und indirekt unterstützt wurden, sieht sich Deutschland mit einer neuen Realität konfrontiert. Heute unterstützen nicht nur Russland und China diese Akteure, sondern auch Teile der US-amerikanischen MAGA-Bewegung sowie mit ihr ideologisch assoziierte Unternehmen und milliardenschwere Unternehmer.

In der Zukunft ist eine weitere Verschärfung dieser Bestrebungen zu erwarten – und das Szenario des Spannungs- und Bündnisfalls ist ebenfalls deutlich wahrscheinlicher geworden. Russland und China wollen die Grenzen des Willens und der Fähigkeit von NATO und der USA durch ihre strategische und taktische Kooperation testen und letztlich überwinden.

„Wir brauchen die Dienste für die Abschreckung feindlicher Akteure.“

Christoph Meyer und Daniel Neumann

In dieser Sicherheitslage ist der Wert und die Notwendigkeit leistungsfähiger Nachrichtendienste immens gestiegen – und würde im Bündnisfall noch weiter steigen: Sie werden gebraucht, um mögliche Attacken zu antizipieren und damit entweder zu vereiteln oder die möglichen Schäden drastisch zu verringern – wie es etwa der Ukraine bei der Abwehr des russischen Entführungsangriffs im Februar 2022 gelang. Sie werden gebraucht, um nach Attacken schnell und verlässlich herauszufinden, wer die direkten und indirekten Urheber dieser Attacken waren, um diese gegebenenfalls öffentlich zu machen, die Täter zu finden oder Strafmaßnahmen einzuleiten – wie etwa bei den russischen Attentaten auf den Ex-Agenten Sergey Skripal und Oppositionellen Alexander Navalny.

Wir brauchen die Dienste auch für wirksame Abschreckung, um Schwachstellen der Gegner zu identifizieren und mögliche Gegenmaßnahmen, zum Beispiel Hackbacks, erfolgreich durchführen zu können. Es gilt, die ausländischen Finanzquellen extremistischer Kräfte aufzudecken, abzustellen und ideelle Unter-

stützung und Korruption öffentlich zu machen und strafrechtlich zu verfolgen.

Effektive Dienste können enorm von der Kooperation mit Partnerdiensten profitieren, da diese oft über komplementäre Expertise und Methoden verfügen. Arbeitsteilung und gemeinsame Investitionen in teure Fähigkeiten wie Satelliten, Kryptographie oder KI-Systeme sind effizienter und billiger. Zudem bilden gemeinsame Bedrohungsanalysen und Zukunftsszenarien eine wichtige Basis für gemeinsame Interessen und gemeinsames Handeln – bilateral, innerhalb der EU und NATO sowie in kleineren Kooperationsformen. Nachrichtendienstliche Zusammenarbeit kann zwischenstaatliches Vertrauen aufbauen, das auch Zerwürfnisse auf Regierungsebene überleben kann und damit Beziehungen stabilisiert.

Nachrichtendienste sind wichtig, um Zukunftsräume durch robuste Analyseverfahren auszuloten, den Vorstellungsräum zu vergrößern und die Wahrscheinlichkeit unangenehmer Überraschungen zu verringern. Sie können dazu beitragen, der Politik Handlungsoptionen aufzuzeigen, um erfolgreiche Strategien in der Außen- und Sicherheitspolitik zu verfolgen, anstatt nur Politik auf (Kurz-)Sicht zu fahren und ständig auf die Aktionen anderer reagieren zu müssen.

Die wehrhafte Demokratie braucht effektive Nachrichtendienste, deren Wissen und Analysen von Entscheidern genutzt werden und die nicht leicht ignoriert werden können, wenn es unbequem ist. Es braucht Dienste, die die Unterstützung und das Vertrauen von Öffentlichkeit und Parlament genießen. Und sie müssen auch genug Vertrauen von Partnerdiensten gewinnen, um tiefere und weitergehende Kooperation zu ermöglichen. Das erfordert hinreichende Vertraulichkeit bei der Behandlung von Erkenntnissen und Methoden dieser Dienste, und Gegenseitigkeit beim Austausch wertvoller Informationen und Analysen. Naturgemäß hört die Öffentlichkeit selten von den Erfolgen der Dienste, insbesondere wenn Attacken vereitelt wurden, um Methoden und Quellen nicht zu gefährden.

Es ist klar und auch vom Bundesverfassungsgericht anerkannt, dass deutsche Nachrichtenwesen eine zentrale Funktion für die Sicherheit Deutschland erfüllen. Allerdings ist auch klar, dass das Potential der Nachrichtendienste bisher bei weitem nicht genutzt wurde – und die Fähigkeiten angesichts der Sicherheitslage bei weitem nicht ausreichend sind. Wie wir in einem [Paper für den Gesprächskreis Nachrichtendienste](#) herausgearbeitet haben, gibt es einige Defizite. Die besten Fähigkeiten nützen nichts, wenn sie aus rechtlichen Gründen nicht genutzt werden dürfen. So fehlt unseren Nachrichtendiensten der rechtliche >

Rahmen für Beschaffungskompetenzen und Informationsübermittlung mit anderen Behörden, die in Europa bei unseren Verbündeten gängige Praxis sind.

Gleichzeitig wurden gewonnene Erkenntnisse im politischen Prozess oft nur unzureichend gehört und genutzt. Dies war teilweise politisch gewollt, wenn Nachrichtendienste von Kanzlern und Ministern bewusst auf Abstand gehalten wurden, teilweise geschah dies aufgrund mangelnden Interesses und Wertschätzung ihrer Arbeit, teilweise um das politische Risiko unbequemer Lageeinschätzungen zu minimieren.

Das Nachfrage- und Nutzungsdefizit lag andererseits daran, dass nachrichtendienstliche Lageeinschätzungen häufig mit den „Hauslagen“ der Ministerien konkurrierten und es an der Instanz und Fähigkeit fehlte, diese Unterschiede auf der Basis aller Quellen und Methoden kritisch zu diskutieren und in einer gemeinsamen Einschätzung aufzulösen. So konnten sich Entscheider das für sie am meisten Genehme herausuchen und leichter in Wunschdenken verfallen. Die Fragmentierung der Sicherheitsarchitektur behinderte zudem das koordinierte Handeln über Politikfelder, Ländergrenzen und Akteurstypen hinweg, das die komplexe Bedrohungslage erfordert.

Dabei unterliegen die deutschen Dienste einer sehr starken Kontrollarchitektur, die insbesondere rechtlich prüft und damit einen hohen bürokratischen Aufwand erzeugt. Diese technokratische, justizielle Überprüfung schafft aber kein „Vertrauen durch Kontrolle“, sondern erscheint eher als eine Institutionalisierung des Misstrauens. Gerade gesellschaftlich gab es bisher wenig Anerkennung, sondern vor allem Misstrauen gegen die wichtige Funktion von Nachrichtendiensten. So begrenzt sich auch die parlamentarische Beschäftigung mit den Diensten auf einen sehr

allgemeinen Charakter. Weder wird oft genug die Expertise der Dienste genutzt, noch wird im Sinne einer ‚Befähigungskontrolle‘ ausreichend auf die Sicherherstellung der Wirksamkeit und Befähigung der Nachrichtendienste geschaut.

DIE SITUATION DER DEUTSCHEN DIENSTE

Die neue Regierung hat wichtige Weichenstellungen zur Behebung einer Reihe dieser Defizite vorgenommen. So wurde die Schuldenbremse für Sicherheitsfragen in weiten Teilen ausgesetzt, um Investitionen in ein Aufwachsen der entsprechenden Behörden und Fähigkeiten zu ermöglichen. Durch eine ambitionierte Reformierung des Rechtsrahmens soll der BND künftig neue Befugnisse erhalten, nachdem bereits ein fachlich besonders qualifizierter Botschafter ungewöhnlicherweise auf direkten Wunsch des Bundeskanzlers zum neuen Präsidenten des BND berufen wurde.

Mit der Schaffung des Nationalen Sicherheitsrates soll eine bessere Koordinierung der zahlreichen Akteure stattfinden, wobei auch eine stärkere Nutzung nachrichtendienstlicher Erkenntnisse in Strategie- und Entscheidungsprozessen zu erwarten ist. Nicht zuletzt wurde auch die öffentliche Kommunikation über die Wichtigkeit der Nachrichtendienste in einer zunehmend unsicheren Welt ausgebaut, wobei insbesondere die Bundesregierung selbst starken Rückhalt viel aktiver kommuniziert.

Dieser Weg der Bundesregierung ist richtig. Die Stärkung der Nachrichtendienste des Bundes ist neben der besseren Erfüllung ihrer primären Funktion auch aus weiteren Gründen wichtig. So dient es der Abschreckung gegenüber feindlich gesinnten Akteuren, wenn der deutsche Staat glaubhaft machen kann, dass er verdeckte Operationen aufzuklären und sanktionieren zu vermag, weil er über starke Nachrichtendienste verfügt. Insbesondere im Cyberbereich sind hier die Fähigkeiten zur Attribuierung von Attacken wichtig, aber auch die Möglichkeit zu sogenannten Hackbacks im Falle eines Angriffs.

Deutschland ist gleichzeitig auf die internationalen Partnerschaften mit seinen Verbündeten auch im nachrichtendienstlichen Bereich erheblich angewiesen. Dies ist keine Schwäche, sondern Ausdruck einer komplexen und globalisierten Welt. Daher ist es wichtig, dass deutsche Dienste ihren Partnern in Stärke und auf Augenhöhe begegnen können, um in der Kooperation substanzielle Erkenntnisse beitragen zu können. Es gilt, die europäische nachrichtendienstliche Zusammenarbeit und Solidarität weiter auszubauen, um gemeinsam stärker handeln zu können. Deutschland kommt hier eine wichtige Rolle zu, weshalb es als Vorreiter vorangehen sollte. >

„Deutschland sollte als Vorreiter der europäischen nachrichtendienstlichen Kooperation vorangehen.“

Christoph Meyer und Daniel Neumann

Insbesondere bei der Reform des BND-Gesetzes sollte die Bundesregierung aber sicherstellen, diese für mehr als lediglich eine Stärkung der Beschaffungsmöglichkeiten des Dienstes zu nutzen. Viel grundsätzlicher sollte sein Charakter als Analyse-dienstleister der Bundesregierung für sicherheitspolitische Entscheidungsprozesse verdeutlicht werden. Dazu gehört, die Gesetzesneufassung nicht auf eine Ausweitung der Befugnisse bei Informationsbeschaffung und Datenübermittlung zu beschränken. Diese sind in der Tat sehr wichtig, sollten aber nicht die einzige große Errungenschaft der Reform werden. Es sollte beispielsweise auch ausdifferenziert werden, wann Berichterstattungs- und Konsultationspflichten bestehen sollten, um wirksame nachrichtendienstliche Berichterstattung sicherzustellen, auch dann, wenn sie politisch unbequem sein mag.

HERAUSFORDERUNGEN UND KONSEQUENZEN

Es gibt jedoch viele Hindernisse zur Umsetzung dieser Vision. Einerseits hat das Bundesverfassungsgericht der Gesetzgebung und der Kontrolle der Nachrichtendienste große Pflichten und Grenzen auferlegt. Innerhalb des vorgegebenen Rahmens müssen jedoch angesichts der Sicherheitslage Spielräume ausgenutzt werden. Zugleich haben wir in Deutschland aber auch ein kulturelles Problem.

Zum Teil ergibt sich dies natürlich aus der deutschen Geschichte, wodurch ein grundsätzliches und historisch berechtigtes Misstrauen gegen Dienste, Zentralisierung, Militarisierung und vor allem die Kooperation zwischen Nachrichtendiensten, Polizei und Unternehmen besteht.

Zu einem anderen Teil entsteht dieses kulturelle Problem aber auch aus mangelndem Wissen über Nachrichtendienste in der allgemeinen Öffentlichkeit, in den Parlamenten, den Medien und der deutschen Wissenschaftslandschaft. Dies machen sich auch Einflussnetzwerke unserer Gegner in der Politik und teilweise in den Diensten selbst zunutze.

Es gibt keine einzelne Stellschraube, die diese Probleme behebt. Vielmehr erfordert es ein kontinuierliches Zusammenwirken von rechtlichen Änderungen, institutionellen Reformen, Investitionen in besseres Wissen – und die Unterstützung eines kulturellen Wandels. ■

„In Deutschland besteht ein grundsätzliches und historisch berechtigtes Misstrauen gegenüber Nachrichtendiensten.“

Christoph Meyer und Daniel Neumann

„In der Analyse sind wir gut“

Vom Kalten Krieg über Afghanistan bis zur Zeitenwende: Ein ehemaliger hochrangiger BND-Mann erklärt, wie sich Auftrag, Prioritäten und Selbstverständnis des Dienstes verändert haben – und warum gute Aufklärung politisch oft folgenlos bleibt.



INTERVIEW _ Klaus Schmidt

Oberst a. D. Klaus Schmidt war in leitenden Funktionen im deutschen Sicherheits- und Nachrichtendienstbereich u. a. als Abteilungsleiter und Referatsleiter im Bundesnachrichtendienst tätig und als Referent im Bundesministerium der Verteidigung. Zuvor diente er als Generalstabsoffizier, Bataillonskommandeur der Deutsch-Französischen Brigade und Offizier der Bundeswehr. Er ist Vorsitzender des Gesprächskreis Nachrichtendienste in Deutschland GKND

Oberst Klaus Schmidt, was hat Sie motiviert, beim BND zu arbeiten?

Klaus Schmidt: Für mich stellte sich die Frage so gar nicht. Als Berufssoldat wurde ich nach der Generalstabsausbildung für verschiedene Verwendungen vorgesehen, bei mir war es der BND. Das Thema interessierte mich, also sagte ich zu. 1988 wurde ich erstmals dorthin versetzt, später folgten weitere Stationen im militärischen Nachrichtenwesen, im Verteidigungsministerium und schließlich die Leitung des Führungsinformationszentrums des BND.

Können Sie Ihre Tätigkeit beim Dienst näher beschreiben?

In meiner ersten Verwendung war ich von 1988 bis 1991 Dezernatsleiter Indication and Warning. Das war enorm wichtig, weil es um die Frage der Warnzeit ging. Wir haben Aktivitätslevel auf der Gegenseite bewertet und daraus Schlüsse gezogen. Mehr kann ich dazu

nicht sagen. Später habe ich das Führungsinformationszentrum geleitet. Dort wird im Schichtbetrieb beobachtet, was weltweit passiert. Von dort aus geht die tägliche Berichterstattung an die Kunden des Dienstes. Es ist sozusagen das Ein- und Ausgangstor des BND.

Wie hat sich die Mission des Dienstes mit dem Ende des Kalten Krieges verändert?

Bestimmte Länder und Themen standen immer im Fokus, aber die Gewichtungen haben sich verschoben. Spätestens z.B. als Polen NATO-Mitglied wurde, veränderten sich die Prioritäten. Gleichzeitig entwickelte sich mit den Balkan-Einsätzen eine neue Qualität. Deutschland beteiligte sich an Friedensmissionen der UN und der EU. Später kam dann Afghanistan. Das waren Regionen, die sehr am Rand deutscher Interessen lagen, aber plötzlich relevant wurden.

Was waren die Folgen für den BND?

Die Auslandseinsätze veränderten den Dienst, die Zusammenarbeit mit der

KEY MESSAGES

- **Der BND** ist primär ein strategischer Dienst und damit ein Frühwarnsystem.
- **Gute Aufklärung** verpufft, wenn die Politik Warnungen ausblendet oder relativiert.
- **Auslandseinsätze und Zeitenwende** haben die Prioritäten des Dienstes mehrfach verschoben.
- **Deutschlands größte Schwäche** liegt im Mangel an strategischem Denken und gemeinsamer Lagebewertung.
- **Wehrhafte Demokratie** braucht die gesellschaftliche Bereitschaft, Gefahren früh zu erkennen und zu reagieren.

Bundeswehr und dem Auswärtigen Amt. Bis etwa 2020 lag der Fokus stark auf Einsatzgebieten. Seit wir aus Afghanistan oder Mali raus waren und wieder Landes- und Bündnisverteidigung priorisieren, mussten auch die internen Prioritäten des Dienstes neu gesetzt werden. Das habe ich aber nicht mehr als aktiver Angehöriger erlebt.

Russland war aber doch immer ein zentrales Aufklärungsziel.

Der Dienst hat berichtet und seine Aufgaben wahrgenommen. Die Krux ist nur: Man kann noch so gut aufklären, wenn politisch nicht zugehört wird. Wenn Warnungen beiseitegelegt werden, weil man einen anderen politischen Ansatz verfolgt, dann hat ein Nachrichtendienst ein Problem. Das ist kein deutsches Sonderphänomen, das sieht man auch bei den Amerikanern. Stichwort 9/11.

Wo liegen aus Ihrer Sicht die zentralen Schwierigkeiten im Verhältnis zwischen Nachrichtendiensten und Politik?

Der Bundesnachrichtendienst hat ein Auftragsprofil, das ihm von der Regierung vorgegeben wird. Es gibt Prioritäten nach Ländern, Aktivitäten und Themen wie internationalem Terrorismus. In Deutschland ist es traditionell so, dass der BND die sogenannten Ressortlagen ergänzt. Jedes Ministerium hat sein eigenes Lagebild. Das Lagebild des Auswärtigen Amtes ist oft optimistischer als das des Verteidigungsministeriums. Wenn dann das Lagebild des BND dazukommt, kann es passieren, dass gesagt wird, so schlimm ist das nicht, wir sehen das anders. Afghanistan ist dafür ein gutes Beispiel.

Was ist damals passiert?

Bundeswehr und BND haben über Jahre gesagt, wenn wir Afghanistan verlas-

sen, wird es zu einer Machtübernahme durch die Taliban kommen. Der politische Wille, dauerhaft zu bleiben, war aber nicht vorhanden. Was ein Dienst nicht kann, das ist, den einen Tropfen zu benennen, der das Fass zum Überlaufen bringt. Das Auswärtige Amt hat z.B. auf Gespräche mit afghanischen Spitzenvertretern verwiesen, die versichert haben, man werde standhalten. Drei Tage später ist der Präsident geflohen. Das zeigt das Problem sehr deutlich.

gilt. Das wird noch dauern. Ein Vorbild wäre das britische Joint Intelligence Committee. In diese Richtung bewegen wir uns, aber das braucht Zeit.

Wie haben Ukrainekrieg und „Zeitenwende“ die Ausrichtung des BND verändert?

Die Neubewertung hätte eigentlich schon 2014 beginnen müssen, mit der Annexion der Krim, das ist aber nicht geschehen. Seit 2022 ist der Blick klar zurück auf Landes- und Bündnisverteidigung gerichtet. Das wird noch stärker

„Man kann noch so gut aufklären, wenn politisch nicht zugehört wird.“

Klaus Schmidt

Heißt das, es fehlt an einer gemeinsamen Lagebewertung?

Genau. Eine gemeinsame Lagefeststellung ist entscheidend. Diese soll jetzt ja durch den Nationalen Sicherheitsrat erfolgen. Es geht auch um strategische Analysen. Deutschland hat hier lange Defizite gehabt. Erst seit 2022 gibt es überhaupt eine nationale Sicherheitsstrategie, aus Sicht eines Nachrichtendienstlers noch mit vielen Lücken. Wir fahren strategisch oft auf Sicht und entscheiden kurzfristig.

Wie kann die Lagebewertung besser organisiert werden?

Neben einem Bereich, der langfristig strategisch denkt, braucht es ein Lageelement, das zu Entscheidungen kommt. Es darf kein runder Tisch sein, bei dem jeder seine Meinung sagt und man danach auseinandergeht. Irgendwann muss entschieden werden, was

werden. Wir können nicht mehr selbstverständlich davon ausgehen, dass wir ein vollständig aufbereitetes Lagebild von der NATO bekommen wie im Kalten Krieg. Die Amerikaner setzen andere Schwerpunkte. Deshalb müssen wir eigene Kapazitäten aufbauen, innerhalb der NATO und der EU, gemeinsam mit Partnern, langfristig und in die Tiefe.

Der BND als „strategischer“ Dienst: Was heißt das konkret?

Ein strategischer Dienst ist primär ein Frühwarnsystem. Er muss die großen Linien der deutschen Sicherheitsinteressen im Blick haben, Veränderungen erkennen und Indizien benennen. Diese Hinweise müssen in ein Gremium wie den Nationalen Sicherheitsrat eingebracht und bewertet werden. Das Problem in Europa ist, dass strategisches Denken wenig ausgeprägt ist. Wir reagieren oft nur kurzfristig. >

Wie würden Sie heute Stärken und Schwächen des Dienstes einschätzen?

Zu technischen Fähigkeiten und Quellenarbeit kann oder darf ich nichts sagen. Klar ist aber: Wir brauchen Fachkompetenz und starke Analysten, was bei öffentlichen Gehaltsstrukturen schwierig ist. Trotzdem bin ich überzeugt, dass wir sehr engagierte und leistungsfähige Leute haben. In der Analyse sind wir gut. Im Kreis vergleichbarer Dienste, also mit Briten, Franzosen oder Italienern, können wir mithalten. Die Amerikaner spielen in einer anderen Liga. Sie zu kopieren wäre illusorisch.

Der BND gilt als analytisch stark, aber operativ zu langsam...

Der Begriff „langsam“ ist mir zu grob. Wir haben allerdings Begrenzungen, etwa durch unser Kontroll- und Rechtsregime. Bei der Auslandsfernmeldeaufklärung gibt es verfassungsrechtliche Vorgaben. Taucht ein deutscher Staatsbürger auf, muss gelöscht, informiert und dokumentiert werden. Das sind Restriktionen, die andere Dienste so nicht haben. Das macht uns nicht lang-

wir haben es uns in Deutschland lange bequem gemacht mit der Annahme, dass die Amerikaner das schon regeln und uns die Informationen liefern. Diese Haltung wird so nicht mehr tragen. Aktive Maßnahmen, wie sie etwa die Franzosen haben, kann ich mir bei uns allerdings zur Zeit kaum vorstellen. Die haben eigene Einheiten für solche Operationen. Das wird es bei uns nicht geben. Im Bereich der technischen Aufklärung hingegen wird man weiter gehen müssen.

Im Kontext hybrider Bedrohungen: Könnten Sie sich vorstellen, dass Deutschland etwa auf einen Sabotageakt mit ähnlichen Maßnahmen antwortet?

Im Moment kann ich mir das nicht vorstellen. Dafür müsste noch sehr viel passieren. In der Bevölkerung müsste ein deutlich stärkeres Bewusstsein für hybride Bedrohungen vorhanden sein. Vor allem bräuchte man klare Beweise, wer dahintersteckt. Schon bei Drohnen sehen Sie, wie komplex die Fragen sind. Wer steckt dahinter, wer darf eingreifen, wann darf man reagieren? In einer

Operativer zu werden heißt nicht Aktionismus, sondern gezielten Ausbau der Fähigkeiten. Im HUMINT-Bereich ist das besonders schwierig, klassische Quellenarbeit dauert Jahre. Technische Aufklärung bietet mehr Spielraum trotz rechtlicher Grenzen. Dazu gehören das Eindringen in digitale Netzwerke und der Aufbau eigener Satellitenfähigkeiten mit der Bundeswehr. Auch Open Source Intelligence und KI werden wichtiger. Operativ heißt: aktiv und gezielt suchen, nicht nur abwarten.

Wie sehen Sie die Abhängigkeit von den USA im Intelligence-Bereich?

Beim Teilen von Informationen muss man immer aufpassen, dass man sie nicht ungeprüft übernimmt. Hinweise werden abgeklopft und eingeordnet. Die Amerikaner werden Europa nicht verlassen. Sie verlagern Schwerpunkte in den Pazifik, aber sie bleiben präsent. Sie erwarten allerdings, dass Partner etwas beitragen. Dieses Geben-und-Nehmen bleibt zentral. Gleichzeitig muss man beim Austausch genau hinschauen, denn Informationen können auch politisch gefärbt sein.

Sehen Sie die Vereinigten Staaten aus nachrichtendienstlicher Perspektive weiterhin als Partner?

Für mich bleiben die Amerikaner Partner. Der Gedanke, dass sie uns dauerhaft schützen und sich um alles kümmern, wird schwächer werden, aber Partner bleiben sie. Das zeigt sich auch daran, dass in den USA gesetzlich festgelegt ist, wie viele amerikanische Soldaten in Europa stationiert bleiben müssen. Ich bin überzeugt, dass die USA auch aus eigenem Interesse präsent bleiben wollen, um zu wissen, was in Europa passiert. Beziehungen sind dabei immer interessengeleitet, nicht von Romantik getragen. >

„Wir haben es uns bequem gemacht mit der Annahme, dass uns die Amerikaner die Informationen liefern.“

Klaus Schmidt

sam, aber es setzt Grenzen. Diese werden derzeit ja auch politisch diskutiert.

Soll der Dienst in Zukunft auch aktiv handeln dürfen, statt nur zu beobachten, also zum Beispiel Computer hacken?

Diese Diskussion wird sehr stark juristisch geprägt sein. Persönlich denke ich,

Demokratie dauert das. Deshalb sehe ich aktuell keine Bereitschaft für solche Schritte.

Der heutige BND-Präsident Martin Jäger spricht davon, höhere Risiken einzugehen und operativer zu werden. Wie interpretieren Sie das?

In Deutschland spielt das Konzept der wehrhaften Demokratie eine große Rolle. Wie interpretieren Sie das aus Intelligence-Perspektive?

Lange war das eher ein Schlagwort. Heute wird es konkreter. Wir haben uns jahrzehntelang unter dem Schutzschirm der NATO sicher gefühlt und geglaubt, wir müssten selbst nicht wehrhaft sein. Dieses Bewusstsein ändert sich gerade. Gleichzeitig sehen wir eine zweite Bedrohung nach innen. Die gesellschaftliche Mitte wird schwächer, die Ränder werden stärker. Radikalisierung findet nicht nur in eine Richtung statt. Das ist eine reale Herausforderung für unsere Demokratie.

Was bedeutet wehrhafte Demokratie nach außen?

Zunächst die klare Erkenntnis, dass man sich verteidigen können will. Schweden und Finnland sind dafür gute Beispiele. Das sind keine militaristischen Gesellschaften, aber Verteidigungsfähigkeit ist dort selbstverständlich. Auch bei uns wird manches, was heute noch kontrovers diskutiert wird, bald Normalität sein. Wenn das einsetzt, sind wir auf einem guten Weg.

Was ist aus Ihrer Sicht aktuell die größte Herausforderung, gerade für den Auslandsnachrichtendienst?

Aus meiner Sicht ist es der mentale Wandel in der Gesellschaft. Wehrhafte Demokratie heißt nach außen wie nach innen, dass wir Gefahren früh erkennen und bereit sind zu reagieren. In diese Richtung müssen Gesetzgebung und konkrete Aufträge an die Dienste entwickelt werden.

Welche Rolle soll der »Gesprächskreis Nachrichtendienste« dabei spielen?

Unser Anliegen ist es, sicherheits- und nachrichtendienstliche Themen sachlich in die öffentliche Debatte einzubringen.

Das geschieht durch Veranstaltungen, Gespräche und Beiträge. In der sicherheitspolitischen Community in Berlin sind wir inzwischen etabliert und arbeiten mit Partnern wie der Deutschen Atlantischen Gesellschaft, der Deutschen Gesellschaft für Auswärtige Politik (DGAP) und der Bundesakademie für Sicherheitspolitik. Das Interesse und die Offenheit dafür sind gewachsen.

Was muss geschehen, um die deutsche Intelligence-Kultur zu fördern?

Ein großes Defizit ist, dass es in Deutschland kaum Intelligence Studies an Universitäten gibt, insbesondere nicht in der Politikwissenschaft. Es existieren nur wenige Ansätze, etwa in Potsdam, Bonn oder an der Hochschule des Bundes. Dabei gibt es viele interessierte junge Leute. Ohne stärkere aka-

demische Verankerung fehlt dem Thema Reichweite und Tiefe.

Gibt es etwas in Ihrer Laufbahn, auf das Sie besonders stolz sind?

Besonders stolz bin ich darauf, dass ich erst die Nachrichtenzentrale der Bundeswehr geleitet habe und später gefragt wurde, ob ich dieselbe Aufgabe im Führungsinformationszentrum des Bundesnachrichtendienstes übernehmen möchte. Das war für mich ein Zeichen von Vertrauen. Sechs Jahre lang diese Funktion ausüben zu dürfen, war ein guter Abschluss meiner Laufbahn.

Was würden Sie jungen Menschen sagen, die überlegen, für einen Nachrichtendienst zu arbeiten?

Dass sie ein sehr interessantes Berufsleben erwartet. Man beschäftigt sich >

LICHT DER ÖFFENTLICHKEIT

■ **Der Gesprächskreis Nachrichtendienste in Deutschland e. V. (GKND)**

ist ein unabhängiger gemeinnütziger Verein, dessen Ziel es ist, zu einer konstruktiven und öffentlichen Diskussion über die geheimen staatlichen Nachrichtendienste in demokratischen Rechtsstaaten beizutragen. Dabei will er sich in erster Linie mit Zukunftsfragen der Dienste beschäftigen, wie sie sich aus Veränderungen der Welt und der globalpolitischen Interessenlage der Bundesrepublik Deutschland ergeben. Dies betrifft Ziele, Aufgaben, Methoden und Strukturen sowie die internationale Kooperation der Dienste und ihre Kontrolle.

■ **Zu den Mitgliedern gehören** ehemalige Angehörige der deutschen Nachrichten- und Sicherheitsdienste, der Bundeswehr sowie Personen aus Politik und Wissenschaft, die sich mit der Thematik des Vereins beschäftigen. Der GKND erarbeitet Stellungnahmen und Hintergrundpapiere zu aktuellen Themen mit Bezug zu den Nachrichtendiensten in Deutschland und stellt diese auf seine Webseite (www.gknd.org) ein.

■ **Im GKND-Monitor** stellt er Hinweise auf Meldungen, Berichte, Publikationen und öffentlich zugängliche offizielle Dokumente zu sicherheitspolitisch und nachrichtendienstlich relevanten Sachverhalten zusammen. Der GKND organisiert darüber hinaus regelmäßig eigenständig oder mit Partnern Veranstaltungen zu aktuellen Themen mit sicherheitspolitischem und nachrichtendienstlichem Bezug.

mit Themen, die nicht jedem zugänglich sind, und bekommt einen sehr weiten Blick auf politische und sicherheitspolitische Zusammenhänge. Natürlich sind Gehalt und Besoldung ein Thema, gerade im Vergleich zur Privatwirtschaft. Aber inhaltlich ist das Feld außergewöhnlich.

**Wie finden Sie eigentlich die aktuelle
BND-Kampagne in den sozialen Medien?**

Die neue Kommunikationskampagne des BND hat mich zunächst altersbedingt irritiert. Aber sie funktioniert offenbar gut und spricht junge Leute an. Entscheidend ist, dass diese Motivation erhalten bleibt. Ich kenne Fälle, in denen junge Mitarbeiter den Dienst wieder verlassen haben, weil sie die starke Bürokratisierung frustriert hat. Jede Idee erst rechtlich prüfen zu müssen, kann lähmen. Hinzu kommen strukturelle Probleme, etwa bei der Verbeamtung von Fachkräften, die keine Juristen sind. Auch daran muss gearbeitet werden. Das gehört ebenfalls zur Zukunftsfähigkeit der Dienste. ■

„Man beschäftigt sich mit Themen, die nicht jedem zugänglich sind.“

Klaus Schmidt

Demokratien im Nachteil?

Während autoritäre Regime Krieg als legitimes Machtinstrument begreifen, sehen Demokratien ihn als Ausnahme und Scheitern. Diese normative Asymmetrie prägt Entscheidungsprozesse, hybride Konflikte und die Verwundbarkeit offener Gesellschaften im geopolitischen Wettbewerb.

Wir – das heißt, die NATO-Staaten – befinden uns seit einigen Jahren in einem neuen Kalten Krieg. Damit gemeint ist ein Konflikt, in dem es nicht nur um Macht, sondern auch um Ideologien geht, wobei der Kampf indirekt, für uns unblutig ausgeführt wird, aber durchaus für Andere ein blutiger Krieg sein kann. Gegenwärtig bluten die Ukrainer, 2008 waren es die Georgier. Für uns geht es in diesem Kampf, wie schon im Kalten Krieg, erneut um die Herzen und Gemüter ganzer Völker, und die beiden gegnerischen Lager kämpfen darum, diese Völker auf ihre Seite zu ziehen. Auf der einen Seite die "offene Gesellschaft", von Karl Popper 1945 definiert als eine, in der "das Individuum mit persönlichen Entscheidungen konfrontiert wird", im Gegensatz zu einer „magischen, Stammes- oder Kollektiven Gesellschaft.“¹ Das Individuum, und individuelle Menschenrechte, stehen damit im Zentrum der Werte der offenen Gesellschaft. Schon Poppers Definition sagt uns, wo die Werte der anderen, der "kollektiven Gesellschaft" liegen: Sie priorisieren die Kollektivität und ihre Rechte über denen des Individuums. Mehr noch, sie widersetzen sich der Idee, dass führende weltliche Eliten Werte definieren (und auch solche Definitionen revidieren) können, und halten ein Dogma dagegen, das aus metaphysischen Quellen („eine höhere, unergründliche² Autorität“) stammt. Wir finden dies direkt formuliert vom Chef der Abteilung für Internationale Beziehungen an der russischen Eliteuniversität MGIMO, Ale- >

¹ Popper, Karl: The Open Society and Its Enemies, Volume One, London: Routledge, 1945, Neudruck 2006, Kap. 10, Teil I.

² "unknowable" in der englischen Übersetzung.

TEXT_ Beatrice Heuser

Prof. Dr. Beatrice Heuser ist Distinguished Professor an der Brussels School of Governance, VUB sowie Head of Strategy Teaching an der Führungsakademie der Bundeswehr. Im Zentrum ihrer Forschung steht die Frage, warum Menschen Kriege führen, welche Mittel und Strategien sie wählen – und wie sie diese rechtfertigen.

KEY MESSAGES

- **Demokratien** beschränken sich bewusst durch Völkerrecht, Transparenz und öffentliche Kontrolle.
- **Langsame Entscheidungsprozesse** und Rechtsbindung machen offene Gesellschaften berechenbar.
- **„Hybridkrieg“** nutzt Grauzonen unterhalb der Kriegsschwelle, auf die Demokratien schlecht vorbereitet sind.
- **Propaganda, Desinformation und Cyberangriffe** treffen offene Informationsräume besonders effektiv.
- **Der neue Kalte Krieg** ist ein Systemkonflikt: zwischen individueller Freiheit und kollektivistischer Machtlogik.

xander Lukin, in einem 2014 veröffentlichten Artikel – Russland war gerade dabei, die Krim zu annektieren.³

Hier soll untersucht werden, wie unsere Sichtweise des Krieges in liberalen Demokratien und unsere Praktiken, sich von denen unserer Gegner unterscheiden, und was das für Konsequenzen hat.

I. Der demokratische Rechtsstaat und der Krieg

Der Rechtsstaat, der sich der Befolgung des Völkerrechts und der Menschenrechte verschrieben hat, schränkt seine eigene Handlungsfreiheit bewusst ein. Er baut dabei auf die Traditionen des "gerechten Krieges", von denen auch heute noch das unbestreitbarste Kriterium dominiert: nur die Verteidigung ist legitim.

In der Entwicklung des modernen Staats gab es einen sich bis zur Gegenwart hinziehenden Strang, der die Unabhängigkeit, die Souveränität des Staates über alles stellte. In der Realität war nie ein Herrscher oder Staat je so ganz unabhängig vom Einfluss anderer, und damit war keiner absolut souverän, auch wenn er oder sie dieses Ideal vor Augen hatte. Auch souveräne Herrscher sahen sich weitgehend ans Gewohnheitsrecht (wie etwa spätestens ab dem 17. Jahrhundert dem Austausch von Kriegsgefangenen) gebunden. Solche, die es missachteten, wurde als barbarisch und unzivilisiert angesehen, oft Veranlassung genug für andere Herrscher, gegen sie vorzugehen.

Dies bezog sich auch auf Entscheidungen, einen Krieg zu beginnen. Nach der Tradition des gerechten Krieges musste man den Nachweis erbringen, dass einem Unrecht widerfahren war, dass die Gegenseite sich weigerte, dies Unrecht wieder gut zu machen, und dass der Krieg die ultimative Möglichkeit war, eigenständig dieses Unrecht zu beheben, in Ermangelung einer höheren Autorität oder eines Vermittlers. Nur das außergewöhnliche 19. Jahrhundert räumte dem souveränen Staat uneingeschränkt das Recht ein, aus „Staatsraison“ oder aus „Nationalinteresse“, wie es später hieß, einen Krieg anzufangen.

Dieses Recht, nach dem Österreich und Deutschland noch 1914 gehandelt hatten, wurde aber schon im späten 19. Jahrhundert wieder von Juristen in Frage gestellt. Es ist auf den Einfluss dieser Juristen – und die revanchistische Stimmung der Bevölke-

rungen der Siegermächte – zurückzuführen, dass 1919 in den Friedensverträgen für das besiegte Österreich und das besiegte Deutschland diesen beiden Staaten eine Kriegs-*Schuld* zugesprochen wurde. Im Denken des 19. Jahrhunderts lud ein souveräner Staat keine *Schuld* auf sich, wenn er aus Staatsräson einen Krieg begann.⁴ Diese beiden Verträge läuteten eine Rückkehr zu völkerrechtlichen Beschränkungen ein, weg vom absolut souveränen Staat. Nur, wo früher Gewohnheitsrecht gegolten hatte, das man nicht vor einem internationalen Gericht einklagen konnte, setzte sich jetzt das Vertragsrecht an seine Stelle, seit 1920 mit einem internationalen Gerichtshof.

Schon der Völkerbund, im selben Jahr ins Leben gerufen, verpflichtete Mitglieder, Schlichtung zu suchen, und beauftragte einen (Sicherheits-)Rat, Mitgliedsstaaten gegen Angriffe zu schützen. Seine Verfassung räumte immer noch das Recht ein, in den Krieg zu ziehen, falls sich keine Schlichtung als möglich erwies. Aber 1928 wurde ein weiterer Entwicklungsschritt gemacht: Auf Vorschlag des damaligen französischen Außenministers Aristide Briand und seines amerikanischen Kollegen Frank Kellogg beschränkten sich die 31 Signatarmächte selbst mit einer Erklärung, den Krieg hinfort nicht mehr aggressiv als Instrument der „nationalen“ (d.h. staatlichen) Politik zu benutzen.

Die Charta der Vereinten Nationen übernahm diese Beschränkung des Rechtes zur Kriegführung auf die einzelne oder kollektive Selbstverteidigung.⁵ Die Organisation zur Sicherheit und Zusammenarbeit in Europa (OSZE) bestätigte diese Beschränkung erneut, indem sie ausdrücklich die Veränderung von Grenzen durch Anwendung von Gewalt ausschloss.⁶ So ist der Angriff Russlands auf die von ihm selbst im Budapester Abkommen von 1994 als unabhängiger Staat anerkannte Ukraine in jeder Hinsicht völkerrechtswidrig.

Das Völkerrecht beschneidet die Handlungsfreiheit der Staaten, wie auch jeder Vertrag es tut. Das Prinzip dabei ist, dass man sich selbst beschränkt, aber dafür den Vorteil genießt, dass andere dasselbe tun. Dieses Denken, das jeder geregelten Gemeinschaft zugrundeliegt, hat sich aber nicht in allen Kulturen festgesetzt. In etlichen Kulturen, besonders in solchen mit Großmacht-Geschichte, lebt noch die Überzeugung des 19. Jahrhunderts weiter, dass man vollkommen unbeschnittene Souve- ➤

³ Lukin, Alexander: "Eurasian Integration and the Clash of Values", *Survival*, 56:3 (2014), S. 43–60.

⁴ Hathaway, Oona & Scott Shapiro: *The Internationalists*, New York 2018.

⁵ UN Charta, Art. 51

⁶ Schlussakte von Helsinki, Art. I, <https://www.osce.org/de/mc/39503>, eingesehen am, 18.VIII.2023.

ränität genießen möchte und sich nicht durch irgendwelche äußeren Gesetze und Mächte einschränken lassen will. Die Vereinigten Staaten sind von dieser Tradition geprägt, obgleich sie ebenfalls eine internationalistische Tradition haben, aus der Völkerbund und UN hervorgegangen sind. Die erste Tradition führte dann paradoxerweise dazu, dass der amerikanische Kongress seinem Land verweigerte, diesem weitgehend von US-Präsident Woodrow Wilson und seinen Beratern entworfenen Völkerbund beizutreten. Unter Donald Trump hat sich diese souveränistische Tradition wieder voll entfaltet.

Souveränismus schwingt immer mal wieder mit, wenn es um die französische Verteidigung geht; er drückte sich in Frankreichs Selbstausschluss aus der NATO-Integration 1966-2009 aus. Auch ist er im britischen Brexit zu finden. Dennoch hat keines dieser beiden europäischen Länder das Verbot der Grenzänderung durch Gewalt angezweifelt.

Anders bei China und Russland: China ignoriert schlicht die Entscheidung des Internationalen Gerichtshofs zu Besitzansprüchen im Südchinesischen Meer, die von Chinas Nachbarländern angefochten werden. Russland hat einen Teil Georgiens besetzt und führt seit 2014 einen Krieg, um sich die Ukraine anzueignen.

II. Entscheidungsprozesse

Rechtsstaaten sollten sich generell an das Prinzip der Nichtangriffsverpflichtung der UN-Charta halten. Peinliche Ausnahme war der Interventionskrieg, den die USA mit einigen Partnern 2003 gegen den Irak führte. Immerhin waren von den jetzigen EU-Mitgliedsländern nur Polen daran beteiligt, und auch im beteiligten Großbritannien gab es lebhaftere öffentliche Proteste, sowie den Rücktritt von Regierungsberatern und den Selbstmord eines Sicherheitsexperten.⁷

Für die USA war dies keine Ausnahme, wie bei ihrem Einmarsch 1983 im Inselstaats Grenada, bei Luftangriffen 1986 auf den Präsidentenpalast in Libyen, 2017, 2018 und 2025 auf Terroristen in Syrien, oder 2025 in Angriffen auf Syrien, den Iran und Venezuela. Aber auch in Amerika sind solche Aktionen regelmäßig heftig kritisiert worden.

In Demokratien wird die politische Zustimmung der öffentlichen Meinung zumindest in Wahljahren abgefragt. Aber auch über reguläre Wahlen hinaus sind demokratische Staaten stärker von der öffentlichen Meinung abhängig und brauchen eine breite politische Zustimmung für militärische Maßnahmen. Auch der Ausgang von Regionalwahlen oder von Europawahlen kann als Missbilligung der Politik einer Regierung gedeutet werden und etwa zu Druck zu Neuwahlen auf Staatsebene führen. Es gibt Beispiele dafür, wie Regierungen, ohne dazu konstitutionell gezwungen zu sein, diesem Druck nachgegeben haben.⁸ Wenn man vom Streit darüber absieht, ob Großbritannien, Frankreich und das Deutsche Reich am Vorabend des Ersten Weltkrieges Demokratien waren,⁹ war der Erste Weltkrieg ein Beispiel dafür, wie große Bevölkerungsteile einen Krieg geradezu herbeisehnen konnten. Politiker beschworen ihn als „mannhaft“, ruhmversprechend und gesellschaftlich „reinigend“.

In Großbritannien, Frankreich und etlichen anderen Staaten (aber nicht in Deutschland), schlug dies nach 1919 um, so wie es europaweit nach 1945 dazu führte, dass die demokratischen Gesellschaften ihre Regierungen zur Zurückhaltung bei der Anwendung von Gewalt aufforderten. Sogar eine Abschreckungshaltung – eine offensichtliche Wehrtüchtigkeit, um Gegnern gar nicht erst der Gedanke an einen erfolgsversprechenden Angriff kommen zu lassen – stieß und stößt bei großen Teilen der Bevölkerungen der Niederlande, den Bundesrepubliken Deutschland und Österreich, von Großbritannien, Italien usw. immer wieder auf Proteste.

Regierungen demokratischer Staaten sind auch zu größerer Transparenz und Rechenschaftspflicht gegenüber der Öffentlichkeit und internationalen Gemeinschaft gezwungen als autoritäre Staaten. Dies kann sie in internationalen Konflikten verwundbar machen, da autoritäre Staaten sich unkonventioneller oder aggressiver Maßnahmen bedienen können, ohne sich um öffentliche Meinung oder internationale Normen zu scheren. Weiter werden Rüstungsausgaben in der Öffentlichkeit bestenfalls als ein geduldetes Übel besprochen. Rechtsstaatliche Demokratien und insbesondere ihre Bündnisse brauchen aus zwei Gründen >

⁷Es gab eine ausführliche Untersuchung, deren Ergebnisse abschließend im zwölf-Bändigen „Report of the Iraq Inquiry“ (a.k.a. Chilcot Report) veröffentlicht wurden, der zu einem sehr belastenden Ergebnis für die Nachrichtendienste und die Regierung führte. Allein schon das „Executive Summary“ hatte 145 Seiten. Siehe <https://www.gov.uk/government/publications/the-report-of-the-iraq-inquiry>, eingesehen am 14. VIII. 2023

⁸So etwa Präsident Macron in Frankreich im Juni 2024 nach dem Ausgang der Europawahlen. In Großbritannien war die East-Fulham By-Election von 1933, die Wahl eines Nachfolgers für einen im Amt verstorbenen Parlamentarier, der Startschuss für eine lange Politik der Kriegsvermeidung.

⁹In keinem dieser drei Staaten waren auch nur 50% der über 18-jährigen wahlberechtigt: in allen dreien hatten Frauen kein Wahlrecht, und viele der jungen Soldaten, die im Krieg von 1914-18 dienten, waren unter 21 und damit auch vom Wahlrecht ausgeschlossen.

sehr viel länger in ihren Entscheidungsfindungsprozessen als Diktaturen. Es sind die systemimmanenten Konsultativprozesse, mit Einbindung von Parlamenten außer im direkten Verteidigungsfall, und die Erörterungen der Rechtslage. Autokratien, die sich wenig für das Völkerrecht interessieren, können viel schneller entscheiden, solange sie die Mittel haben. Entsprechend können Autokratien Demokratien leicht überrumpeln und lähmen.

Autoritäre Regierungen erstrecken sich mitunter über Jahrzehnte. Sie können so ungehindert langfristige strategische Ziele verfolgen. Dagegen sind Regierungen demokratischer Staaten prinzipiell durch Wahlzyklen auf kurzfristigere Planung begrenzt, bzw. Langzeitprojekte – insbesondere militärische Forschungs-, Entwicklungs-, und Beschaffungsprojekte, sowie Umstrukturierung der Verteidigungs-Infrastruktur und des Personals – können von Folgeregierungen annulliert werden. Zwar treten im Kriegsfall Notstandsgesetze in Kraft, die gemeinhin die Rechte der Regierungen auch in Demokratien erweitern. Aber in Krisenzeiten ist die Trägheit des demokratischen Regierungssystems gut erkennbar, da weitreichende Maßnahmen – insbesondere die Einführung der Wehrpflicht – meist auf eine langsame Konsensbildung in der breiten Öffentlichkeit angewiesen sind. Leicht kann dort ein Gegner der offenen Gesellschaft durch Propaganda (und Geld) eine Opposition stärken.

III. „Hybridkrieg“

Dies bringt uns zu den Mitteln unblutigen Kampfes, heute oft als „Hybridkrieg“ bezeichnet, obwohl einige dieser Mittel Jahrtausende alt sind. Der Ausdruck Hybridkrieg stammt ursprünglich vom amerikanischen Strategen Frank Hoffman, der damit Kriege beschreiben wollte, die verschiedene Mittel vermischen, ohne ganz zur Gewaltanwendung überzugehen. Er wollte damit gegnerische Aktionen beschreiben, und wies darauf hin, dass wir in unserem binären Denken – Krieg *oder* Frieden – schlecht mit solchen Grauzonen umgehen können.¹⁰ Dieser Ausdruck wurde dann aber von russischen Strategen, allen führend Generalstabchef V.V. Gerasimov, aufgenommen, dabei allerdings als *westliches* Verhaltensmuster ausgelegt.¹¹

Eigentlich beschreibt beides nur, was insbesondere die UdSSR seit ihrer Gründung (und die Bolschewiken noch früher) tat, nämlich "fünfte Kolonnen" in Form von kommunistischen Parteien in anderen Ländern, Friedensbewegungen, Propaganda und andere Mittel der psychologischen Kriegsführung einzusetzen, eventuell noch Stellvertreterkriege zu führen, dabei möglichst einen Weltkrieg zu vermeiden. Was in den letzten Jahren – insbesondere in russischen Operationen gegen die Ukraine vor der klassischen Invasion ab Februar 2022 – neu hinzukam, ist die gezielte Meidung von Aktionen, die bei der NATO den Vertragsfall auslösen würde. So fing man an in der westlichen Strategiedebatte, von „Nicht-Artikel 5“-Aktionen zu sprechen, also Aktionen, die nicht als direkter Angriff auf das Territorium eines NATO-Mitgliedsstaats ausgelegt werden können. Der Artikel 5 des Nordatlantik-Vertrages beschreibt einen Angriff auf einen Mitgliedsstaat als einen Angriff auf alle und postuliert, dass die anderen Mitglieder dann etwas tun müssen (was, ist unklar gelassen: es könnte alles sein von einem Protestbrief bis hin zum Gebrauch von Kernwaffen, um den Bündnispartner zu verteidigen).¹² Die NATO schreibt durchaus in geringeren Fällen Konsultation vor (Artikel 4). Diese ist aber schwer in Handlungsvorgaben umzusetzen. Dies wieder erschwert der Entscheidungsfindung.

Maßnahmen, die zwar empören, wenn sie aufgedeckt werden, aber keinen Krieg auslösen, sind etwa die Ermordung einzelner Personen (etwa westlicher Staatsbürger, die aus Russland geflohen sind, weil sie dort als Regimegegner verfolgt wurden oder als Überläufer Informationen über russische Geheimdienste mitgebracht haben), Bestechung oder Erpressung einzelner Politiker oder Industrieller, physische Sabotageakte gegen Strom-, Gas-, Wasserwerke, Lahmlegung von Flughäfen usw.¹³

PROPAGANDAKRIEG

Propagandakrieg ist nichts Neues: der Versuch, die Bevölkerung im eigenen Staat zur Unterstützung einer Strategie zu überzeugen, lässt sich in die Antike zurückverfolgen; das gleiche gilt für die Beeinflussung der gegnerischen Seite. Immer schon kursierten dabei absichtlich oder unbewusst Halbwahrheiten oder >

¹⁰Hoffman, Frank: Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, Virginia 2007.

¹¹Fridman, Ofer: Russian Hybrid Warfare, Oxford 2018.

¹²Im Artikel 5 steht: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

¹³Kristan Stoddart: Russia's Hybrid Warfare Offensive Against the West (Berlin: De Gruyter, 2026)

Unwahrheiten zum Einsatz gekommen. Fake News a.k.a. Lügen sind dabei an sich nichts Neues. Neu ist nur die Art, wie sie verbreitet werden kann. Wo sich früher Gerüchte von Mund zu Mund verbreiteten, gibt es heute die Soziale Medien.

Der Rückgang des Zeitungslesens, insbesondere der Lektüre von Zeitungen mit gut recherchierten und verifizierten Artikeln, die Objektivität in der Reportage anstreben, ist für die offene Gesellschaft eine Bedrohung von innen. Es ist ein Zersetzungsprozess der Werte, auf der die offene Gesellschaft gebaut sind, denen des mündigen Bürgers, der aufgrund der kritischen Lektüre Positionen einnimmt. An seine Stelle tritt der faule Konsument der 400 Zeichen eines Tweets, der aus Echokammern Gleichgesinnter stammt, denen er „folgt“. Hier erreicht ihn am leichtesten die gegnerische Propaganda. Dabei werden wissentlich Lügen und Verleumdungen benutzt, wie etwa die Gleichsetzung all der Ukrainer, die ihr Land nicht in die russische Föderation einverleibt sehen wollen, mit „Nazis“, oder die Behauptung, Russisch-sprachige Ukrainer wären im Donbas genozidal verfolgt.

Hannah Arendt hat das Problem treffend beschrieben:

„Lügen erscheinen dem Verstand häufig viel einleuchtender und anziehender als die Wahrheit, weil der Lügner den großen Vorteil hat, im Voraus zu wissen, was das Publikum zu hören wünscht.“

Weiter ist es schwer, diese Unwahrheiten mit Gegenargumenten zu bekämpfen, heißt es doch im Volksmund, dass es "keinen Rauch ohne Feuer" gibt, das wohl „etwas dran sein muss“. Wie Arendt schrieb,

„In einer sich ständig verändernden, unverständlichen Welt hatten die Massen den Punkt erreicht, an dem sie gleichzeitig alles und nichts glaubten, alles für möglich und nichts für wahr

hielten. ... Die Massenpropaganda entdeckte, dass ihr Publikum jederzeit bereit war, das Schlimmste zu glauben, egal wie absurd es auch sein mochte, und dass es sich nicht sonderlich dagegen wehrte, getäuscht zu werden, weil es ohnehin jede Aussage für eine Lüge hielt. Die totalitären Massenführer stützten ihre Propaganda auf die richtige psychologische Annahme, dass man unter solchen Bedingungen die Menschen an einem Tag die phantastischsten Behauptungen glauben lassen und darauf vertrauen konnte, dass sie, wenn sie am nächsten Tag unwiderlegbare Beweise für deren Unwahrheit erhielten, sich in Zynismus flüchten würden; statt die Führer, die sie belogen hatten, zu verlassen, würden sie protestieren, dass sie die ganze Zeit gewusst hätten, dass die Behauptung eine Lüge war, und die Führer für ihre überlegene taktische Klugheit bewundern.“¹⁴

Dies beschreibt sehr gut nicht nur die Situation der 1930er Jahre, die Arendt vor Augen stand, sondern auch die der russischen und chinesischen Propaganda heute.

CYBERKRIEG UND SPIONAGE

Der Propaganda-Krieg der sozialen Medien ist nur eine Facette des Hybridkrieges. Er umfasst auch andere Arten der Intervention mit Hilfe des Internets, von der Lahmlegung von Wahl-

¹⁴Arendt, Hannah: Elemente und Ursprünge Totaler Herrschaft (Frankfurt/Main, 1955).

ämtern oder Kernenergie-Laboren bis zur Spionage durch Hackerangriffe reichen kann. Dies kann physische Sabotageakte durch elektronische ersetzen.¹⁵ Auch hier sind unsere rechtstaatlichen Gesellschaften schwächer als solche, die das Völkerrecht missachten. So schließt etwa die Bundesrepublik Deutschland in ihrer Nationalen Sicherheitsstrategie von 2023 explizit aggressive Gegenmaßnahmen wie Desinformation aus. Auch „Hackbacks“ lehnen wir als Mittel der Cyberabwehr prinzipiell ab.¹⁶ Auch Ermordungen von gegnerischen Führern sind unter den europäischen Staaten tabu, waren es auch seit der Präsidentschaft Ronald Reagans in den USA; diese Einstellung ist aber mit der Möglichkeit gezielter Tötungen durch Drohnen gewichen, wie etwa der des iranischen Generals Qasem Soleimani 2020. Israel macht von diesem Mittel ebenfalls ausgiebig Gebrauch.

Spionage selbst ist in den offenen Gesellschaften nur dann verpönt, wenn sie von Gegnern (oder Bündnispartnern) gegen uns betrieben wird. Die Überzeugung scheint weit geteilt zu sein, dass es nötig ist, sie abzuwehren, und dass ideologisch motivierte Spione im gegnerischen Land Helden sind, die für unsere Sache kämpfen. Spionage, die auf dem Abhören gegnerischer Kommunikation beruht oder aus Bildern aus dem All und anderen technischen Mitteln, empören westliche Bürger nur, wenn sie gegen ihre eigenen Länder gerichtet sind. Würde aufgedeckt, dass westliche Geheimdienste Ähnliches in Russland oder China bewerkstelligen könnten, würde dies eher als Erfolg gesehen. Eine Prise Machiavellismus ist durchaus mit der Verteidigung der offenen Gesellschaft zu vereinbaren.

IV. Wie der Krieg gesehen wird

Kommen wir ganz konkret zur europäischen Sicht des Krieges. Im 19. Jahrhundert florierte nicht nur auf deutschem Boden, sondern auch in den Republiken Frankreich und Amerika oder im demokratischen Großbritannien die Meinung, dass Krieg nun einmal zur Natur gehöre, Teil der condition humaine sei. In dieser Bewusstseinslage ist Russland aber heute noch. Wie Putin am 28. Jan 2020 auf dem World Economic Forum in Davos verkündete,

“Wir alle wissen, dass der Wettbewerb und die Rivalität zwischen den Ländern

in der Weltgeschichte nie aufgehört haben, nicht aufhören und auch nicht aufhören werden. Differenzen und Interessenkonflikte sind auch für ein so kompliziertes Gebilde wie die menschliche Zivilisation ganz natürlich.”¹⁷

In dieser sozialdarwinistischen Sichtweise der Welt, die über den Umweg des Marxismus-Leninismus mit seinem Glauben an den unausweichlichen Krieg, solange die ganze Welt noch nicht kommunistisch geworden ist, im 19. Jahrhundert steckengeblieben ist, ist der Krieg auch weiter ein Instrument der Machtpolitik. Auch können Instabilität und Konflikte in der Nachbarschaft dienlich sein, denn dies erlaubt einer Großmacht, ihre Hegemonie in der Region zu befestigen.

Obwohl der Krieg über Jahrhunderte in Europa eine alljährliche Unternehmung war, gibt es eine in die Antike zurückzuführende Tradition, den Krieg als Ausnahmezustand zu sehen. Wie der britisch-amerikanische Strategie Colin S. Gray unterstrich: Wenn westliche Staaten einschließlich der USA seit 1945 in einen Auslandseinsatz gerieten, so wollten sie sich so bald wie möglich wieder zurückziehen; dass dies dann nicht die Realität wurde, steht auf einem anderen Blatt. Während Autokratien lang andauerndes Chaos jenseits der eigenen Grenzen gerne zur Einflussnahme ausnutzen, bevorzugen die Handel-treibenden Demokratien zu diesem Zweck Stabilität.

Seit den 1920er Jahren spätestens geht es europäischen Demokratien nicht mehr darum, ihren Landbesitz zu vermehren. Sogar bei den Interventionskriegen der USA seit 1991 war meist schon gleich von einer „Exit-Strategie“ die Rede. Als „Weltpolitisten“ fühlten sich die drei westlichen permanenten Mitglieder des UN Sicherheitsrats USA, Großbritannien und Frankreich auch nach Ende des Kalten Krieges zwar immer wieder verpflichtet, in regionalen Konflikten einzugreifen und Frieden zu stiften oder – oft zu spät – Massaker zu verhindern, aber generell ohne eigenes Interesse an Territorialgewinn. In europäischen Demokratien ist das Mantra, wie es auch in der UN-Charta zu lesen ist, dass der Krieg eine Plage ist, zur Grundüberzeugung geworden. Um so schockierender ist es für Bürger europäischer Gesell- ➤

¹⁵Stoddart: Russia's Hybrid Warfare Offensive

¹⁶<https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf>, S. 62.

¹⁷Session of Davos Agenda 2021 online forum • President of Russia, eingesehen am 2. Februar 2026.

schaften, dass mit Donald Trump eine amerikanische Regierung es den expansionistischen Mächten Russland und China gleich tut und Territorialgewinn anvisiert.

V. Staat, Bürger, Wehrpflicht: Sichtweisen der Demokratien

Die Wehrpflicht wurde von der französischen Revolution in Verbindung mit Volks-Souveränität als Pflicht des Bürgers definiert. Seither ist Frankreich ein besonders gutes Beispiel der vielseitigen Sichtweisen auf die Wehrpflicht in Demokratien. In den sukzessiven französischen Republiken des 19. Jahrhunderts kam eher rechts im politischen Spektrum das Argument auf, dass eine solche Pflicht nicht mit der bürgerlichen Freiheit zu vereinbaren sei. Zugespitzt wurde argumentiert, dass der grobe Tagelöhner oder Bauernknecht die Wehrpflicht als weniger belastend empfände als der Städter (ganz zu schweigen von den verwöhnten Söhnen der Großbourgeoisie).

Bald schon wurde ein sehr in-egalitärer Kompromiss gefunden: die Möglichkeit für Reiche, sich vom Wehrdienst freizukaufen, und andere dafür zu bezahlen, sie für einen zu erfüllen. Dies war schon zu römischen Zeiten geschehen, und wieder im Mittelalter, aber dieser Kompromiss stand im Kontext moderner Demokratien im krassen Gegensatz zum Prinzip der Gleichheit. Diese Grundspannung zwischen Freiheit und Pflicht hindert auch heute im Gefahren-trächtigen internationalen Kontext viele westliche Demokratien daran, zur Wehrpflicht zurückzukehren.

Die Wehrpflicht kann allerdings als Instrument der sozialen Integration betrachtet werden, da sie Menschen aus verschiedenen sozialen und ethnischen Hintergründen zusammenbringt und sie zu einem gemeinsamen Zweck ausbildet. Dies könnte zur Förderung nationaler Einheit und Zusammenhalt beitragen, ein Argument, das insbesondere in Europa, wo die Bevölkerungsproportion mit Migrationshintergrund stetig anwächst, von Interesse sein könnte. Weiter kann man argumentieren, dass die Verteidigung eine zu wichtige Aufgabe ist, um sie ganz einer Untergruppe der Bevölkerung – den Militärs – zu überlassen.¹⁸ Hier ist ein grundsätzliches Misstrauen dem Militär gegenüber impliziert, meist aus der linken Seite der Politik stammend, da es auch in Demokratien kollektiv politisch eher Rechts als Links ist.

Die Wehrpflicht gibt jungen Staatsbürgern einen Einblick in das Militär und einen Blick hinter die Kulissen, wo republikfeindliche Ideen herrschen könnten, um diese dann anzuprangern und zu bekämpfen. Insgesamt bleibt die Frage der Wehrpflicht in offenen Gesellschaften ein komplexes und kontroverses Thema, das verschiedene politische, soziale, ökonomische und ethische Überlegungen berührt. Die Diskussion über die Frage wird dabei von der jeweiligen nationalen Sicherheitslage, der historischen Erfahrung, der militärischen Tradition und den politischen Prioritäten beeinflusst.

Autoritäre Regime brauchen eine solche Diskussion und etwa Opposition zur Wehrpflicht nicht im gleichen Maße zu fürchten. Dennoch kann man sehen, dass sogar der russische Präsident Vladimir Putin für seinen Ukraine-Krieges bislang von einer allgemeinen Wehrpflicht abgesehen hat, und lieber Söldner aus Nordkorea und aus dem Mittleren Osten anheuert.¹⁹ Dadurch sind seine Landsleute wenig von dieser „besonderen militärischen Operation“ betroffen.

Noch im Herbst 2021, also vor der russischen Großoffensive gegen die Ukraine, meinten bei einer Befragung der Friedrich Ebert Stiftung 54% der Russen, ihr Land habe nicht die Stellung in der Welt, die ihm gebühre. Damit lagen aber die Russen weit hinter den Türken (82%!), den Serben und Ukrainern (jeweils 79%) und den Armeniern, Italienern und Polen zurück (jeweils 72%, 68% und 57%). 65% der russischen Befragten meinten, Russland sei „Teil der europäischen Kultursphäre“, während dies nur 57% der Briten und 62% der Norweger meinten. Insgesamt fanden damals 75% der befragten Russen, Russland solle am besten Konflikte im Ausland friedlich regeln.

Es befanden zwar 47% der befragten russischen Männer (aber nur 24% der Frauen), Russland habe durchaus das Recht, zur „Selbstverteidigung“ Militäraktionen in anderen Ländern durchzuführen; insgesamt waren 47% aber dagegen und nur 35% dafür. 75% der befragten Russen befanden, ihr Land solle doch mit allen Ländern zusammenarbeiten, wenn die friedlich seien, auch wenn sie andere Werte haben – das fanden nur 53% der Deutschen, 54% der Franzosen, und 52% der Amerikaner (obgleich es die Nationalen Sicherheitsstrategien aller drei Länder seit 2022 eher so sehen wie die Russen!). Dennoch verteidigten im Herbst 2021 die befragten Russen mehrheitlich, aber nicht >

¹⁸Berühmt für diesen Ausspruch ist 1887 der französische Staatsmann Georges Clemenceau geworden, der meinte, « La guerre ! C'est une chose trop grave pour la confier à des militaires »

¹⁹Margarete Klein: „Wie Russland für einen langen Krieg rekrutiert: Verdeckte Mobilisierung über »Freiwillige«, Vorbereitung einer neuen Mobilmachung“, SWP-Aktuell 2024/A 26 (07.06.2024), <https://www.swp-berlin.org/publikation/wie-russland-fuer-einen-langen-krieg-rekrutiert>, eingesehen am 04. VII. 2024.

mit überwältigender Mehrheit, die russische Ukrainepolitik. 57% meinten, die USA seien die größte Bedrohung für den Frieden in Europa und 55% fanden, der Ukraine-Konflikt sei die Schuld der Ukraine, 51% beschuldigten (auch) die USA, und nur 16% suchten die Schuld bei Russland. (Es ist noch abzuwarten, wie sich seit 2025 die freundliche Zuwendung Trumps an Putin auf die russische Propaganda auswirken wird.) Während 2019 noch über die Hälfte der Befragten die Schuld ebenfalls bei der EU suchten, waren dies 2021 nur noch 19%. 73% waren 2021 der Meinung, die Krim sei legal von Russland annektiert worden.²⁰

2025 fürchteten 61% der von der Friedrich Ebert Stiftung befragten Russen einen Weltkrieg, so wie 58% der Georgier, 43% der Deutschen, 40% der Italiener, aber nur 20% der Ukrainer (die offensichtlich an der Hilfe der Westmächte verzweifelten), 27% der Amerikaner, 28% der Franzosen und Polen, sowie 34% der Briten.²¹

VI. Wie führen Demokratien Krieg?

Die Behauptung, dass ein Nexus bestünde zwischen der Verfassung eines Staates und seiner Art Krieg zu führen, kann bis in die Antike zurückverfolgt werden. Aristoteles schrieb in seiner "Politik" (VII.7) verschiedenen Ethnien oder Rassen verschiedene Stile der Kriegführung zu. Montesquieu brachte Anfang des 18. Jahrhunderts Unterschiede im Stil der Kriegführung mit verschiedenen Staatsverfassungen in Verbindung, wobei Republiken seiner Meinung nach milder mit Gegnern umgingen als Tyraneien. Solche Gedanken wurden von Guibert und Henry Lloyd Mitte des 18. Jahrhunderts aufgegriffen. Clausewitz wiederum konstatierte, ohne zu werten: „Halbgebildete Tataren, Republiken der alten Welt, Lehnsherren und Handelsstädte des Mittelalters, Könige des achtzehnten Jahrhunderts, endlich Fürsten und Völker des neunzehnten Jahrhunderts: alle führen den Krieg auf ihre Weise, führen ihn anders, mit anderen Mitteln und nach einem anderen Ziel...“.²² Was Ausschreitungen gegen die Zivilbevölkerung anbetrifft, kann man allerdings leider nicht sagen, dass sich das Verhalten von Demokratien in den Kriegen des 20.

Jahrhunderts qualitativ völlig von dem von Tyraneien unterschied. Generell haben demokratische Regimes Kriegsgefangene nicht verhungern lassen oder direkt umgebracht. Aber in der Zwischenkriegszeit wurden Maßnahmen wie die Bekämpfung von Aufständen in den Kolonien durch die Bombardierung von Dörfern aus der Luft von den Demokratien Frankreich und Großbritannien ebenso angewandt wie von den faschistischen Regimes Spaniens und Italiens. Dies gilt ebenso für die Städtebombardierung im Zweiten Weltkrieg durch Großbritannien und die USA, und noch danach, im Korea- und Vietnamkrieg. Man kann auch nicht sagen, dass zivile Opfer dabei nur unbeabsichtigte Kollateralschäden waren, wie die Forschung Richard Overys belegt.²³

In der Hoffnung, die „Moral“ der gegnerischen Nation zu brechen, wurden etwa im Zweiten Weltkrieg von der Royal Air Force absichtlich Wohngebiete bombardiert.²⁴ Schon die Hungerblockade der britischen Marine gegen Deutschland im Ersten Weltkrieg betraf besonders Zivilisten. Vergewaltigungen von Frauen gehen auf das Konto von Soldaten aller Länder, allerdings in quantitativ verschiedenen Größenordnungen, und die Militärjustiz der Demokratien ging auch solchen Straftaten sehr viel gewisserhafter nach.²⁵ Auch andere Gräueltaten wurden vereinzelt von den Soldaten Demokratien ausgeübt, wie das Foltern von Gefangenen in Kriegen des frühen 21. Jahrhunderts. Auch da kann man immerhin quantitative Unterschiede feststellen, vor allem seit der zweiten Hälfte des 20. Jahrhunderts. Wiederum kommt die Selbstkritik in der offenen Gesellschaft zum Tragen.

VII. Auswirkungen auf die Dialektik des Krieges: Demokratien vs. autoritäre Systeme

Wie wirken sich all diese Unterschiede auf die Dialektik des Krieges aus? Seit der Finanzkrise von 2008 hat es, in Analogie zu den Effekten des Wall Street Crash von 1929 (allerdings abgefedert von den europäischen Sozialstaaten) ein Aufblühen von Nationalismus und populistischen Parteien gegeben, verschlimmert >

²⁰<https://peace.fes.de/security-radar-2022>

²¹<https://www.fes.de/security-radar-2025#c403845>

²²Beatrice Heuser: 'The Conceptual Heritage of Strategic Culture and Collective Mentality' in Jeannie Johnson, Kerry Kartchner, and Briana D. Bowen (eds): Routledge Handbook of Strategic Culture, Abingdon: 2023, S. 17–30.

²³Richard Overy: The Bombing War: Europe 1939–1945, New York: 2013.

²⁴Richard Overy: "Operation Gomorrah: Ruthlessness and the British Air War 1943", in David Trim und Brendan Simms (Hrsg.), Harfleur to Hamburg: Five Centuries of English and British Violence in Europe, London: 2024, S. 219–236.

²⁵Michèle Battesti: « Le viol: une arme multiséculaire ? », in Jean Baechler & Marion Trévisi (Hrsg.): La Guerre et les Femmes, Paris: 2018, S.120–140.

durch die finanziellen Auswirkungen der Covid-19 Krise, gestiegene Energie- und Lebensmittelpreise seit 2022. Heute lebt die Mehrheit der Menschheit nicht in offenen Gesellschaften. Sukzessive Regierungen der USA haben in ihren Nationalen Sicherheitsstrategien zugestanden, dass ihre Macht relativ zum Rest der Welt abnimmt. Europa auf der anderen Seite des Atlantik ist zwar wirtschaftlich stark, aber militärisch schwach.

Die multiplen Schwächen der offenen Gesellschaft treten in diesem Kontext besonders zutage. Wir verstehen unsere Gegner schlecht oder gar nicht, weil wir unsere eigene Aversion gegen Krieg, aber auch unsere relative Zufriedenheit mit dem Status quo (in dem unser Einkommen und soziale Sicherheit verglichen mit dem der meisten anderen Länder hoch sind) auf die gesamte Menschheit projizieren. Wir selbst sind weiterhin willens, den Krieg nicht als Mittel unserer Politik zu betrachten; in der Tat ist dies zu einem unserer wichtigsten gemeinsamen Werte geworden. Als Demokratien sind unsere Entscheidungsprozesse sehr langsam und juristisch geprägt, wobei wir entscheidungsunfähig sind, wenn kein klarer Rechtsfall vorliegt. Als offene Gesellschaften debattieren und kritisieren wir endlos unsere eigenen Regierungen, mit disproportional ausgeprägtem Hang zur Selbstkritik. Und weil wir eine offene Gesellschaft sind, liegen unsere Schwächen offen zutage, werden in den freien Medien und in der wissenschaftlichen Literatur diskutiert.

Trotz ihrer Wurzeln im Christentum sind unsere heutigen Werte das, was über Jahrhunderten von Menschen debattiert wurde und heute juristisch verankert ist – wir berufen uns nicht auf eine metaphysische Autorität. Dagegen ist es eine Stärke unserer Gegner in autoritären Systemen, dass sie sich auf solche Autoritäten berufen, ob das nun Gott oder Allah ist, oder Marxismus-Mao.

Autoritäre Regierungen können sehr viel schneller Entscheidungen treffen als wir, denn Tyrannen brauchen keine anderen Minister oder Juristen zu konsultieren. Sie können Kritiker zum Schweigen bringen, durch Verhaftung oder eine Prise Nowitschok. Sie können auch ungestraft lügen, den Zugang ihrer Bürger zum Internet beeinträchtigen oder abschalten, und zumindest ohne Kritik aus eigenen Reihen Cyberkrieg führen. Sie können die Medien und die Unterhaltungsindustrie zur Unterstützung ihrer eigenen Propaganda konfigurieren und damit die Gehirnwäsche der Nation vorantreiben. Kurzum, Autokratien haben es leicht, sich über die Präferenzen der eigenen Bevölkerung hinwegzusetzen, offene Gesellschaften dagegen nicht. ■

02_Insight

Vorsprung durch Erkenntnis

„Intelligence is about understanding competition, understanding how knowledge is distributed across that competition, and then gaining decision advantage.“

Jennifer E. Sims, USA

Illustration Grafissimo/iStock



Was, wenn Intelligence weniger mit Wissen als mit Nichtwissen zu tun hat? Die Politikwissenschaftlerin und Künstlerin Jennifer E. Sims, langjähriges Mitglied der US Intelligence Community, über echte Entscheidungsstärke, die aus dem bewussten Umgang mit Unsicherheit entsteht.

„Gewissheit ist gefährlich.“

„Intelligence ist kompetitives Lernen.“

Jennifer E. Sims

Jennifer Sims, welche Art von Wissen erzeugt Intelligence – und auf welche Art von Wissen sollte sie abzielen?

Jennifer Sims: Viele Menschen glauben, dass es bei Intelligence um Wahrheitssuche geht. Diese Vorstellung ist tief verankert. Sie ist sogar wörtlich in Stein gemeißelt – an der Wand der Central Intelligence Agency in den Vereinigten Staaten, in Form eines Bibelzitats: „*And you shall know the truth, and the truth shall make you free.*“ Das klingt, als sei dies der Auftrag von Intelligence. Aber das ist er nicht. Intelligence ist kompetitives Lernen. Es geht darum, Konkurrenz zunächst überhaupt zu verstehen, zu begreifen, wie Wissen innerhalb dieses Wettbewerbs verteilt ist, und daraus Entscheidungsvorteile zu gewinnen. Ganz einfach gesagt: Es geht darum, mehr zu wissen als der Gegner oder der Wettbewerber. Nicht alles – aber mehr von dem, was zählt.

Also geht es bei Intelligence nicht darum, zu erkennen, wie die Welt „wirklich“ ist?

Nein, jedenfalls nicht in diesem umfassenden Sinn. Intelligence erzeugt begrenztes Wissen. Sie erzeugt genau das Wissen, das hilft zu gewinnen – oder zumindest zu vermeiden, zu verlieren. Im besten Fall kann sie sogar Win-win-Ergebnisse ermöglichen, indem sie versteht, was die andere Seite in einem Konflikt tatsächlich will, und Wege findet, diese Interessen zu den geringstmöglichen Kosten zu bedienen. Wird Intelligence auf diese Weise global

praktiziert, kann sie eine Form politischer Transparenz schaffen. Diese Transparenz kann Kriege verhindern, die aus Fehlwahrnehmungen entstehen. Sie wird jedoch nicht alle Kriege verhindern, denn Intelligence zielt nicht auf Allwissen. Sie ist eine sehr schmale, fokussierte Form des Wissens.

Sie lehnen sehr deutlich die Vorstellung ab, Intelligence über das Handeln von Geheimdiensten zu definieren.

Genau. Intelligence gab es lange bevor moderne Geheimdienste entstanden. Deshalb darf unser Verständnis von Intelligence nicht auf das beschränkt werden, was diese Institutionen tun. Moderne Nachrichtendienste sind zu einem bestimmten historischen Zeitpunkt entstanden und haben ihre Aufträge auf spezifische Weise definiert. Doch daraus folgt nicht, dass ihre Tätigkeiten definieren, was Intelligence an sich ist. Mein Ziel war es, Intelligence in einem weiteren, grundsätzlicheren Sinn zu denken.

Warum ist es irreführend, Intelligence als Wahrheitssuche zu begreifen? In Ihrem Buch verwenden Sie ein Tierbeispiel – war es nicht ein Bär?

Es war ein Hirsch. Aber Ihre Verwechslung bestätigt eigentlich meinen Punkt. Natürlich hat Intelligence immer auf Zuverlässigkeit (accuracy) gezielt. Zuverlässige Information zu suchen, ist Teil des Erlangens von Vorteil. Es gibt Wahrheit in der Intelligence – aber nicht Wahrheit mit großem „W“. Die tiefere Vorstellung von Wahrheit, die

INTERVIEW_ Jennifer E. Sims

Dr. Jennifer E. Sims arbeitete in leitenden Funktionen im US-Sicherheitsapparat, u. a. im US Senate Select Committee on Intelligence und als Geheimdienst-Koordinatorin im State Department. Auch lehrte sie an der Georgetown University. 2022 erschien ihr Buch *Decision Advantage*. Sie ist zudem Künstlerin und Gründerin des Stuart Street Atelier.

KEY MESSAGES

- **Intelligence** ist keine Wahrheitssuche, sondern kompetitives Lernen, um Entscheidungsvorteile zu gewinnen.
- **Sie erzeugt begrenztes Wissen** – ausreichend, um Niederlagen zu vermeiden oder Erfolg zu ermöglichen.
- **Der Kern von Intelligence** liegt im Verschieben von Unsicherheit, nicht in ihrer Beseitigung.
- **Übermäßige Abhängigkeit** von Prognosen und KI erzeugt gefährliche Gewissheitsillusionen
- **Wirksame Intelligence** braucht imaginative Vielfalt, um blinde Flecken aufzudecken

wir aus Philosophie oder Theologie kennen, zielt auf universelle Prinzipien und eine allwissende Perspektive, eine Art göttlichen Blick auf die Realität. Wenn Intelligence das anstrebt, versagt sie gegenüber den Entscheidungsstrategien. Diese suchen keine Allwissenheit. Sie wollen gewinnen – oder zumindest eine Niederlage vermeiden. Dafür braucht es nur eine begrenzte Menge an Information: genug, um ein Urteil zu fällen, das Verlust verhindert.

Wie hilft das Hirsch-Beispiel, diesen Punkt zu erklären?

Ich verwende diese Analogien, weil viele Menschen Intelligence mit dem gleichsetzen, was Geheimdienste tun – Drohnenschläge, verdeckte Operationen, Spezialmissionen. Das sind Aufgaben von Institutionen, nicht von Intelligence selbst. Stellen Sie sich einen Jäger und einen Hirsch vor. Auf der offenen Wiese hat der Jäger einen klaren Vorteil. Er sieht weit, verfügt über eine Fernwaffe und ist erfahren. Der Hirsch jedoch kann in den Wald fliehen. Dort verliert der Jäger die Sicht. Die Tarnung des Hirsches wirkt zu seinen Gunsten. Der Hirsch hat nichts Neues gelernt. Er hat das Terrain der Unsicherheit verschoben. Es geht also nicht darum, mehr Fakten zu sammeln, sondern Unsicherheit so zu verschieben, dass sie zu deinem Vorteil wirkt und nicht zu deinem Nachteil. Vergessen wir das, verlieren wir die Dimension der Counterintelligence (Abwehr) völlig aus den Augen. Und wir verfehlen den eigentlichen Zweck von Intelligence: die Interaktion beider Seiten in jedem Wettbewerb zu beeinflussen, indem relative Wissens- und Handlungsvorteile geschaffen werden.

Und wenn man diese Analogie weiterdenkt – was bedeutet relativer Vorteil konkret?

In diesem Fall passt sich der Jäger an, indem er einen Hochsitz baut und in einen Baum steigt. Er verbessert seine Sicht und gewinnt einen Teil seines Vorteils zurück. Doch entscheidend ist, was hier geschieht: Beide Seiten passen sich ständig an. Intelligence ist die Fähigkeit zu wissen, wie man konkurriert – indem man Unsicherheit verschiebt und Informationen schneller oder wirksamer sammelt und auswertet als die Gegenseite.

zepte. Heute herrscht oft die Überzeugung, Vorhersage sei die wichtigste Aufgabe von Intelligence: Sie solle sagen, was die Zukunft bringt. Das ist gefährlich, weil es voraussetzt, dass Intelligence mit etwas Statischem zu tun hat. Wettbewerb ist jedoch niemals statisch. Er entfaltet sich in Echtzeit. Er bewegt sich. Er reagiert. Nehmen wir wieder den Jäger und den Hirsch. Analysiert man die Situation als eingefrorenen Moment – ein erfahrener Jäger auf

„Auch in asymmetrischen Situationen, in denen eine Seite nach allen konventionellen Maßstäben schwächer ist, kann sie gewinnen.“

Jennifer E. Sims

Das ist eine Form von Macht, die wir häufig übersehen. Macht wird meist in Ressourcen, Bevölkerung oder Waffen gemessen. Doch selbst in asymmetrischen Situationen, in denen eine Seite nach allen konventionellen Maßstäben schwächer ist, kann sie gewinnen. Der Hirsch verfügt über weit weniger Fähigkeiten als der menschliche Jäger – und entkommt dennoch. Nicht durch Stärke, sondern durch ein instinktives Verständnis dafür, wie der Wettbewerb auf ein Terrain verlagert werden kann, auf dem er im Vorteil ist. Das ist im Kern Intelligence.

Aber erfordert dieser Ansatz nicht letztlich so etwas wie perfekte Vorhersage?

Diese Annahme ist sehr verbreitet – und genau hier liegt einer der zentralen Denkfehler moderner Intelligence-Kon-

einer Wiese mit einem leistungsstarken Bogen –, lassen sich sehr überzeugende lineare Prognosen darüber erstellen, wer gewinnen wird. Wenn man nicht berücksichtigt, dass der Hirsch plötzlich in den Wald fliehen könnte, wirkt diese Prognose stabil. Doch der Hirsch denkt ebenfalls. Er reagiert. Und sobald man all diese Wechselwirkungen einbezieht, wird der Versuch, alles vorherzusagen, zu einem törichten Unterfangen.

Das Problem ist also nicht der Mangel an Daten, sondern der Charakter der Situation selbst?

Genau. Was der Jäger wirklich braucht, ist nicht perfektes Wissen über jede einzelne Variable, sondern das Bewusstsein für eine entscheidende Möglichkeit: dass der Hirsch in den Wald fliehen könnte. Diese eine Einsicht >

wiegt schwerer als jede noch so ausgefeilte Vorhersage. Intelligence sollte sich darauf konzentrieren, wie sich Unsicherheit verschieben kann – statt auf die Illusion, man könne Unsicherheit vollständig beseitigen.

Ich mag ein weiteres, leicht spielerisches Beispiel aus dem Film *Jäger des verlorenen Schatzes*. Ein Schwertkämpfer stellt sich dem Protagonisten auf einem Marktplatz entgegen. Nach allen sichtbaren Maßstäben – Grad des Könnens, der Bewaffnung und der aktuellen Situation – müsste der Schwertkämpfer gewinnen. Eine traditionelle Intelligence-Analyse würde genau diese Bedrohung bewerten und eine Niederlage prognostizieren. Sie läge falsch, weil sie das Unsichtbare ausblendet: die Pistole in der Tasche des Protagonisten, die die Begegnung augenblicklich beendet.

Ist Intelligence also gescheitert, weil sie nur nach außen geblickt hat?

Ja. Genau das geschieht häufig in Geheimdiensten, insbesondere in Demokratien. Sie sind darauf trainiert, Bedrohungen überall zu messen. Sie schätzen ein und treffen Vorhersagen, indem sie ausschließlich den Gegner betrachten. Gleichzeitig ist es ihnen oft nicht erlaubt, den Entscheidungsträger, dem sie dienen, mit derselben Tiefe zu verstehen. Sie wissen nicht, über welche Werkzeuge, Optionen oder Absichten dieser verfügt. Wenn eine starre Trennung zwischen Intelligence und Entscheidungsfindung besteht, vervielfältigen sich Intelligence-Produkte in Form von Prognosen, Schätzungen und Warnungen, die für den tatsächlichen Bedarf des Entscheidungsträgers irrelevant sind. Das Ergebnis ist ein überwältigendes Bedrohungsbild, das eher erschreckt als leitet.

Können Sie dafür ein konkretes historisches Beispiel nennen?

sches Beispiel nennen?

Ja – ein tragisches: den Irakkrieg 2003. Intelligence-Schätzungen konzentrierten sich darauf, was der Irak haben könnte und was er tun könnte – Urananreicherung, Yellowcake, Worst-Case-Szenarien. Alles folgte linearer Projektion: wie gefährlich Saddam Hussein wäre, falls diese Fähigkeiten existierten. Wir fixierten uns auf die Klinge und den Schwertkämpfer. Der Krieg zeigte jedoch, dass die Waffen nicht existierten. Irakische Diplomaten fragten, was sie beweisen könnten. Die Antwort lautete: nichts. Bloßer Glaube hatte die Untersuchung ersetzt.

Intelligence sollte sich weniger auf große Gesamteinschätzungen konzentrieren und stärker auf Informationsgewinnung: darauf, spezifisches Nichtwis-

Ziele auf eines: eine Landung zu verhindern. Indem sie das Terrain der Unsicherheit gestaltete, gewann sie einen entscheidenden Vorteil – das ist ein Ansatz, den heutige Regierungen weitgehend verlernt haben.

Könnten Sie das genauer erläutern?

Regierungen – insbesondere in den Vereinigten Staaten – sind nicht darauf trainiert, das Terrain der Unsicherheit zu kartieren. Vorhersage und Einschätzung werden auf falsche Weise eingesetzt. Ich mag das Wort „Vorhersage“ nicht, auch wenn es begrenzte Fälle gibt, in denen es sinnvoll ist. Man kann zum Beispiel vorhersagen, dass ein Hirsch bei Gefahr in den Wald flieht, weil die Erfahrung zeigt, dass Hirsche so handeln. Aber das ist eigentlich keine Intelligence. Das kommt eher

„Heutige Regierungen sind nicht darauf trainiert, das Terrain der Unsicherheit zu kartieren.“

Jennifer E. Sims

sen zu reduzieren und Unsicherheit zu kartieren – wer weiß was, wo ist Wissen schwach, und wo liegt der Vorteil. Strategische Intelligence ist einschätzend (estimative), aber nicht statisch. Als Jäger fragt man nicht, was passiert, wenn man hier stehen bleibt. Man fragt, wo man einen Vorteil gewinnt. Man meidet den Wald. Man wählt die Wiese. Genau das verstand Elisabeth I., als sie Philipp II. und der spanischen Armada gegenüberstand. Sie verlagerte den Kampf in den Ärmelkanal, wo ihre Flotte Vorteile hatte, und begrenzte ihre

einer wissenschaftlichen Regelmäßigkeit nahe. Intelligence beginnt erst, nachdem der Hirsch im Wald ist. Was dann geschieht, lässt sich nur schwer vorhersehen. Es erfordert Einschätzung, Urteilsvermögen und kontinuierliche Anpassung. Das ist der schwierigste Teil – und zugleich der wichtigste.

Was hat Sie zur Kunst geführt, speziell zur figurativen Malerei und zur klassischen Ölmalerei? Und wie hängt das mit dem „Intelligence-Teil“ Ihrer Laufbahn zusammen?

Das ist eine tiefgehende Frage. Ein >

Teil der Krise, vor der wir heute stehen – national und vielleicht global –, ist das Fehlen einer künstlerischen Sensibilität, dessen, was ich den *art spirit* nennen würde. Kunst lädt uns ein, uns mit Schönheit, innerer Tiefe, Form, Struktur und Proportion auseinanderzusetzen und Probleme auf eine Weise zu lösen, die sich grundlegend von analytischem oder bürokratischem Denken unterscheidet.

Klassische Traditionen betonten Proportion und Resonanz, fast in mathematischem Sinn. Moderne Kunst hingegen verweigert oft jede einfache Bedeutungszuweisung. Sie verlangt Kontemplation. Menschen fühlen sich zunächst vielleicht abgestoßen, wenn sie vor einer scheinbar leeren Leinwand stehen und fragen, warum das Kunst sein soll. Aber wenn sie bleiben, entdecken sie möglicherweise eine Antwort. Dieser Akt der Betrachtung ist entscheidend. Das führt direkt zur Frage des Nichtwissens – dessen, was wir wissen, und dessen, was wir nicht wissen. Kunst ist eine Möglichkeit, das Unbekannte zu erkunden. Beim Schaffen beginnen wir mit persönlicher Erfahrung; wenn das Werk bei anderen Resonanz findet, entsteht eine nicht-verbale, nicht-hierarchische Form gemeinsamen Sinns. Ein großer Teil meines früheren Lebens war von Autorität geprägt: Wissenschaft, Regierung, Doktrin. Das sind

legitime Formen des Wissens. Doch vor all dem war ich Tänzerin – und heute bin ich Künstlerin. Als ich aus dem Staatsdienst ausschied, entschied ich mich, Malerei als eine Form des Wissens zu studieren. Das ist keine Abkehr von meiner Vergangenheit, sondern ihre Fortführung.

Viele Menschen im Westen empfinden die politische und gesellschaftliche Lage als absurd, ja grotesk. Läuft Kunst vor diesem Hintergrund nicht Gefahr, bedeutungslos zu werden?

Ich glaube nicht, dass Kunst jemals nutzlos ist. Sie existiert um ihrer selbst willen. Politische oder persuasive Kunst interessiert mich nicht besonders; sie gehört in eine andere Kategorie und funktioniert oft wie Propaganda. Für mich ist Kunst in zeitloser Schönheit und Tugend verankert. Sie ist eine Form des Erkennens, nicht der Einflussnahme – und gerade deshalb überdauert sie, selbst inmitten politischer Absurdität. In den Vereinigten Staaten hat das Bildungssystem zunehmend Mathematik und Naturwissenschaften privilegiert. Diese Disziplinen sind wichtig, werden aber häufig ohne schöpferische Praxis oder innere Erkundung vermittelt. Kunst lehrte uns einst, zu fragen, was richtig oder wahr ist, uns selbst durch das Machen zu entdecken und Kritik anzunehmen, ohne defensiv zu werden. Zivilisationen gedeihen nicht

durch eine einzige Form des Wissens, sondern durch viele.

Deshalb möchte ich ein Projekt des Nichtwissens verfolgen. Zivilisationen entwickeln sich, indem sie unterschiedliche Wissensformen integrieren – doch wir hierarchisieren sie und behandeln Wissenschaft als die einzig legitime. Dabei entsteht Vorstellungskraft – Einsteins eigentliches Genie – gerade durch Grenzüberschreitungen, auch durch Kunst. Das Malen eines Auges lehrt Geduld und Sorgfalt, Tugenden, die unsere geschwindigkeitsgetriebene Kultur weitgehend vergessen hat. Wir vergessen auch, dass Einstein einst Patentbeamter war. Seine wichtigste Erkenntnis war nicht überliefertes Wissen, sondern Vorstellungskraft.

Was bedeutet KI für unser Verständnis von Wissen?

Ich habe darauf keine abschließenden Antworten. In vielerlei Hinsicht bin ich selbst eine Anfängerin und versuche, eine Welt zu verstehen, in der sich Informationsverarbeitung in atemberaubender Geschwindigkeit verändert. Künstliche Intelligenz ist außerordentlich leistungsfähig darin, enorme Mengen externen Wissens zu integrieren. Doch sie lernt ausschließlich aus dem, womit sie gefüttert wird – aus menschlichem Wissen, das von Annahmen und Verzerrungen geprägt ist. KI verarbeitet das, was wir zu wissen glauben, nicht das, was wir nicht wissen. Sie kann sich nicht mit Nichtwissen befassen – und genau dort liegt der Kern von Unsicherheit. KI kann uns zeigen, was wir für wahr halten, aber nicht, was uns fehlt.

Das Problem ist also nicht nur Bias, sondern eine strukturelle Begrenzung?

Genau. Und diese Begrenzung wird in einer kompetitiven Welt, in der Staa- ➤

*„Kunst ist eine Möglichkeit,
das Unbekannte zu erkunden.“*

Jennifer E. Sims

ten einander gegenüberstehen, gefährlich. KI wird als geheimdienstliches Instrument eingesetzt werden. Staaten werden versuchen, ihr alles zuzufüttern, was sie über ihre Gegner wissen oder zu wissen glauben. Doch KI ist äußerst schlecht darin, Risiken sichtbar zu machen, die aus Unwissen entstehen. Sie erzeugt immer größere Gewissheit. Und Gewissheit ist gefährlich. Sobald man sicher ist, wird man vorhersehbar. Das ist im Wettbewerb fatal. Ein wesentlicher Teil der Kunst, Entscheidungsvorteile zu gewinnen, besteht darin zu verstehen, was man selbst nicht weiß – und zu gestalten (shape), was der Gegner nicht weiß.

Treibt uns KI also in die entgegengesetzte Richtung?

Ja. Sie beschleunigt Entscheidungsprozesse. Sie komprimiert Zeit. Sie belohnt Geschwindigkeit statt Reflexion. Meine Sorge ist, dass sie die menschliche Fähigkeit verdrängt, innezuhalten, zu zögern, zu spüren, dass etwas nicht stimmt – selbst dann, wenn alle Daten scheinbar konsistent sind.

Versuchen wir es so zusammenzufassen:

Wenn alle Staaten KI nutzen, um das Verhalten ihrer Gegner vorherzusagen, wird Entscheidungsfindung gefährlich, weil alle glauben, die andere Seite vorhersehen zu können.

Das ist nah dran. Die Gefahr liegt nicht nur in wechselseitiger Vorhersehbarkeit, sondern in der Geschwindigkeit, mit der Entscheidungen erzwungen werden. Die Bedenken jener, die spüren, dass etwas nicht stimmt, werden unterdrückt. Diese Bedenken entspringen oft der Intuition, dem Bewusstsein fehlender Puzzleteile. Doch Intuition braucht Zeit. Sie kann in einer Umgebung, die von algorithmischer Gewissheit dominiert wird, nicht überleben.

Denken wir noch einmal an den Irak. Immer mehr Daten über Urananreicherung und Yellowcake in ein KI-System einzuspeisen, hätte das Problem nicht gelöst. Was gebraucht wurde, war eine Pause. Ein tiefes Durchatmen. Eine andere Frage: Was wissen wir nicht? Woher wissen wir, dass wir es nicht wissen? Und wie könnten wir es herausfinden? KI ist sehr schlecht darin, solche Fragen zu stellen.

Weil künstliche Intelligenz eine Illusion von Gewissheit erzeugt.

Genau. Und wenn auch der Irak selbst über fortgeschrittene KI-Fähigkeiten verfügt hätte, hätte er die Lage in den Vereinigten Staaten möglicherweise so interpretiert, dass ein Krieg unvermeidlich sei. Kein Spielraum mehr. Keine Unsicherheit. Keine Hoffnung. Ich habe dieses Szenario nicht vollständig durchdacht, aber es zeigt, wie schnell Gewissheit zu Schicksal gerinnen kann. Was mich am meisten interessiert, ist der Moment von Führung, der sich dem widersetzt. Der Moment, in dem eine

echte Führungspersönlichkeit innehält und sagt: Hier stimmt etwas nicht. Wir scheinen alles zu wissen – und doch passt etwas nicht. Ich will stoppen. Ich will das Tempo drosseln. Ich will erkunden, was wir übersehen.

Dieser Moment lässt sich nicht automatisieren. Er beruht auf Geduld, Vorstellungskraft, Demut und dem Mut, mit Unsicherheit zu leben. Diese Eigenschaften gehören zum Menschsein. Und wenn wir sie verlieren, werden uns weder mehr Daten noch höhere Geschwindigkeit retten.

Selbst wenn ich für dieses Gefühl keinerlei positive Belege habe.

Ja – genau. Darauf habe ich immer wieder hingewiesen, als ich Führungskräfte im Außen- und Verteidigungsministerium unterrichtet habe. In Krisen leiden Entscheidungsträger häufig nicht an einem Mangel, sondern an einem Übermaß an Informationen. Ab einem gewissen Punkt helfen weder mehr Daten noch größere Teams weiter. Entscheidend ist dann die Frage: Was >

„Ein wesentlicher Teil der Kunst, Entscheidungsvorteile zu gewinnen, besteht darin zu verstehen, was man selbst nicht weiß – und zu gestalten, was der Gegner nicht weiß.“

Jennifer E. Sims

muss ich jetzt wirklich wissen?

Manchmal führt das zu unerwarteten Entscheidungen – sogar dazu, mit einem Gegner zu sprechen. Vor dem Münchener Abkommen 1938 stand Großbritannien vor widersprüchlicher Intelligence über Hitler. Chamberlain traf ihn persönlich – ein Schritt, der später als Appeasement verurteilt wurde. Doch diese Begegnung führte dazu, dass Großbritannien Hitler als Gefahr erkannte und den Kurs änderte. Dieser Wandel entstand nicht aus besserer Analyse, sondern aus Urteilsbildung durch Erfahrung.

Rationale Analyse ist eine Form des Wissens, aber nicht die einzige. Führungskräfte wägen weiterhin Autorität, Quellen und Intuition gegeneinander ab – etwas, womit KI große Schwierigkeiten hat. Wenn KI diesen menschlichen Impuls unterdrückt, kann sie zwar Fehlwahrnehmungen reduzieren, zugleich aber zu einem tiefgreifenden Risiko werden.

Würden Sie sagen, dass es eine eindeutig menschliche Form von Intelligence gibt – in beiden Bedeutungen des Wortes? Nicht nur im Sinne von Geheimdiensten, sondern auch im kognitiven Sinn?

Ja. Ganz eindeutig ja. Das ist das, was ich *inneres Wissen* nenne. Es ist eine Form des Erkennens, zu der Künstler

Zugang haben, die Dichter und Musiker vermitteln – oft ohne sie vollständig erklären zu können. Sie ist nicht analytisch im üblichen Sinn und lässt sich schwer in Worte fassen.

Westliche Gesellschaften tun sich mit dieser Form des Wissens schwer, weil wir nicht gelernt haben, sie zu kultivieren, in diese Tiefen hinabzusteigen und das, was wir dort finden, in unser Leben zu integrieren. Ich glaube, das ist einer der Gründe für die gegenwärtige Faszination für Künstliche Intelligenz. Wir sind so stark auf Berechnung, Effizienz und äußeres Wissen fixiert, dass wir diesen anderen Teil des menschlichen kognitiven Terrains vernachlässigen. Maschinen werden diese Art des Wissens niemals ersetzen. Aber sie können sie irrelevant machen. Und genau das ist für mich die wirklich beängstigende Möglichkeit.

Was Sie beschreiben, erinnert an ältere Traditionen – sowohl westliche als auch östliche. Im antiken Griechenland gab es den Begriff *métis*, eine Form von List oder praktischer Klugheit. Und auch im chinesischen Denken finden sich ähnliche Vorstellungen. Ist das die Richtung, in die Sie denken?

Ja, sehr. Bemerkenswert ist, dass diese Einsicht kultur- und traditionsübergreifend auftaucht. Man findet sie in Reli-

gion, Mystik, Philosophie und sogar in der modernen Psychologie: Lernen durch Stille, durch Zuhören, durch die Fähigkeit, mit Nichtwissen vertraut zu sein. Ob bei Platon, im Gebet, in der Stille oder in C. G. Jungs Vorstellung des Geistes als Filter statt als Quelle des Wissens – der gemeinsame Nenner ist die Hinwendung nach innen. Maschinen werden diesen Bereich niemals erreichen, weil ihnen inneres Leben und Bewusstsein fehlen. Unsere Faszination dafür, ihn zu ersetzen, zeigt, wie sehr wir uns von ihm entfernt haben – und genau das untersucht meine aktuelle Forschung.

Wozu dient Intelligence-Wissen letztlich? Und was darf es niemals werden?

Intelligence darf niemals als Quelle menschlicher Wahrheit verstanden werden. Selbst in Demokratien gibt es innerhalb von Intelligence-Communities die Versuchung, genau diese Rolle zu beanspruchen – oft ausgedrückt in der Formel „*speaking truth to power*“. Diese Wendung impliziert, dass Wahrheit bei professionellen Geheimdienstlern liege und nicht bei den Entscheidungsträgern. Ich halte das für ein gravierendes Missverständnis. Wenn sich diese Vorstellung verbreitet, beginnen Bürger, Intelligence als moralische oder politische Kontrollinstanz ihrer gewählten Führung zu sehen. Doch Intelligence ist keine unabhängige moralische Autorität. Sie ist ein Produkt von Führung. Sie existiert, um Entscheidungsfindung zu unterstützen – nicht um Wahrheit zu schürfen oder zu verkünden.

Und das unabhängig davon, wer an der Spitze steht?

Ja – unabhängig davon, wer der jeweilige Entscheidungsträger ist. Intelligence ist nur so vertrauenswürdig wie die jeweilige Führung, der sie dient. >

„Intelligence darf niemals als Quelle menschlicher Wahrheit verstanden werden.“

Jennifer E. Sims

Wenn Intelligence-Institutionen sich von dieser Rolle entfernen, verschwenden sie Ressourcen. Ich frage oft, warum Behörden globale Zukunftsprognosen über das Schicksal der Menschheit veröffentlichen. Sie tun das, weil sie sich selbst als Wahrheitsinstanzen begreifen. Das ist gefährlich. Geheime Budgets sollten keine quasi-philosophischen Weltdeutungen mit implizitem moralischem Anspruch finanzieren. Intelligence existiert, um in Wettbewerbssituationen Entscheidungsvorteile zu erzielen. Sie produziert Informationen für Handeln, nicht zeitlose Wahrheit. Ihre Produkte sind vorläufig, zeitgebunden und notwendigerweise begrenzt. Ich beobachte mit Sorge eine Tendenz, dass sich Geheimdienste als moderne Orakel von Delphi inszenieren.

Und was ist mit der in Europa verbreiteten Vorstellung, Geheimdienste dienen dem Schutz der Demokratie?

Intelligence kann Demokratie nicht bewahren. Im besten Fall kann sie zur demokratischen Gesundheit beitragen, indem sie sich aus der Politik heraushält. In dem Moment, in dem Intelligence in den politischen Raum eintritt, wird sie gefährlich – denn Informationen, die für Entscheidungsvorteile gedacht sind, lassen sich leicht in politische Waffen verwandeln. Intelligence muss dienen, sie darf niemals herrschen. Geheimdienste dürfen niemals zu Wahlkampfinstrumenten werden oder eingesetzt werden, um die Macht eines Führers zu sichern oder innenpolitische Gegner anzugreifen. Wahlkämpfe betreiben immer eigene Intelligence – das ist ihre Aufgabe. Nationale Intelligence hat eine andere, klar begrenzte Mission: die Unterstützung von Außen- und Verteidigungspolitik. Klare Grenzen sind unerlässlich. Ohne

„Die stärksten Geheimdienste haben stets unkonventionelle Denker einbezogen, statt sie auszusortieren.“

Jennifer E. Sims

sie läuft Intelligence Gefahr, bürokratischen oder parteilichen Interessen zu dienen. In Demokratien wie den Vereinigten Staaten ist ein fragmentiertes Intelligence-System bewusst angelegt. Die Konzentration von Intelligence bei einem Akteur oder einer Weltanschauung untergräbt Neutralität. Intelligence muss allen Entscheidungsträgern gleichermaßen dienen – oder sie hört auf, dem Staat zu dienen.

Von Intelligence bis Kunst haben wir ein weites Feld abgedeckt. Fehlt aus Ihrer Sicht noch etwas?

Die stärksten Geheimdienste haben stets unkonventionelle Denker einbezogen, statt sie auszusortieren. Sie streben nicht nach einem einheitlichen professionellen Denkstil. Sie schätzen Vielfalt im tiefsten Sinn. Vielfalt ist kein Schlagwort, sondern der Kern wirksamer Intelligence. Künstler neben Wissenschaftlern. Migranten mit gelebtem Erfahrungswissen neben akademischen Spezialisten. Philosophen neben Ingenieuren. Praktiker neben Theoretikern. Ohne diese Mischung entwickelt Intelligence blinde Flecken. Nichtwissen ist unvermeidlich – aber nicht zu wissen, dass man nicht weiß, ist fatal. Ein gesunder Dienst ist einer, in dem jemand sagen kann: „Das verstehen wir nicht wirklich“ – und gehört wird. Ohne solche Stimmen werden asymmetrische Konflikte missverstanden und Chancen verpasst. Die heute am meisten vernachlässigte

Figur ist der Künstler. Die britische Gegenspionage im Zweiten Weltkrieg lebte von exzentrischen, fantasievollen Köpfen – Musikern, Zauberkünstlern, unkonventionellen Denkern. Ihre Kreativität war entscheidend.

Intelligence ist nicht dann am stärksten, wenn sie homogen ist, sondern dann, wenn sie über eine vielfältige Vorstellungskraft verfügt. ■

„Mich interessieren Fakten“

„Open Source Intelligence“ (OSINT) gilt als Wundermittel im Informationszeitalter. Doch offene Quellen liefern nur dann Erkenntnis, wenn sie methodisch und verantwortungsvoll ausgewertet werden. Alana Gramm über Intuition, KI, Wahrheit – und demokratische Standhaftigkeit.



Alana Gramm, im Intelligence-Umfeld wird viel über OSINT (Open Source Intelligence) gesprochen. Was genau verstehen Sie darunter?

Alana Gramm: Aus meiner praktischen Erfahrung bedeutet OSINT, offene Informationen zu sammeln, sie zielgerichtet zu analysieren und daraus verwertbare Erkenntnisse zu gewinnen. Viele Daten zu haben hilft niemandem, wenn sie nicht relevant und verständlich aufbereitet sind.

Wo ziehen Sie die Grenze zwischen offenen und nicht offenen Informationen?

Die Grenze verläuft dort, wo man hacken, täuschen oder Schutzmechanismen überwinden muss. OSINT basiert auf Informationen, die öffentlich zugänglich sind. Öffentlich heißt aber nicht zwangsläufig kostenlos oder leicht auffindbar. Ein Buch in einer Bibliothek ist auch öffentlich, obwohl ich einen Ausweis brauche.

Informationen können doch auch offen zugänglich sein, die daraus gewonnenen Erkenntnisse aber hochsensibel.

Genau. Ein klassisches Beispiel war ein Skandal um eine Lauf-App. Eine einzelne aufgezeichnete Laufstrecke ist harmlos. Wenn jedoch viele Personen regelmäßig um eine militärische Anlage herumlaufen und ihre Routen aufzeichnen, lassen sich aus der Überlagerung dieser Daten die Umrisse von Gebäuden, Zugangswegen und Strukturen rekonstruieren. Erst die Kombination der einzelnen, für sich unkritischen Informationen macht die Daten sicherheitsrelevant.

Wenn sich Informationen ständig ändern: Wie beherrschbar ist OSINT überhaupt?

Man muss akzeptieren, dass Erkenntnisse nie statisch sind. Informationen sind dynamisch. Was heute gilt, kann morgen überholt sein. OSINT ist deshalb immer ein Prozess, kein Endzustand.

INTERVIEW_ Alana Gramm

Dr. Alana Gramm ist OSINT-Spezialistin und Senior Strategy Consultant bei IBM iX. Ihre Schwerpunkte liegen im Bereich Open Source Intelligence an der Schnittstelle von Intelligence, Law Enforcement und Defence.

KEY MESSAGES

→ **OSINT ist ein laufender Prozess** aus Sammlung, Analyse und Kontextualisierung offener Quellen.

→ **Datenmenge ersetzt keine Qualität;** selektive, fachkundige Auswertung ist entscheidend.

→ **KI beschleunigt,** erhöht aber auch Manipulationsrisiken – menschliches Urteilsvermögen bleibt zentral.

→ **Wahrheit** bedeutet überprüfbare Tatsachen; ihre Leugnung schadet Opfern und Gesellschaft.

→ **Europas Stärke** liegt in gemeinsamer Methodik, Standards und Wissenstransfer – nicht im Datensammeln.

Wie wichtig ist Intuition in der OSINT-Arbeit?

Erfahrung erzeugt ein Gespür dafür, wo Informationen liegen könnten. Viele erfahrene Analysten sagen: „Ich weiß nicht genau warum, aber ich hatte das Gefühl, dass es dort relevant sein könnte.“ Dieses Bauchgefühl kommt durch jahrelange Praxis.

Aber Intuition kann auch in die Irre führen.

Absolut. Gerade bei der Bewertung muss man aufpassen, nicht voreingenommen zu sein. Confirmation Bias oder Community Bias sind reale Risiken. Deshalb braucht es systematische Verfahren, Kolleginnen und Kollegen, die widersprechen, und die Bereitschaft, ergebnisoffen zu arbeiten.

Welche Rolle spielt Künstliche Intelligenz?

KI beschleunigt OSINT massiv. Mustererkennung, Priorisierung, Analyse – all das geht heute viel schneller. Gleichzeitig steigt aber auch das Risiko von Manipulation und Desinformation. Deshalb darf OSINT nie isoliert betrachtet werden.

Was heißt das für Analysten?

Kritisches Denken wird zentral. Informationen müssen aus verschiedenen Quellen abgeglichen werden. Je mehr KI wir einsetzen, desto wichtiger wird menschliches Urteilsvermögen.

Man könnte doch eigentlich denken, man muss nur möglichst viele Daten sammeln und eine KI darüber laufen lassen, die einem dann sagt, was wirklich relevant ist,

Das Problem ist, dass Masse keine Qualität ersetzt. Wenn die Datengrundlage falsch, verzerrt oder gezielt manipuliert ist, produziert auch eine KI keine verlässlichen Ergebnisse.

Also sind „mehr Daten“ nicht automatisch besser?

Im Gegenteil. Das Internet besteht aus sehr viel Irrelevantem. Wenn ich unse-

„Wenn ich Inhalte analysiere, muss ich Sprache, Codes und Bilder verstehen. Sonst erkenne ich weder Fakes noch Bedeutungsnuancen.“

Alana Gramm

lektiv sammle, mache ich mich sogar angreifbar – etwa durch vergiftete Daten oder gezielte Täuschung. Gute OSINT-Arbeit ist selektiv. Sie braucht Fachwissen und Kontextverständnis.

Was heißt das konkret?

Wenn ich bestimmte Inhalte analysiere, muss ich Sprache, Codes, Bilder und kulturelle Bezüge verstehen. Sonst erkenne ich weder Fakes noch Bedeutungsnuancen. Diese Expertise kann keine KI ersetzen. In der Praxis wird dieser Auswertungsteil oft unterschätzt.

Ist denn schon erkennbar, dass immer mehr KI-generierte Inhalte im Umlauf sind?

Absolut. Dafür muss man keine OSINT-Recherche machen, es reicht, durch soziale Medien zu scrollen. KI-generierte Bilder, Videos und Texte nehmen stark zu. Viele Nutzer spüren intuitiv, dass etwas nicht stimmt

Was folgt daraus gesellschaftlich?

Menschen müssen lernen, Inhalte zu hinterfragen: Ist das plausibel? Passt es in den Kontext? Gerade Kinder sollten früh dafür sensibilisiert werden, dass nicht alles echt ist, was sie sehen.

Brauchen wir heute eine Art „Default-Misstrauen“ gegenüber Internet-Inhalten?

Eher eine gesunde Skepsis. Nicht alles sofort glauben, aber auch nicht alles ablehnen. Diese Balance wird immer wichtiger, für Analysten genauso wie für die Gesellschaft insgesamt.

Was bedeutet Wahrheit für Sie?

Für mich ist das eine sehr praktische Frage. Wahrheit zeigt sich dort, wo etwas tatsächlich geschehen ist. Es geht nicht um abstrakte Debatten, sondern um überprüfbare Tatsachen, die verstanden und eingeordnet werden müssen.

Es geht also darum zu erkennen, was wirklich passiert ist?

Ja. Mich interessieren Fakten, weil sie die Grundlage für Gerechtigkeit und Verantwortung sind. Ist etwas geschehen oder nicht? Wurde eine Grenze überschritten? Diese Fragen müssen beantwortet werden – für die Betroffenen, für Institutionen, für die Gesellschaft. Wenn reale Ereignisse geleugnet oder relativiert werden, entsteht zusätzlicher Schaden, weil Vertrauen und Orientierung verloren gehen.

Und wie vermeidet man Verzerrungen?

Durch Transparenz, kritisches Denken und Widerspruch. Analysten müssen ergebnisoffen arbeiten, ähnlich wie in der Wissenschaft. Sobald man nur noch bestätigt, was man ohnehin glaubt, verliert man Professionalität.

Hat OSINT auch eine demokratische Dimension?

Als Methode funktioniert OSINT grundsätzlich überall, auch in nicht-demokratischen Systemen, so wie jede andere nachrichtendienstliche Disziplin auch. Der Unterschied liegt weniger in der

Technik als im Umfeld. In autoritären Staaten sind Informationen fragmentierter, stärker kontrolliert und oft bewusst manipuliert. Das erhöht den Aufwand, das Risiko von Verzerrungen und die Unsicherheit der Ergebnisse.

Wo liegt konkret die Stärke von OSINT?

Vor allem auf der strategischen Ebene. OSINT kann langfristige Entwicklungen sichtbar machen: Diskurse, Mobilisierung, Infrastrukturveränderungen, Bewegungen, die sich über Social Media oder Satellitenbilder abzeichnen. Das sagt nicht, wann etwas passiert, aber dass sich etwas zusammenbraut.

Und operativ?

Operativ geht es um Lagebegleitung. Was passiert gerade? Wo bewegen sich Menschen? Wo entstehen Fluchtbewegungen? Je schneller Behörden diese Informationen haben, desto besser können sie reagieren. Das ist ein zentraler Bestandteil gesellschaftlicher Resilienz.

Liegt der Wert von OSINT eher in der Krisenfrüherkennung oder in der nachträglichen Aufklärung?

Aus meiner polizeilichen Erfahrung gibt es zwei zentrale Ebenen. Erstens die Gefahrenabwehr: frühzeitig zu erkennen, was passieren *könnte*, um Menschen zu schützen. Zweitens die Aufklärung: zu rekonstruieren, was *tatsächlich passiert ist*. Beides ist notwendig. Wenn Ereignisse geleugnet werden, etwa Kriegsverbrechen oder Gewaltakte, kann OSINT helfen, Fakten sichtbar zu machen. Offene Quellen ermöglichen es, Aussagen zu überprüfen und Falsches zu widerlegen.

In einem Fachartikel plädieren Sie dafür, europäische OSINT-Fähigkeiten stärker zu bündeln. Warum ist das notwendig?

Weil wir es allein nicht schaffen. In Europa arbeiten viele Akteure parallel

„Das Internet ist ein Spiegel der Gesellschaft. Wer sie verstehen will, muss diesen Spiegel lesen können.“

Alana Gramm

in ihren jeweiligen Silos. Methoden, Werkzeuge und Ausbildungsansätze werden mehrfach entwickelt, obwohl man voneinander lernen könnte. Gleichzeitig agieren unsere Gegner häufig sehr koordiniert.

Was genau meinen Sie mit Bündelung von Fähigkeiten?

Nicht das Zusammenlegen von Daten. Das wäre datenschutzrechtlich und demokratisch problematisch. Es geht um Methoden, Ausbildung, Erfahrungsaustausch. Gemeinsame Standards, gemeinsame Lernräume, gegenseitige Unterstützung. Wir erfinden zu oft dasselbe Rad neu.

Führt das zwangsläufig zu einer europäischen Nachrichtendienststruktur?

Mir geht es nicht um neue Institutionen, sondern um Wissenstransfer. Ob daraus irgendwann strukturelle Konsequenzen entstehen, ist eine politische Entscheidung.

Was treibt Sie persönlich an, sich so intensiv mit OSINT zu beschäftigen?

In Zeiten von Informationskrieg ist OSINT eine zentrale Methodologie. Es geht darum zu erkennen, was tatsächlich passiert, und wie wir uns als Gesellschaft schützen können.

Sehen Sie sich dich dabei eher als Analytikerin oder als Jägerin?

Beides. Natürlich gibt es diesen Jagdmoment – den Kick, wenn man über Umwege etwas findet. Das macht Spaß. Aber der Ernst überwiegt. Es geht um Einflussnahme, um gesellschaftliche

Prozesse. Das Internet ist ein Spiegel der Gesellschaft. Wer sie verstehen will, muss diesen Spiegel lesen können.

Würden Sie offensive Gegenmaßnahmen befürworten, etwa eigene Desinformation?

Nein. Damit verliert man Glaubwürdigkeit. Man kann nicht Wahrheit verteidigen und gleichzeitig selbst manipulieren. Wenn wir unsere Prinzipien aufgeben, verlieren wir genau das, was Demokratie ausmacht.

Was bleibt also?

Standhaftigkeit. Rechtsstaatlichkeit. Und die Fähigkeit, Dinge auszuhalten, ohne selbst autoritär zu werden. Das ist anstrengend, aber alternativlos, wenn wir unsere Gesellschaft nicht verlieren wollen.

Vielleicht stehen wir gerade am Beginn einer neuen Aufklärung in Europa, getragen von der Erfahrung, dass Demokratie, Wahrheit und Freiheit fragil sind. Das wäre eine hoffnungsvolle Perspektive.

Autoritäre Systeme folgen oft denselben Mustern: Wirklichkeit wird umgedeutet, Kritik delegitimiert, Pressefreiheit schrittweise eingeschränkt. Unabhängiger Journalismus ist dabei eines der ersten Ziele, weil er gesellschaftliche Selbstkorrektur ermöglicht. Wird er geschwächt, verliert eine Gesellschaft Orientierung und Widerstandskraft. Hoffnungsvoll wäre diese Phase, wenn daraus mehr Wachsamkeit, starke Institutionen und ein praktisches Freiheitsverständnis im politischen Alltag entstehen.

Weil es dabei um Kontrolle über Wahrnehmung geht...

Genau. Wenn Menschen nicht mehr unterscheiden können, was real ist und was nicht, braucht man sie nicht mehr zu unterdrücken. Das sage ich nicht polemisch, sondern aus persönlicher Beobachtung. Die neue Aufklärung, wenn man so will, bedeutet vor allem: Realität erkennen zu lernen.

Also weniger abstrakte Wahrheit, mehr Wirklichkeit?

Es gibt unterschiedliche Perspektiven, aber manche Dinge sind eben faktisch passiert. Und die Leugnung dieser Fakten ist Unrecht gegenüber den Opfern. Kriegsverbrechen, Gewalt, historische Verbrechen – das ist keine Meinung. Das ist geschehen.

Heißt das für Sie, OSINT ist Teil dieser Aufklärung?

Ja, wenn es verantwortungsvoll eingesetzt wird. Information ist Macht. Je persönlicher Informationen sind, desto sensibler wird dieses Wissen. Nur weil etwas öffentlich ist, heißt das nicht, dass man alles damit tun darf. Es braucht Abwägung, Rechtsstaatlichkeit und Respekt vor der Privatsphäre.

Also keine einfachen Antworten.

Nein. Demokratie ist kompliziert. Aber genau das macht sie wertvoll. Und trotz allem sehe ich Hoffnung: Ich habe sie erlebt – etwa 2022, als junge Menschen freiwillig Geflüchteten geholfen haben, stundenlang, ohne Gegenleistung. Diese Generation gibt mir Zuversicht.

Dann ist diese neue Aufklärung vielleicht weniger ein theoretisches Projekt als eine gemeinsame Praxis.

Ja. Praxis und Theorie müssen voneinander lernen. Wenn wir das tun, werden wir besser – als Gesellschaft und als Demokratie. ■

„Wenn Menschen nicht mehr unterscheiden können, was real ist und was nicht, braucht man sie nicht mehr zu unterdrücken.“

Alana Gramm

Intelligence stärkt Lieferketten

Globale Lieferketten stehen zunehmend unter geopolitischem Druck. Geopolitical Risk Intelligence hilft Unternehmen, Supply-Chain-Risiken zu verstehen und zu bewältigen.

GEOPOLITISCHE RISIKEN ALS HERAUSFORDERUNG FÜR GLOBALE LIEFERKETTEN

Geopolitische Risiken sind die Unsicherheiten in den Entscheidungsprozessen von Unternehmen, die durch den Wettbewerb von Staaten um Macht im internationalen Raum sowie durch globale Machtverschiebungen entstehen.

Die Lieferketten der deutschen Wirtschaft sind in hohem Maße verwundbar für diese Risiken. Der wichtigste Grund dafür ist, dass Staaten die in den Jahrzehnten der Globalisierung gewachsenen wirtschaftlichen Verflechtungen und Abhängigkeiten zunehmend als politisches Druckmittel nutzen. Die Lieferketten deutscher Unternehmen wurden zuletzt etwa durch geopolitisch motivierte Exportkontrollen für Seltene Erden und Halbleiter sowie durch Zölle deutlich beeinträchtigt. Außerdem können Lieferketten durch bewaffnete Konflikte unterbrochen werden, wie es in den vergangenen Jahren etwa in der Ukraine oder entlang des für die Weltwirtschaft wichtigen Seewegs durch das Rote Meer der Fall war.

Dies kann zu steigenden Kosten sowie zu Versorgungsunterbrechungen und Produktionsausfällen führen, welche im äußersten Fall strategische Auswirkungen auf Unternehmen mit sich bringen. Zu

den potenziellen gesellschaftlichen Folgen dieser Risiken gehören steigende Inflation, steigende Arbeitslosigkeit und sinkende volkswirtschaftliche Wettbewerbsfähigkeit, aber auch Herausforderungen für die Verwirklichung politischer Ziele wie der Energiewende, der digitalen Transformation oder der sicherheitspolitischen Zeitenwende. Diese Ziele können nur dann erreicht werden, wenn die dafür erforderlichen Teile und Rohstoffe im Rahmen funktionierender Lieferketten zuverlässig durch Unternehmen bezogen werden können.

RESILIENTE LIEFERKETTEN ERFORDERN GEOPOLITICAL RISK INTELLIGENCE

Wo geopolitische Risiken bekannt sind und in Entscheidungsprozessen berücksichtigt werden, können Lieferketten so gestaltet werden, dass sie gegenüber diesen Risiken resilient sind. Die Ereignisse der vergangenen Jahre haben jedoch gezeigt, dass Unternehmen diesbezüglich vielfach Defizite aufweisen. Vor allem größere Unternehmen haben daher Intelligence-Funktionen aufgebaut, um diese zu beheben.

Mit dem Begriff „Geopolitical Risk Intelligence“ werden die Organisationseinheiten, die Prozesse und die Produkte >

TEXT_ Simon Wunder

Simon Wunder ist in der Volkswagen AG für die Analyse geopolitischer Risiken für Lieferketten verantwortlich. Außerdem ist der Politikwissenschaftler Research Fellow am Center for Advanced Security, Strategic and Integration Studies (CASSIS) der Universität Bonn. Dieser Beitrag gibt seine persönlichen Ansichten wieder.

KEY MESSAGES

- **Geopolitische Machtverschiebungen** und staatliche Eingriffe erhöhen die Verwundbarkeit globaler Lieferketten.
- **Wirtschaftliche Abhängigkeiten** werden zunehmend als politisches Druckmittel eingesetzt.
- **Geopolitical Risk Intelligence** macht Risiken sichtbar, bewertbar und entscheidungsrelevant.
- **Resiliente Lieferketten** entstehen durch Szenarien, Monitoring und datenbasierte Frühwarnung.
- **Unternehmen mit integrierter Intelligence-Funktion** reagieren schneller, vermeiden Schäden und sichern ihre Handlungs- und Wettbewerbsfähigkeit.

bezeichnet, die diese Aufgabe leisten. Mit anderen Intelligence-Funktionen haben diese gemeinsam, dass sie entscheidungs- und handlungsorientiertes Wissen gewinnen, um auf dessen Grundlage zeitgerecht vorgelegte, nutzergerecht aufbereitete, relevante und zuverlässige Informationsprodukte bereitzustellen. Dadurch sollen Unsicherheiten in Entscheidungsprozessen auf eine Weise reduziert werden, die es Unternehmen ermöglicht, bessere Entscheidungen zu treffen.

Wo diese Aufgabe erfolgreich geleistet wird, werden Risiken für Lieferketten transparent, so dass sie durch gezielte Maßnahmen gesteuert werden und Schäden abgewendet sowie Chancen ergriffen werden können. Lieferketten können dann so gestaltet werden, dass sie gegenüber geopolitischen Risiken weniger exponiert sind.

Auf den Eintritt von Risiken sind Beschaffungsorganisationen mit solchen Funktionen besser vorbereitet, so dass Krisen für sie beherrschbarer werden und Versorgungsunterbrechungen entweder ganz vermieden oder deren Dauer zumindest verkürzt werden kann. Auch sind Unternehmen mit einer leistungsfähigen Intelligence-Funktion lernfähiger, was sie dazu befähigt, sich an Änderungen des geopolitischen Umfelds früher und besser anzupassen und aus Ereignissen und Vorfällen relevante Folgerungen zu ziehen.

In einem aufgrund von raschem technologischem Wandel, wachsender globaler Vernetzung und geopolitischer Dynamik zunehmend von Volatilität, Unsicherheit und Komplexität geprägten globalen Umfeld hat die Bedeutung solcher Funktionen daher zuletzt deutlich zugenommen.

Besondere Herausforderungen bei Intelligence-Aufgaben im Bereich Lieferkette

Intelligence-Funktionen wurden in Unternehmen ursprünglich meist im Bereich Konzernsicherheit aufgebaut. In Beschaffungsorganisationen stehen diese vor spezifischen Herausforderungen, die eine Anpassung gängiger Ansätze an diesen Aufgabenbereich erfordern.

■ **Geopolitische Risiken für Lieferketten wurden in der Vergangenheit durch Unternehmen in einigen Fällen zwar zutreffend identifiziert, aber in Entscheidungen nicht angemessen berücksichtigt.** Ein Grund dafür ist, dass Maßnahmen zur Stärkung der Resilienz von Lieferketten meist mit höheren Kosten und sonstigem Aufwand verbunden sind als beispielsweise Sicherheitsmaßnahmen für Standorte und Mitarbeitende. An Intelligence-Produkte besteht dabei die Anforderung, Aussagen zu Eintrittswahrscheinlichkeiten und Auswirkungen von Risiken so zu quantifizieren, dass sie in Entscheidungsprozessen verarbeitet werden können. Diese Quantifizierung wurde von den zuständigen Intelligence-Funktionen in der Vergangenheit jedoch nicht immer durchgeführt, auch weil sie in den gängigen Intelligence-Methoden nicht immer vorgesehen ist.

■ **Die Bewertung der Auswirkungen von Risiken erfordert zudem einen hinreichenden Grad an Transparenz der eigenen Lieferkette sowie die automatisierte Verarbeitung der entsprechenden Daten.** Die technischen und organisatorischen Voraussetzungen dafür sind jedoch noch nicht in allen größeren Unternehmen vorhanden.

■ **Eine weitere Herausforderung besteht darin, dass Intelligence-Prozesse Aussagen über Eintrittswahrscheinlichkeiten von Risiken umso zuverlässiger treffen können, je kürzer der betrachtete Zeithorizont ist.** Lieferketten in der Industrie sind jedoch oft wenig elastisch, so dass die Forderung nach langfristigen Prognosen zu Eintrittswahrscheinlichkeiten erhoben wird, die mit gängigen Methoden jedoch kaum zu leisten sind.

■ **Geopolitische Risiken für Lieferketten sind im Vergleich zu anderen von Intelligence-Funktionen behandelten Risiken sehr komplex.** Ihre Bewertung erfordert eine tiefe Expertise, die Intelligence-Teams nicht zu allen relevanten Risiken vorhalten können, die aber in größeren Unternehmen meist an anderen Stellen vorhanden ist und erschlossen werden muss.

Eine allgemein verbreitete, mit hinreichendem Reifegrad entwickelte Intelligence-Methodik für die Analyse geopolitischer Risiken für Lieferketten existiert bislang nicht, so dass Unternehmen diese überwiegend auf Grundlage von Best-Practice-Beispielen und eigenen Erfahrungen selbst entwickeln müssen. Die unten beschriebenen organisatorischen und methodischen Ansätze sind Beispiele für solche Entwicklungen.

DIE ORGANISATION DER INTELLIGENCE-FUNKTION

In Beschaffungsorganisationen werden Intelligence-Aufgaben zum Teil von kleinen Teams geleistet. Um erfolgreich zu sein, benötigen diese sowohl Expertise im Bereich Beschaffung und Kenntnis der Strukturen und Prozesse des Unternehmens, aber auch eine möglichst breite geopolitische Expertise und Netzwerke außerhalb des Unternehmens, etwa in Verbänden und Think Tanks. Da sich die Analyse geopolitischer Risiken für Lieferketten vor allem auf Daten stützt, ist zudem Expertise im Bereich Data Science erforderlich. Solche Teams nutzen darüber hinaus in der Regel die Unterstützung spezialisierter Dienstleister, um geopolitische Risiken zu identifizieren und zu analysieren.

Die Einführung einer zentralen Funktion, die geopolitische Risiken für alle Bereiche eines Unternehmens analysiert und steuert, hat sich oft nicht als zielführend erwiesen. Ein Grund dafür ist, dass die Auswirkungen dieser Risiken auf die einzelnen Unternehmensbereiche jeweils sehr unterschiedlich sind und deren Identifizierung, Analyse und Bewertung jeweils spezifische Expertise erfordert, die eine zentrale Funktion kaum umfassend abbilden kann. Bewährt hat sich hingegen eine enge Abstimmung zwischen den In-

telligence-Funktionen verschiedener Bereiche, neben der Beschaffung etwa Strategie-, Risiko-, Sicherheits- und Politikabteilungen, und die koordinierte Erstellung strategischer Szenarien und Lagebilder.

METHODEN UND PRODUKTE DER INTELLIGENCE-ANALYSE

Die für die Analyse geopolitischer Risiken für Lieferketten entwickelten Intelligence-Methoden verbinden meist quantitative Ansätze aus dem Risikomanagement mit Strukturierten Analysetechniken und anderen wissenschaftlich fundierten, methodisch transparenten und prozessartig darstellbaren qualitativen Analysemethoden, die ursprünglich von Sicherheitsbehörden entwickelt wurden, um die Qualität der nachrichtendienstlichen Auswertung zu erhöhen.

Die mit ihnen erstellten Produkte umfassen das gesamte analytische Spektrum. Sie beschreiben relevante Ereignisse, bewerten ihre unmittelbaren Auswirkungen auf Lieferketten, und geben einen vorausschauenden Ausblick auf die mögliche künftige Entwicklung von Risiken. Im Vordergrund steht dabei immer die Beantwortung der Frage nach dem „so what“, also nach den Implikationen für die eigenen Lieferketten.

Ein übergeordnetes Analyseprodukt stellt ein strategisches Lagebild dar, das die wichtigsten lieferkettenrelevanten geopolitischen Trends und ihre möglichen Auswirkungen sowie deren mögliche weitere Entwicklung vorausschauend analysiert. Solche Lagebilder unterstützen in der Regel strategische Entscheidungsprozesse und werden mit anderen Stabsfunktionen in Unternehmen abgestimmt.

Ein weiteres vorausschauendes Produkt stellen Szenarioanalysen dar, die einzelne geopolitische Entwicklungen unter-

suchen. Sie können dazu genutzt werden, um Risiken für Lieferketten zu identifizieren, die in ein Risikoregister aufgenommen und weiter beobachtet werden. Auf dieser Grundlage können zudem Risikoanalysen für einzelne Beschaffungsvorhaben erstellt werden. Zu diesem Zweck kommen auch Risiko-Ratings zum Einsatz, größtenteils automatisiert und datengestützt erstellt werden und eine Vielzahl von Risikofaktoren berücksichtigen.

Das gegenwärtige Geschehen wird durch Monitoring- und Forecasting-Prozesse erfasst. Diese beobachten die zuvor identifizierten Risiken, suchen nach Signalen für eventuell neu aufkommende Risiken, bewerten die unmittelbaren Auswirkungen von Ereignissen auf Lieferketten und geben Prognosen darüber ab, mit welcher Eintrittswahrscheinlichkeit bestimmte Risiken kurz- bis mittelfristig eintreten können.

WEITERENTWICKLUNG VON GEOPOLITICAL RISK INTELLIGENCE

Zunehmende Risiken für Lieferketten erzeugen wachsenden Druck auf die Privatwirtschaft, die oben beschriebenen Ansätze und Methoden weiterzuentwickeln. Die anhaltend hohe Frequenz von geopolitisch verursachten Versorgungskrisen, aber auch die zunehmende Lernfähigkeit von Organisationen und Fortschritte im KI-Bereich werden wahrscheinlich dazu führen, dass sich das Feld Geopolitical Risk Intelligence im Lieferkettenkontext in den kommenden Jahren stark verändern wird. Zur Stärkung der gesellschaftlichen Resilienz wäre es daher wünschenswert, wenn dieses Feld über größere Unternehmen hinaus stärkere Beachtung fände – etwa in Form einer gemeinsamen Weiterentwicklung von Methoden und Prozessen durch Staat, Wissenschaft, Thinktanks und Wirtschaft. ■

Chaos als Waffe

Sabotage ist ein zentrales Instrument hybrider Kriegsführung. Expertin Daniela Richterova erklärt, warum Ausmaß, Methoden und psychologische Wirkung der aktuellen Sabotagewelle Europa strategisch herausfordern.

Daniela Richterova, wie definieren Sie Sabotage?

Daniela Richterova: In der Wissenschaft wird über die Definition noch immer gestritten – und das wird sich vermutlich auch nie ganz ändern. Vereinfacht gesagt ist Sabotage eine vorsätzliche Handlung, die darauf abzielt, Systeme, Organisationen oder Prozesse aus politischen, strategischen oder ideologischen Gründen zu beschädigen oder zu stören. Sie wird in der Regel verdeckt durchgeführt.

Welche Formen kann Sabotage annehmen?

Dazu zählen Brandstiftung, Explosionen, die Verunreinigung von Wasser- oder Energieversorgung sowie sogar Attentate, sofern sie darauf abzielen, Schlüsselindustrien oder Kriegsanstrengungen zu beeinträchtigen. Sabotage existiert auch im Cyberraum, insbesondere dann, wenn Cyberoperationen physische Folgen haben.

Es scheint, als könne das Ziel von Sabotage prinzipiell fast alles sein ...

Es kann vieles sein, aber ich wäre vorsichtig, den Begriff zu weit zu fassen. Nicht jede feindselige oder gewalttätige Handlung ist Sabotage. Für mich ist entscheidend, ob das Ziel einen strategischen Zweck oder eine strategische Bedeutung hat.

Was meinen Sie in diesem Zusammenhang mit strategischem Zweck?

Die Handlung muss mit einem übergeordneten politischen oder militärischen Ziel verknüpft sein. Russland hat beispielsweise im Ausland Attentate und Vergiftungen von Gegnern verübt. Das sind schwere Taten, aber nicht zwangsläufig Sabotage. Sie dienen dem Umgang mit Gegnern, nicht immer der Störung eines strategischen Systems.

Das Motiv allein reicht also nicht aus?

Genau. Rache oder Bestrafung genügt

nicht. Sabotage muss sich gegen etwas richten, das strategisch relevant ist, also mit einem größeren Ziel verbunden sein.

Würde die bloße Zerstörung von Eigentum als Sabotage gelten?

Das hängt vom Kontext ab. Wird ein beliebiges Auto zerstört, ist das schlicht eine kriminelle Handlung. Wird jedoch das Auto einer hochrangigen politischen Persönlichkeit zerstört, man wird dafür von einem ausländischen Staat bezahlt und die Ziele sind politischer, militärischer oder nachrichtendienstlicher Natur, dann kann dies als Sabotage gelten. Absicht und Ziel sind entscheidend. Ob eine Handlung tatsächlich als Sabotage eingestuft wird, hängt jedoch auch von rechtlichen Definitionen ab, da nicht alle Staaten diese Art von Handlungen gleich klassifizieren.

Weiten wir den Blick auf das größere Bild: Wie würden Sie die Sabotagewelle seit Beginn des Krieges gegen die Ukraine charakterisieren?

Ich würde argumentieren, dass dies die intensivste Sabotagewelle ist, die wir seit dem Zweiten Weltkrieg erlebt haben. Während des Kalten Krieges gab es umfangreiche Planungen durch die Sowjets, die Stasi und andere Akteure, doch nur sehr wenige dieser Pläne wurden tatsächlich umgesetzt. Was wir heute sehen, unterscheidet sich deutlich in Ausmaß und Frequenz. Die Jahre 2023 bis 2024 waren besonders intensiv, es gab Dutzende von Fällen – von feindlicher Ausspähung bis hin zu tatsächlicher Sabotage auf NATO-Gebiet. 2025 war die Lage ruhiger, aber es kam weiterhin zu ernsthaften Vorfällen.

Was erklärt dieses Ausmaß?

Ein wesentlicher Faktor ist der Einsatz von Akteuren auf niedrigem Niveau. Die meisten Angriffe werden nicht von Profis durchgeführt, was mehr Opera-

INTERVIEW_ Daniela Richterova

Dr. Daniela Richterova ist Associate Professor für Intelligence Studies am Department of War Studies des King's College London. Ihre Forschung zu Geheimdiensten im Kalten Krieg sowie zu staatlichen Bedrohungen und Terrorismus erscheint u. a. in *International Affairs and Foreign Policy*. 2025 veröffentlichte sie *Watching the Jackals* (Georgetown University Press).

KEY MESSAGES

- **Sabotage** ist eine vorsätzliche, meist verdeckte Handlung mit strategischem Zweck
- **Seit 2022** erlebt Europa die intensivste Sabotagewelle seit dem Zweiten Weltkrieg
- Ein „**Gig-Economy-Modell**“ mit niedrigschwelligen Akteuren ersetzt klassische Geheimdienstoperationen.
- **Ziel ist nicht nur physischer Schaden**, sondern vor allem psychologische Wirkung
- **Kritische Infrastruktur** liegt zunehmend in privater Hand.

„Die Methoden haben sich angepasst, aber die zugrundeliegende Logik ist bemerkenswert vertraut.“

Daniela Richterova

tionen in mehr Ländern ermöglicht. Viele Akteure werden online für mehrere Aufgaben rekrutiert. In manchen Fällen zieht eine angeworbene Person Freunde oder Bekannte hinzu. Es ist eine Form des Outsourcings: Man definiert die Aufgabe, und jemand anderes stellt ein Team zusammen.

Warum ist dieses „Gig-Economy-Modell“ der Sabotage so prägend geworden?

Dafür gibt es drei Gründe. Erstens haben wir seit 2014 und insbesondere seit 2022 eine Erosion von Normen und eine Verschiebung der strategischen Landschaft erlebt. Zweitens wurden operativ viele professionelle Geheimdienstoffiziere aus Europa ausgewiesen. Und drittens erschwert moderne Überwachungstechnologie klassische Tarnidentitäten, während Online-Rekrutierung und -Bezahlung einfacher geworden sind.

Was sagt das über das Wesen von Sabotage aus?

Sabotage existiert nicht isoliert. Sie ist ein Instrument, das Staaten als Reaktion auf politische Entwicklungen einsetzen. Phasen der Eskalation – etwa eine verstärkte militärische Unterstützung für die Ukraine – werden häufig von Spitzen in der Sabotageaktivität begleitet.

Sehen Sie Kontinuitäten zur Sabotagedoktrin der Sowjetzeit?

Ja, ganz eindeutig. Viele der strategischen Ziele, die in sowjetischen und osteuropäischen Dokumenten aus der

Zeit des Kalten Krieges diskutiert wurden, gelten bis heute. Die Unterminierung der politischen Einheit des Westens und das Auferlegen wirtschaftlicher Kosten bleiben zentrale Ziele. Heute scheint es manchmal wichtiger zu sein, Chaos und Paranoia zu erzeugen, als große militärische Ziele zu treffen. Die Methoden haben sich angepasst, aber die zugrunde liegende Logik ist bemerkenswert vertraut.

Wie beurteilen Sie den Grad der heutigen Raffinesse von Sabotage?

Das hängt davon ab, wie wir Raffinesse definieren. Wir sehen bereits Formen von Sabotage, die über physische Angriffe hinausgehen. Einige meiner Kolleginnen und Kollegen haben darüber geschrieben, wie KI-Sprachmodelle gezielt mit Desinformation „vergiftet“ werden, was beeinflusst, wie Gesellschaften informiert werden. Auch das lässt sich als Sabotage verstehen, selbst wenn es ganz anders aussieht.

Gibt es eindeutige Beispiele für Cyber-Sabotage mit physischen Folgen?

Ja. Der jüngste Fall ereignete sich in Norwegen, wo prorussische Cyberakteure einen Staudamm angriffen, indem sie die Schleusen öffneten. Große Wassermengen wurden über Stunden freigesetzt, bevor der Vorfall bemerkt wurde. Das war eine Cyberoperation mit realen physischen Auswirkungen.

Könnte Künstliche Intelligenz die Wirksamkeit von Sabotage erhöhen?

Potentiell ja. KI könnte dabei helfen,

besonders verwundbare Ziele zu identifizieren, etwa kritische Eisenbahnknotenpunkte oder Kommunikationsinfrastruktur, bei denen eine kleine Störung große Effekte hat. Sie könnte auch bei der Analyse der Architektur von Unterseekabeln oder anderer Schwachstellen unterstützen. Ich möchte hier allerdings nicht zu sehr spekulieren, und ich will auch keinen Handlungsleitfaden liefern.

Wie können Analysten Sabotage von gewöhnlicher Kriminalität unterscheiden?

Mehrdeutigkeit ist ein Kernelement hybrider Kriegsführung. Außerhalb eines formellen Kriegs sollen solche Handlungen wie Unfälle aussehen. Es gibt jedoch Indikatoren, die man prüfen kann, insbesondere Ziel und Zeitpunkt. Wenn ein Lagerhaus abbrennt, mag das zunächst banal wirken. Wenn es jedoch von einem ukrainischen Logistikunternehmen genutzt wird und Ausrüstung enthält, die für die Ukraine bestimmt ist, verändert das die Lage. Auch der Zeitpunkt ist entscheidend: Gesah es nach einer politischen Eskalation oder nach einer Entscheidung, die vom Gegner möglicherweise als feindselig wahrgenommen wurde?

Wie wichtig ist aus russischer Sicht die psychologische Wirkung von Sabotageoperationen?

Sie ist absolut zentral. Eines der Hauptziele ist es, Reichweite zu demonstrieren. Wenn Vorfälle in mehreren Ländern vermutet werden, entsteht der Eindruck von Handlungsfähigkeit und

„Kommunikations- und Verkehrsnetze sind besonders verwundbar. Man kann nicht jede Bahnstrecke oder jedes Kabel quer durch Europa bewachen.“

Daniela Richterova

Macht. Gleichzeitig untergräbt dies das Vertrauen in die Fähigkeit von Regierungen, ihre Gesellschaften zu schützen.

Das klingt ähnlich wie klassische terroristische Strategien. Ist dieser Vergleich gerechtfertigt?

Es gibt klare Parallelen. Ziel ist nicht nur physischer Schaden, sondern auch die Verbreitung von Angst, Unsicherheit und Vertrauensverlust. In diesem Sinne überschneiden sich Sabotage und Terrorismus in ihrer Wirkung auf Gesellschaften.

Sind Sie damit einverstanden, Sabotage als eine Form von Krieg zu bezeichnen?

Mit dieser Einordnung wäre ich vorsichtig. Man könnte von einem Teil eines verdeckten Krieges sprechen, doch rechtlich und politisch ist es kein Krieg im traditionellen Sinne. Krieg setzt bewaffnete Feindseligkeiten zwischen Staaten voraus und muss bestimmte rechtliche Bedingungen erfüllen. Was wir beobachten, lässt sich treffender als hybrider Konflikt beschreiben.

Wie fügt sich Sabotage in hybride Operationen ein?

Sabotage ist ein Instrument, das zur Kriegsvorbereitung oder zur Beschleunigung von Eskalation eingesetzt werden kann. Vor zehn Jahren bestand hybride Kriegsführung vor allem aus Desinformation und Wahlbeeinflussung. Heute spielen kinetische Operationen eine deutlich größere Rolle.

Im Hinblick auf Vorsorge: Welche Sektoren sind potenzielle Ziele?

Es gibt eine lange Liste von Zielen, die bereits während des Kalten Krieges existierte. Sowjetische Planer unterschieden Kategorien von weichen Zielen über schwer zu schützende Infrastruktur bis hin zu harten Zielen im engeren Sinne. Kommunikations- und Verkehrsnetze sind besonders verwundbar, weil sie nicht vollständig geschützt werden können. Man kann nicht jede Bahnstrecke oder jedes Kabel quer durch Europa bewachen. Militärische oder waffenbezogene Einrichtungen stehen ebenfalls auf dieser Liste.

Sind diese Annahmen aus dem Kalten Krieg heute noch relevant?

Sehr sogar. Wenn man diese historischen Ziellisten mit den jüngsten Angriffen vergleicht, wurde mindestens die Hälfte davon bereits getroffen. Die Technologie hat sich verändert – etwa von Telefonleitungen hin zu Glasfaser- und Unterseekabeln –, doch die strategische Logik ist dieselbe geblieben.

Gibt es bislang auffällige Lücken bei der Zielwahl?

Ja. Wir haben vergleichsweise wenige Angriffe auf politische Parteien oder politische Führungspersonen gesehen. Nach der Logik des Kalten Krieges hätte man davon mehr erwarten können, doch bislang spielen sie keine zentrale Rolle. Auffälliger ist die Verschiebung hin zu anderen Zieltypen. Durch jahrzehntelange Privatisierung befinden sich viele Elemente kritischer Infrastruktur heute in privater Hand. Eisen-

bahnen, Logistikzentren, Einzelhandel und Energie sind keine rein staatlichen Güter mehr. Private Unternehmen stehen inzwischen ganz oben auf der Zielliste.

Warum ist das bedeutsam?

Weil es die Sicherheitslage grundlegend verändert. Angriffe auf private Unternehmen können nationale Auswirkungen haben. Wir haben Brandanschläge auf große kommerzielle Einrichtungen gesehen, etwa auf ein IKEA-Einrichtungshaus in Litauen und ein Einkaufszentrum in Warschau, wodurch Tausende von Unternehmen betroffen waren. Regierungen müssen viel enger mit dem privaten Sektor zusammenarbeiten, um solche Angriffe zu verhindern oder einzudämmen. Nationale Sicherheit kann nicht mehr allein vom Staat gewährleistet werden. Unternehmen sind Teil der Frontlinie.

Was wird neben Bewusstseinsbildung benötigt, um Resilienz aufzubauen?

Eine deutlich stärkere Zusammenarbeit innerhalb der Sicherheitsgemeinschaft bei dieser konkreten Bedrohung. Nachrichtendienste, Strafverfolgungsbehörden und Sicherheitsorgane müssen so eng kooperieren wie im Bereich der Terrorismusbekämpfung. Dafür braucht es Ressourcen, politischen Fokus und den Abbau institutioneller Silos.

Ist die Abwehr von Sabotage auch eine Frage besserer Kommunikation?

Ja, ganz eindeutig. Was wir üblicherweise als innerstaatliche Koordina-

>

„Wenn ein Angriff als wahllos wahrgenommen wird, verbreitet er Angst, Paranoia und Chaos weit über das eigentliche Ereignis hinaus.“

Daniela Richterova

tion bezeichnen, ist hier entscheidend. Das bedeutet, dass verschiedene Akteure gemeinsam an einem Tisch sitzen und offen teilen, was sie wissen: Wer hat was beobachtet, wie hängen diese Informationen zusammen und wie lassen sie sich gemeinsam nutzen? Diese Art von Kommunikation macht einen echten Unterschied.

Welche Rolle spielt Gesetzgebung in diesem Prozess?

Eine sehr wichtige. Viele Staaten passen derzeit ihre Gesetze an, um staatlich gesteuerten Bedrohungen expliziter zu begegnen. Frankreich hat dies kürzlich getan, das Vereinigte Königreich hat seine Gesetzgebung vor zwei Jahren aktualisiert, und andere Länder folgen. Eine vergleichbare Welle rechtlicher Anpassungen gab es zuletzt nach dem 11. September, als neue terrorismusbezogene Bestimmungen ins Strafrecht aufgenommen wurden.

Welche Form von Sabotage bereitet Ihnen persönlich die größten Sorgen?

Am meisten beunruhigt mich ein Szenario mit vielen Opfern an mehreren Zielen gleichzeitig. Es gab einen Plot, der glücklicherweise scheiterte, bei dem Brandsätze auf Frachtflügen nach Deutschland, Großbritannien und Polen verschickt wurden. Wären diese Geräte während des Fluges explodiert, wäre das ein Albtraumszenario gewesen.

Warum genau sticht dieser Fall hervor?

Weil er mehrere Worst-Case-Elemente vereinte. Er war länderübergreifend

koordiniert, hoch sichtbar und hätte viele Todesopfer fordern können. Für Menschen, die in der Terrorismusbekämpfung arbeiten, ist ein solches Szenario immer die größte Befürchtung gewesen.

Wie unterscheidet sich das von gezielten Operationen?

Gezielte Angriffe wirken auf die meisten Menschen weit entfernt. Eine Explosion eines Frachtflugzeugs oder ein vergleichbarer öffentlicher Vorfall ist etwas anderes. Jeder hätte betroffen sein können, ohne irgendeinen Bezug zum Konflikt zu haben.

Es geht bei der Sorge also nicht nur um Opferzahlen.

Genau. Der unmittelbare Schaden wäre schrecklich, doch die weitergehenden Auswirkungen wären noch gravierender. Wenn ein Angriff als wahllos wahrgenommen wird, verbreitet er Angst, Paranoia und Chaos weit über das eigentliche Ereignis hinaus.

Mit anderen Worten: Jeder hat das Gefühl, es hätte ihn selbst treffen können.

Ja. Diese Wahrnehmung ist es, die solche Taten so wirkungsvoll und so gefährlich für Gesellschaften macht. ■

„Intelligence ist eine Führungsaufgabe“

Von Afghanistan zum Konzernkrisenstab: Corporate-Intelligence-Experte Christopher Radler-Morić erklärt, wie Unternehmen Risiken früh erkennen, handlungsfähig bleiben – und warum gute Intelligence oft gerade am besten funktioniert, wenn sie unsichtbar bleibt.



Christopher Radler-Morić, Wie würden Sie Außenstehenden erklären, was Sie beruflich machen?

Christopher Radler-Morić: Meinen Berufseinstieg hatte ich als nachrichtendienstlicher Analyst bei einer Sicherheitsbehörde, von wo aus ich als Risikomanager für die damalige Gesellschaft für technische Zusammenarbeit (GTZ) nach Afghanistan gegangen bin. Dabei bin ich mit allen klassischen Feldern der Unternehmenssicherheit in Berührung gekommen: Lageanalyse, Standortsicherheit, Evakuierungs- und Notfallpläne, Reisesicherheit – das volle Programm.

Und daraus hat sich Ihr heutiger Schwerpunkt entwickelt?

Genau. Ich habe mich Schritt für Schritt in Richtung Notfall- und Krisenmanagement weiterentwickelt, insbesondere während meiner Zeit bei Daimler. Dort habe ich das weltweite Krisenmanage-

mentsystem aufgebaut: den Konzernkrisenstab, das Krisenlagezentrum, Governance-Strukturen. Operativ ging es um Naturkatastrophen, Bürgerkriege, Entführungen, Erpressungen – alles, was man sich vorstellen kann.

Heute arbeiten Sie stark im Bereich Business Continuity Management. Worum geht es dabei?

Notfall- und Krisenplanung eines Unternehmens. Das reicht von Szenarien wie einem Amoklauf oder dem Suizid eines Mitarbeiters bis hin zu großen geopolitischen Krisen. Ein zentraler Teil ist, Krisenstäbe aufzubauen, zu schulen und handlungsfähig zu halten – inklusive fiktiver Übungen und der Moderation eines Stabs im Ernstfall.

Wie unterscheidet sich das vom klassischen Risikomanagement?

Risikomanagement versucht, die Eintrittswahrscheinlichkeit von Schadensereignissen zu minimieren, also

INTERVIEW_ **Christopher Radler-Morić**

Christopher Radler-Morić ist Experte für Corporate Security mit den Schwerpunkten Business Continuity Management, Notfall- und Krisenmanagement, Reisesicherheit sowie Intelligence. Mit nachrichtendienstlichem Hintergrund und einem Masterstudium in Arabistik, Ethnologie sowie Risiko- und Krisenmanagement verbindet er strategische Sicherheitsanalyse mit tiefem kulturellem und geopolitischem Verständnis komplexer Risikolagen.

KEY MESSAGES

→ **Corporate Intelligence** ist keine Zukunftsdeutung, sondern strukturierte Analyse zur Vorbereitung von Entscheidungen unter Unsicherheit.

→ **Business Continuity Management** zielt im Fall von Krisen auf die Wiederherstellung kritischer Prozesse.

→ **Frühzeitige Szenarioanalyse** und klar definierte Kipppunkte schaffen reale Handlungsfähigkeit, bevor Krisen öffentlich sichtbar werden.

→ **Fehlendes Methodenverständnis**, kognitive Verzerrungen und das Präventionsparadox führen dazu, dass erfolgreiche Analyse oft unsichtbar bleibt.

→ **Intelligence** entfaltet ihren Nutzen nur, wenn sie ans Top-Management angebunden ist und in strategische Entscheidungen einfließt.

präventiv zu wirken. Business Continuity Management setzt auf der Schadensausmaß-Seite an, also reaktiv. Es geht davon aus, dass trotz aller Prävention ein Restrisiko besteht, das sich als Schadensereignis materialisieren kann – und fragt: Wie bekomme ich kritische Geschäftsprozesse bei einem Ausfall schnell wieder zum Laufen? Wie stelle ich einen Notbetrieb sicher?

Heißt das, es geht um eine ganzheitliche Krisenvorsorge?

Genau. Der Prozess beginnt bei der Krisenfrüherkennung, also bei der Beobachtung und Analyse von Entwicklungen. Stichworte sind Intelligence, Foresight und Forecasting: Wird etwas passieren? Wie wahrscheinlich ist das? Und welchen Impact hätte es auf das

„Der Prozess beginnt bei der Krisenfrüherkennung, also bei der Beobachtung und Analyse von Entwicklungen.“

Christopher Radler-Morić

Unternehmen? Wenn die Wahrscheinlichkeit hoch genug ist, muss man sich frühzeitig vorbereiten – organisatorisch, operativ und strategisch.

Wie haben Sie etwa den russischen Überfall auf die Ukraine erlebt?

Ein Kollege und ich haben die Lage damals intensiv analysiert und kamen

zu dem Schluss, dass es sich sehr wahrscheinlich nicht um eine Übung, sondern um die Vorbereitung einer Invasion handelte. Wir haben das Management frühzeitig informiert. Das war nicht bequem, weil es sofort Handlungsdruck erzeugt. Aber als der Angriff tatsächlich begann, war das Unternehmen vorbereitet: Ein spezifischer Krisenstab war definiert, Lieferketten und Personalfragen waren geklärt. Diese frühe Analyse hat echte Handlungsfähigkeit ermöglicht.

Wie geht es weiter?

Es folgt die bewertende Analyse: Was bedeuten Entwicklungen konkret für Unternehmen, Prozesse und Risiken? Erst hier geht es über Beschreibung hinaus zur vorausschauenden Analyse, die ableitet, was wahrscheinlich als Nächstes passiert. Wir haben mit Szenariotechnik gearbeitet. Das bedeutet, man entwirft mehrere plausible Zukunftsbilder und fragt sich: Was könnte passieren? Welche Szenarien sind relevant? Und welchen Impact hätten sie jeweils?

Wie bewertet man solche Szenarien?

Wir haben spieltheoretische Prinzipien genutzt. Also die Annahme rational handelnder Akteure. Man schaut sich Gewinn und Verlust an und versucht, sich in das Gegenüber hineinzusetzen. Das ist wichtig, weil wir in Deutschland sehr stark durch unsere eigene ideologische Brille schauen.

Was heißt das konkret?

In der breiten Öffentlichkeit ist das Verständnis für interessengetriebene Außenpolitik weitgehend verschwunden. Viele können sich nicht vorstellen, dass ein Staat interveniert, weil es ihm nützt und weil er es kann. Völkerrecht ist ein wichtiges moralisches Ziel, aber so funktioniert die Welt nicht immer.

Wenn ich ernsthaft Vorhersagen treffen will, muss ich mich von solchen Denkblockaden lösen.

Zum Beispiel im Blick auf Russland?

Genau. Man muss sich fragen, welchen Nutzen Putin aus einem Überfall ziehen könnte. Dann betrachtet man das global und holistisch. Wir haben drei Szenarien entwickelt und für jedes sogenannte Kippunkte definiert. Also Indikatoren, die anzeigen, dass ein Szenario wahrscheinlicher wird.

Haben Sie dafür ein Beispiel?

Ein sehr bekannter Kippunkt war die Verlegung von Blutkonserven in Feldlazarette nahe der Grenze zur Ukraine. Das macht man bei Militärübungen nicht, weil Blutkonserven schnell verderben und extrem knapp sind. Als das geschah, war für uns klar: Die Skala steht auf dunkelrot. Eine Invasion wird sehr wahrscheinlich.

Wie kommen Sie an die Informationen für solche Analysen?

Man nutzt alle verfügbaren Quellen: Open Source, Veröffentlichungen, Datenbanken, Dienstleister. Dazu kommen persönliche Netzwerke und Kontakte vor Ort. Man fragt nach Stimmungen, Wahrnehmungen, Eindrücken. Ziel ist es, daraus ein einheitliches Lagebild zu erstellen.

Und wie unterscheidet sich das von staatlicher Intelligence-Arbeit?

Der wesentliche Unterschied ist, dass Unternehmen keine nachrichtendienstlichen Mittel einsetzen. Es gibt keine V-Leute oder geheimen Quellen. Man spricht mit Mitarbeitenden vor Ort, mit Partnern, mit anderen Unternehmen. Teilweise sind die Quellen sogar besser, weil wir auf Unternehmensnetzwerke zugreifen können.

Arbeiten konkurrierende Unternehmen dabei zusammen?

>

Ja, sehr stark sogar. Die Corporate-Security-Community in Deutschland ist hervorragend vernetzt. Viele wissen in eigenen Unternehmen gar nicht, dass es diese Funktion gibt oder was sie eigentlich machen. Aber innerhalb der Community gibt es einen starken Gemeinschaftsgeist. Man teilt Analyseerkenntnisse, ohne Geschäftsgeheimnisse preiszugeben.

Auch wenn das einen strategischen Vorteil bringen könnte?

Die meisten ticken nicht so machiavellistisch. Der unmittelbare Business Impact ist oft begrenzt. Und es ist auch ein Geben und Nehmen. Man bewegt sich in einer Community, in der man heute gibt und morgen bekommt. Während Corona hatten wir etwa im DAX-40-Forum regelmäßige Calls. Wöchentlich oder zweiwöchentlich, während der Arbeitszeit. Dort haben sich die Notfall- und Krisenmanager der großen Unternehmen ausgetauscht. Erkenntnisse, Best Practices, ganz pragmatisch.

Das klingt nach einer Community, in der man einander vertraut.

Das ist sie auch. Man kennt sich. Der Austausch ist sehr offen. Es herrscht eine ausgeprägte Need-to-share-Mentalität.

Wie wirkt sich die aktuelle geopolitische Lage auf Corporate Security aus?

Ehrlich gesagt wird das Thema momentan eher schwächer behandelt. Wir erleben eine massive Deindustrialisierung. Die wirtschaftliche Lage ist sehr angespannt. Unternehmen verlieren Geld und sparen dort, wo sich die Folgen erst mittel- oder langfristig zeigen. Corporate Intelligence gehört dazu.

Ist das so zu verstehen, dass diese Funktionen abgebaut werden?

Ja. Auch nachweislich erfolgreiche Stellen werden bei Vakanz oft nicht

nachbesetzt. Obwohl Krisen gut gemanagt wurden, obwohl frühzeitig antizipiert wurde. Gleichzeitig gibt es einen gegenläufigen Trend. Business Continuity Management wächst stark, weil es regulatorisch vorgeschrieben ist. Durch die neue NIS2-Gesetzgebung sind rund 40.000 Unternehmen verpflichtet, Risiko und BC Management Systeme einzuführen. Dafür muss Geld ausgegeben werden. Andere Bereiche zahlen den Preis.

Wo liegen die größten Schwierigkeiten für Corporate Intelligence im Unternehmensumfeld?

Entscheider kennen die Methoden geopolitischer Analyse schlicht nicht. Sie halten das für Kristallkugelleserei. Dass es strukturierte Verfahren gibt, wird ausgeblendet. Dazu kommen kognitive Verzerrungen. Auf Seiten der Analysten, aber auch bei Vorgesetzten.

Welche Folgen hat das?

In Bereichen, deren Ergebnisse schwer messbar sind, gilt oft das Präventionsparadox. Du bist erfolgreich, wenn nichts passiert. Aber ein Nicht-Ereignis lässt sich schlecht quantifizieren. Das führt dazu, dass viele Sicherheitsabteilungen defensiv agieren. Bloß nichts falsch machen. Nicht auffallen. Nicht innovativ sein. Wer nichts macht, macht nichts verkehrt. Analyseergebnisse versanden dann oft auf mittleren Ebenen.

Und wenn es gut läuft?

Dann liegt das meist an einer starken Führungspersönlichkeit, die fachlich versiert ist, Rückhalt hat und bereit ist, auch unbequeme Themen nach oben zu tragen. Nicht aus Karrieregründen, sondern um wirklich etwas zu bewegen.

Wie verändert Künstliche Intelligenz diese Arbeit?

Massiv. Schon jetzt. Trotz aller Unreife ist KI aus meinem Arbeitsalltag nicht

„Trotz aller Unreife ist KI aus meinem Arbeitsalltag nicht mehr wegzudenken.“

Christopher Radler-Morić

mehr wegzudenken. Texte, Analysen, Auswertungen, Systemaufbau. Das ist eine enorme Erleichterung. Sie ersetzt den Analysten noch nicht, weil es weiterhin Fachwissen und kritisches Denken braucht. Aber sie greift auf Datenmengen zu, die man manuell nie bewältigen könnte. Wir stehen erst am Anfang. Der Impact wird enorm sein.

Sie haben eigentlich Arabistik studiert.

Welche Rolle spielt der geisteswissenschaftliche Hintergrund für Ihre Arbeit?

Denken Sie auch in Fremdsprachen?

In mehreren Sprachen denken kann ich leider nicht. In mehreren Sprachen fluchen schon eher. Aber Spaß beiseite. Das ist ein sehr guter Punkt. Ich bin mit Arabistik und Ethnologie in der Konzernsicherheit tatsächlich ein Exot. Dort kommen viele aus Polizei oder Militär.

Hat Ihnen dieses Studium im Job konkret geholfen?

Sehr. Allein schon, weil ich mich in arabischen Ländern frei bewegen kann und keine Berührungsängste habe. Die Sprache öffnet Türen. Araber sind sehr stolz auf ihre Sprache. Als ich bei Daimler anfang, gab es Tochtergesellschaften in arabischen Ländern, und schnell war klar: Die betreue ich. Ich war dort willkommen. Man arbeitet einfach anders >

zusammen, wenn man sich versteht und respektiert fühlt.

Hat diese Erfahrung auch Ihre Einschätzungen geprägt?

Ja. Beim Arabischen Frühling zum Beispiel. Ich habe früh gesagt, dass diese Demokratisierungsversuche scheitern werden. Hoher Analphabetismus, freie Wahlen, daraus folgt der Wahlsieg der Muslimbrüder. Und dann folgt zwangsläufig die Gegenreaktion des Militärs. Genau so kam es. Das war kein formales Analysemodell. Das war ein Gefühl, gespeist aus Zeit vor Ort und aus kulturellem Verständnis.

Und jenseits spezieller Sprach- und Kulturkenntnisse?

Ein geisteswissenschaftliches Studium lehrt vor allem eines: sich in fremde Sachverhalte einzuarbeiten. Autodidaktisch. Ich habe gelernt zu lernen. Das hilft mir bis heute. Ich arbeite inzwischen in der Informationssicherheit, umgeben von IT-lern, Entwicklern, Hackern. Ich hatte davon anfangs keine Ahnung. Trotzdem bin ich schnell reingekommen, weil ich vernetztes Denken gewohnt bin.

Wie wichtig ist das Schreiben für Ihre Arbeit?

Schreiben können heißt nicht nur orthografisch korrekt sein. Es heißt, Gedanken zu strukturieren. Komplexes nachvollziehbar zu machen. Das ist ein Schlüsselskill. Egal ob beim Aufbau eines Krisenmanagementsystems oder bei einer geopolitischen Analyse.

Wie viel Raum hat in Ihrer Arbeit das Nicht-Rationale? Emotionen, Unberechenbarkeit?

Eigentlich keinen. Ich behaupte, dass es kaum irrationales Verhalten gibt. Das klingt provokant. Natürlich gibt es Ausnahmen. Aber 99 Prozent dessen, was passiert, folgt einer Rationalität.

Auch bei scheinbar irrationalen Entscheidungen?

Ja. Die Rationalität erschließt sich oft nur nicht aus unserer Perspektive. Man muss versuchen, die Welt durch die Brille des anderen zu sehen. In der Ethnologie spricht man von „emisch“ und „etisch“. Der eigene Blick und der Blick aus der Perspektive des Gegenübers. Dann wird vieles plötzlich logisch. Vielleicht nicht ökonomisch rational, aber sozial oder psychologisch rational.

„Man muss versuchen, die Welt durch die Brille des anderen zu sehen.“

Christopher Radler-Morić

Was würden Sie deutschen Unternehmern jetzt raten, gerade mit Blick auf Intelligence und Sicherheit?

Sicherheit im weitesten Sinne sollte ernst genommen werden, besonders Intelligence. Sie sollen sich gute Leute einkaufen. Und sie sollen diese Funktion ans Top-Management anbinden. Oft fristet Sicherheit ein Nischendasein, irgendwo bei HR oder in einem anderen Bereich. Besser wäre eine Stabsstelle. Dann wird Intelligence auch für Geschäftsentscheidungen nutzbar und nicht nur dafür, zu prüfen, ob ein Expat in einer bestimmten Straße neben einem bestimmten Hotel wohnen kann.

Das heißt, proaktiver werden – Intelligence früh in Entscheidungen einbeziehen?

Absolut. Da steckt viel Potenzial drin. Klassische Analysten sind häufig keine Betriebswirte, die nur auf die Marge schauen. Sie bringen einen unverbrauchten Blick mit. Sie denken eher außerhalb des bekannten Rahmens. Und sie filtern Chancen und Risiken durch eine andere Brille.

Wo sehen Sie das besonders?

Bei Standortentscheidungen zum Beispiel. Oft entscheidet eine Geschäftsführung, irgendwo einen Standort zu eröffnen. Und erst später wird Sicherheit eingebunden. Ich habe mehrfach erlebt, dass man früher bessere Standorte hätte wählen können, aus ganz unterschiedlichen Gründen. Nicht nur aus Sicherheitssicht. Aber dann ist die Entscheidung schon gefallen. ■

„Zweifel bleibt menschlich“

Was unterscheidet strukturierte Analyse von bloßem Bauchgefühl? Intelligence-Analyst Ole Donner erklärt, wie man kognitive Verzerrungen vermeidet, was gute und schlechte Fragen unterscheidet – und warum KI nur ein Hilfsmittel ist.

Ole Donner, angenommen, Sie sind Teil einer Task Force, die die Ursachen des Berliner Blackouts im Januar 2026 untersuchen soll. Wie würden Sie vorgehen?

Ole Donner: Wichtig ist, den Analyseprozess breit anzulegen und nicht ersten Intuitionen zu folgen. Zunächst werden verschiedene Hypothesen zu möglichen Ursachen oder Akteuren gebildet. Anschließend geht es darum, nicht einzelne Annahmen zu bestätigen, sondern konkurrierende Hypothesen systematisch zu falsifizieren. Grundlage ist die Analysis of Competing Hypotheses: Alle Hypothesen werden mit verfügbaren Informationen abgeglichen. Am Ende gilt jene als am wahrscheinlichsten, gegen die am wenigsten spricht.

Jetzt sitzt in dieser Task Force jemand mit 30 Jahren Erfahrung, etwa ein Polizeibeamter, der sagt: Mein Bauchgefühl sagt mir, das war X. Wie gehen Sie damit um?

Intuition ist am Ende ein Ausfluss von Erfahrung und die würde man selbstverständlich einbeziehen. Diese Intuition ist zunächst einmal eine Annahme und wird auch als solche in die Analyse aufgenommen. Man würde ihr aber eine andere Glaubwürdigkeit beimessen als harten Fakten.

Was unterscheidet eine gute von einer schlechten Frage in Analyseprozessen?

Das ist immer kontextabhängig. Schlecht formulierte Fragen sind oft zu eng oder zu weit. Häufig sind „Gib-mir-alles-Fragen“ wie „Schreiben Sie etwas zum Blackout in Berlin“ – das sind keine echten Fragen. Problematisch sind auch annahmengetriebene Fragen, etwa „Wo sind die Massenvernichtungswaffen?“, weil sie Antworten vorwegnehmen. Hinzu kommen rhetorische Fragen, unklare Begriffe oder Fragen, die mit den verfügbaren Informationen nicht beantwortbar sind. >



INTERVIEW_ Ole Donner

Ole Donner ist Gründer von Strukturierter Analyse Deutschland und berät staatliche Institutionen, internationale Organisationen und Unternehmen zu Intelligence- und Analysefähigkeiten. Zuvor war er 13 Jahre bei der Bundeswehr als Analyst, Vorgesetzter und Dozent tätig und prägte dort die Analyseausbildung. Er ist Mitautor u. a. des Buchs „Clear Thinking“ (2025) sowie Initiator der German Intelligence Community Conference (GICC).

KEY MESSAGES

→ **Gute Analyse** beginnt mit konkurrierenden Hypothesen und dem Versuch, Annahmen zu widerlegen, statt zu bestätigen.

→ **Intuition** ist wertvoll, aber nur als Ausgangspunkt – nicht als Ersatz für überprüfbare Evidenz.

→ **Kognitive Verzerrungen** lassen sich nicht individuell „abschalten“, sondern nur durch strukturierte Teamarbeit begrenzen.

→ **KI kann Analyse unterstützen**, etwa bei Hypothesenbildung, ersetzt aber weder Urteilsvermögen noch Verantwortung.

→ **Der entscheidende menschliche Vorteil** bleibt abstraktes Denken: Sinnstiftung, Zweifel und das Fragen nach dem Warum.

Die Mutter aller kognitiven Verzerrungen ist der Bestätigungsfehler. Also nur nach Informationen zu suchen, die die eigene Hypothese stützen. Warum ist dieser Bias so schwer in den Griff zu bekommen?

Der Bestätigungsfehler entsteht, weil wir Ambivalenz und kognitive Dissonanz schlecht aushalten. Widersprüche werden ausgeblendet, bestätigende Informationen bevorzugt. Das ist menschlich – und gefährlich. Abhilfe schafft Teamarbeit: Analyse sollte nicht allein erfolgen. Heterogene Teams mit unterschiedlichen Hintergründen und Perspektiven erkennen Biases besser und erhöhen die Analysequalität.

Also Diversity in einem weiten Sinn?

Organisationen glauben oft, Diversität bereits zu leben. Die NATO wirkt vielfältig durch Nationen, Geschlechter und Dienstgrade. Doch ähnliche Sozialisation prägt stärker als formale Unterschiede. Ein Soldat aus Spanien hat oft mehr gemeinsam mit einem deutschen Soldaten als mit einem spanischen Zivilisten. Entscheidend ist daher nicht äußere Vielfalt, sondern die Diversität der Perspektiven und Denkweisen, etwa durch unterschiedliche akademische Hintergründe.

Reicht es dann nicht, wenn eine Person im Team eine Gegenmeinung vertritt?

Darauf zu bauen, ist gefährlich. Es gibt Techniken wie den Devil's Advocate. Aber in der Praxis funktioniert das oft nicht. Wenn ein Team viel Arbeit investiert hat und dann jemand von außen kritisiert, führt das meist nicht zu Selbstkritik, sondern zu stärkerer Gruppenkohäsion. Das Ergebnis wird noch vehementer verteidigt. Deshalb sind solche Techniken in neueren Standardwerken zurückgenommen worden. Stattdessen setzt man auf Methoden, die die ganze Gruppe zur

Kritik befähigen, etwa die Premortem-Analyse.

Worum geht es dabei?

Bei der Premortem-Analyse stellt man sich vor, das Analyseprodukt wurde veröffentlicht und wir befinden uns 36 Monate in der Zukunft. Rückblickend stellen wir fest: Wir lagen spektakulär falsch. Dann fragen wir uns gemeinsam: Woran lag das? Dieser Perspektivwechsel macht es viel leichter, Schwachstellen offen zu benennen. Kritik wird nicht nur erlaubt, sondern eingefordert.

Analysten, die verstehen, wie diese Systeme funktionieren und ihre Ergebnisse kritisch einordnen können.

Das klingt nicht nach Komplexitätsreduktion durch KI, sondern eher nach Komplexitätssteigerung.

Man muss zwei Ebenen trennen: den Intelligence-Prozess mit Sammlung, Verarbeitung und Aufbereitung sowie die eigentliche Analyse. In den ersten Bereichen kann KI Effizienzgewinne bringen – etwa Zeitersparnis für Analysten. Strukturierte Analysetechniken

„KI fungiert im Analyseprozess eher als Praktikant oder neue Kollegin.“

Ole Donner

Welchen Einfluss hat KI auf Analyse im Intelligence-Bereich?

Zunächst muss man klären, was man mit KI meint. Meist sind es Large Language Models. Die eignen sich dort, wo Ergebnisse nicht zwingend richtig sein müssen, etwa beim Generieren von Hypothesen, Fragen oder Collection-Plänen.

Für das Liefern von Antworten wäre ich sehr vorsichtig. LLMs sind nicht deterministisch. Gleicher Input führt nicht immer zu gleichem Output.

Kann eine KI in einem Analyseprozess als Teammitglied fungieren ?

Eher als Praktikant oder eine neue Kollegin. Da kann Brillantes kommen oder kompletter Unsinn. Alles muss überprüft werden. KI spart kein Personal, sondern erfordert eher mehr und besser qualifizierte Analystinnen und

beruhen jedoch auf kritischem, rationalem Denken. Das lässt sich nicht an LLMs auslagern, da auch sie Biases haben. Hypothesen, Fragen oder Vorschläge ja, aber die eigentlichen Schlussfolgerungen bleiben menschlich.

Was ist, wenn ein LLM etwa einen Unsicherheitsfaktor identifiziert, den Sie als Analyst gar nicht sehen oder für unplausibel halten?

Wenn etwas wirklich absurd ist, würde ich es verwerfen. Wenn es abwegig klingt, aber nicht ausgeschlossen ist, und der Impact im Falle des Eintretens enorm wäre, dann würde ich es aufnehmen. Nicht weil das LLM recht hat, sondern als Anlass, noch einmal darüber nachzudenken. Gerade bei Low-Probability-High-Impact-Szenarien kann das sinnvoll sein, wenn ich die Kapazitäten habe. >

Gibt es nicht auch einen umgekehrten Bias? Also die Annahme, dass der Mensch der KI grundsätzlich überlegen ist? Und wie geht man mit Schatten-KI um, also Analysten, die KI heimlich nutzen?

Beides sind reale Probleme. Automation Bias auf der einen Seite, Überheblichkeit auf der anderen. Und natürlich gibt es die Versuchung, schnell etwas produzieren zu lassen. Deshalb steigen die Anforderungen an Ausbildung massiv. Wer versteht, dass bei nicht lokal gehosteten Systemen Daten nach außen gehen, sollte solche Tools in sensiblen Bereichen nicht nutzen.

Was ist aus Ihrer Sicht der entscheidende menschliche Faktor in der Analyse?

Menschen können Dinge, die LLMs nicht können. Ein zentrales Beispiel ist abstraktes Denken. Menschen erkennen Bedeutungen, Analogien und Beziehungen, die nicht explizit vorliegen. LLMs verstehen weder wirklich den Input noch den Output. Im Kern ist das Statistik. Abstraktes Denken bleibt menschlich. Das gilt auch für Zweifel. Dieses Gefühl, dass etwas nicht stimmt. Und für die Frage nach dem Warum. Sinnstiftung, Sense-Making, ist weiterhin Domäne des Menschen.

Dieses Gefühl, dass etwas nicht stimmt, woher kommt das?

Das ist Intuition, also System-1-Denken. Sie sollte nicht dazu führen, sofort etwas zu verwerfen. Aber sie ist ein Signal, genauer hinzuschauen. Intuition kann auf Lücken oder Fehler hinweisen. Diese überprüfe ich dann strukturiert mit System-2-Denken. Beides gehört zusammen.

Wie kann man aus Analysefehlern lernen?

Die Voraussetzung ist Nachvollziehbarkeit. Viele Analysen entstehen noch immer im stillen Kämmerlein. Wenn sich später herausstellt, dass etwas falsch war, kann niemand mehr rekonstruieren, warum bestimmte Schlüsse gezogen wurden. Der Analyseprozess muss daher dokumentiert werden. Strukturierte Analysetechniken externalisieren den Denkprozess. Sie erzeugen einen Audit Trail. Nur so kann man auch Monate später noch lernen. Struktur schützt nicht vor Irrtum, aber sie macht ihn sichtbar und erklärbar.

Nutzen Sie strukturierte Analyse auch bei privaten Entscheidungen?

Das hängt von der Tragweite der Entscheidung ab. Bei Routineentscheidungen mit geringen Kosten reichen Heu-

ristiken. Bei großen Entscheidungen lohnt Struktur. Beim Hauskauf haben wir zunächst eine Pair Comparison genutzt und Faktoren wie Kita-Nähe und Internet paarweise gewichtet. Das führte zu sehr aufschlussreichen Diskussionen. Wir wollten das dann noch in eine Decision Matrix überführen. Das wurde durch den engen Immobilienmarkt aber weitgehend überflüssig.

Das klingt ganz schön kopflastig!

Diese Arbeit verändert die Art zu denken. Beim Kinderarzt sah ich eine Frau aus einer Kita kommen, ein Fahrrad nehmen und wegfahren. Mein erster Gedanke: Sie hat ihr Kind gebracht. Der nächste Schritt ist jedoch, weitere Möglichkeiten zu prüfen: Sie könnte Mitarbeiterin sein, etwas erledigen – oder das Rad gehört ihr gar nicht. Dieses Nicht-Verharren bei der ersten Hypothese, mehrere plausible Erklärungen zu bilden, prägt meinen Alltag. Teilweise übernehmen das heute sogar meine Kinder. ■

„Abstraktes Denken bleibt menschlich. Das gilt auch für Zweifel, dieses Gefühl, dass etwas nicht stimmt. Und für die Frage nach dem Warum. Sinnstiftung, Sense-Making, ist weiterhin Domäne des Menschen.“

Ole Donner

03_ Technology

Eigene Fähigkeiten statt Abhängigkeiten

„The most effective use of cyber operations is for information operations: deceiving, confusing, and altering the decision-making calculus of your adversary.“

Marcus Willett, UK

Illustration clu/Stock





„The Doughnut“ – Zentrale des GCHQ in Cheltenham, Gloucestershire (Südwestengland)

„Am Ende geht es immer um Menschen“

Das britische Government Communications Headquarters (GCHQ), zuständig für Fernmeldeaufklärung und Cybersicherheit, gilt als einer der besten Geheimdienste der Welt. Ex-GCHQ-Mann Marcus Willett über offensive Cyberoperationen, den Wert von All-Source-Assessment – und den Sinn seiner früheren Arbeit.



INTERVIEW_ Marcus Willett

Marcus Willett (CB, OBE) arbeitete 33 Jahre für das britische Government Communications Headquarters (GCHQ), zuletzt als stellvertretender Leiter des Dienstes mit persönlicher Verantwortung für Nachrichtengewinnung und Cyberoperationen. Davor war er der erste Cyber-Director im GCHQ und leitete das UK National Offensive Cyber Programm. Seit seinem Ausscheiden 2018 ist er Senior Advisor beim International Institute for Strategic Studies (IISS). 2024 erschien sein Buch „Cyber Operations and their Responsible Use“.

Marcus Willett, Sie haben mehr als drei Jahrzehnte beim GCHQ gearbeitet, zuletzt als stellvertretender Leiter des Dienstes. Wie fühlt es sich für Sie an, wenn Sie als ehemaliger Geheimdienst-Mitarbeiter auf die heutige Welt blicken?

Marcus Willett: „Bedrückend“ ist vermutlich das Wort, das ich verwenden würde, wenn ich an die aktuelle Lage mit den Vereinigten Staaten denke. Ich habe viele Jahre sehr eng mit ihnen zusammengearbeitet, auch im Rahmen der Five-Eyes-Nachrichtendienstallianz. Eine unserer Überzeugungen war, dass Präsidenten und Premierminister kommen und gehen, die Allianz jedoch Bestand haben würde, weil sie den nationalen Interessen aller Beteiligten dient – auch denen der Amerikaner. Diese Logik reichte über „Five Eyes“ hinaus und galt ebenso für die Zusammenarbeit mit europäischen und ande-

ren internationalen Partnern, die enge Verbündete sowohl des Vereinigten Königreichs als auch der USA sind.

Was steht hier konkret auf dem Spiel?

Einer der zentralen strategischen Vorteile des Westens gegenüber autoritären Gegnern ist genau diese Fähigkeit, in Allianzen so eng zusammenzuarbeiten. Derzeit scheint dieser Vorteil ernsthaft unter Druck zu stehen. Der gegenwärtige US-Präsident und seine Administration stellen die größte Herausforderung für diese Annahme dar, an die ich mich erinnern kann. Mitunter fühlt es sich schwieriger an, Verbündeter der Vereinigten Staaten zu sein als ihr Gegner. Dieses Verhalten stellt Dinge infrage, die wir vielleicht zu naiv als selbstverständlich angesehen haben: die regelbasierte internationale Ordnung, die Stärke von Allianzen und die Art und Weise, wie wir über Jahr-

KEY MESSAGES

- **Cyberoperationen** reichen von niedrigschwelligen Störaktivitäten bis zu Angriffen, die Systeme lahmlegen.
- **Die effektivste Nutzung** liegt in Informationsoperationen, die auf Täuschung und Verwirrung des Gegners zielen
- **Cyberoperationen** können Gegner stören, sind aber nicht zuverlässig genug für strategische Abschreckung.
- **Verantwortungsvolle Operationen** müssen sich am präzisen Verständnis der Wirkung orientieren.
- **Wichtige Entscheidungen** sollten auf All-Source-Assessment, also Bewertung unterschiedlicher Quellen beruhen.

„Vertrauen ist für gemeinsame Operationen und den Aufbau gemeinsamer Fähigkeiten unerlässlich.“

Marcus Willett

zehnte hinweg unsere Fähigkeiten miteinander verflochten haben. Plötzlich sprechen alle von strategischer Autonomie – sei es in wirtschaftlichen, sicherheits- oder verteidigungspolitischen Arrangements. Die Welt wirkt deutlich komplexer und erinnert in mancher Hinsicht eher an die Zeit vor dem Zweiten Weltkrieg: ein System aus Supermächten und Mittelmächten, in dem Letztere sehr sorgfältig darüber nachdenken müssen, wie sie sich zu allen Supermächten verhalten – nicht nur zu ihren traditionellen Gegnern. Insofern muss ich sagen, ja: Insgesamt ist das deprimierend.

Wie könnte sich das auf die praktische Zusammenarbeit zwischen den Diensten auswirken?

Vertrauen ist für gemeinsame Operationen und den Aufbau gemeinsamer Fähigkeiten unerlässlich und hat historisch auch Regierungswechsel überstanden. Gleichwohl gab es immer nationale Vorbehalte, die den Austausch mit Verbündeten einschränken, und diese könnten nun zunehmen. Wichtiger ist jedoch, dass Partner wie das Vereinigte Königreich, die anderen Five-Eyes-Mitglieder und die europäischen Staaten Washington zunehmend an ihre eigenen Beiträge und an die Abhängigkeit der USA von ihnen erinnern sollten. Ich bin der Auffassung, dass Nachrichtendienstpartnerschaften immer auf gegenseitiger Abhängigkeit beruht haben – ein Ziel, das für jeden Partner weitaus realistischer und sinnvoller ist

als vollständige Unabhängigkeit und Autonomie. Während dies auf technokratischer Ebene in den USA verstanden wird, zeigt die aktuelle Administration ein überraschend oberflächliches Verständnis dafür, wie internationale Allianzen funktionieren – ein Ansatz, der gefährlich ist, auch für die USA selbst, und der ihre internationalen Partner dazu zwingt, sie an die Realität zu erinnern. In der Welt der Geheimdienst-Allianzen kann das Land, das man – um es in trumpianischer Sprache zu sagen – als den „Big Dog“ betrachtet, je nach Thema und Kontext wechseln. Manchmal sind es die USA, manchmal auch nicht.

Als stellvertretender Leiter des GCHQ trugen Sie unter anderem die persönliche Verantwortung für sämtliche Cyberoperationen. Was ist der Unterschied zwischen Cybersicherheit, Cyber Intelligence und Cyberoperationen?

Cybersicherheit konzentriert sich auf den Schutz von Netzwerken, Daten und Informationen und basiert auf dem klassischen Dreiklang aus Vertraulichkeit, Integrität und Verfügbarkeit. Sie umfasst Angriffserkennung, Schutzmaßnahmen, Risikoreduzierung, Resilienz, Wiederherstellung und Reaktion. Ich habe sie einmal als „Torlinienvorverteidigung“ beschrieben – ein ausgereiftes Feld mit einer eigenen Industrie. Eng damit verwandt – so wie Wildhege und Wilderei miteinander verwandt sind – ist Cyber Intelligence, im Grunde moderne SIGINT, da die meisten Signale

heute im Cyberraum existieren. Grob gesprochen gibt es zwei Formen: passive und aktive. Passiv bedeutet, Datenverkehr abzugreifen, während er einen Sammelpunkt passiert – die Comic-Version wären Krokodilklemmen an einem Kabel. Aktiv meint Hacking, in der „Five-Eyes“-Community „Computer Network Exploitation“ genannt. Dann gibt es Cyberoperationen. Das ist eine sehr breite Kategorie. Sie umfasst cybergestützte Informationsoperationen sowie niedrigschwellige Störaktivitäten wie DDoS-Angriffe oder Defacement (Verunstaltung) öffentlich zugänglicher Webseiten. Solche Aktivitäten werden oft als Cybervandalismus bezeichnet und mit sogenannten patriotischen Hackern in Verbindung gebracht. Am oberen Ende des Spektrums stehen tatsächlich offensive Operationen, die darauf abzielen, gegnerische Systeme lahmzulegen oder zu zerstören – also Aktivitäten, die den Begriff „Angriff“ wirklich verdienen.

Was sind „offensive“ Cyberoperationen im engeren Sinne?

Die pauschale Verwendung des Begriffs „offensives Cyber“, um alle Cyberoperationen zu beschreiben, hat sich als irreführend erwiesen, weil nicht alle Cyberoperationen offensiv sind. Informationsoperationen oder Vandalismus sind es nicht wirklich, und selbst lahmlegende Cyberoperationen werden häufig zu defensiven Zwecken durchgeführt, etwa um die Infrastruktur von Cyberkriminellen zu stören. Es gibt >

öffentliche Beispiele für US-amerikanische und britische Operationen gegen Cyberkriminelle oder – im Fall der USA – für das Abschalten der Internet Research Agency während der Zwischenwahlen 2018, und zwar aus defensiven, nicht aus offensiven Gründen. Deshalb haben wir uns im Vereinigten Königreich auf den weiter gefassten Begriff „Cyberoperationen“ verständigt, der offensive Elemente einschließt, aber weit darüber hinausgeht. Cyber Intelligence unterstützt sowohl die Cybersicherheit als auch Cyberoperationen. Sie hilft, Bedrohungen und Risiken zu verstehen – oft mit Erkenntnissen, denen man vertrauen kann, weil man die Quelle kennt und überprüfen kann.

Wo endet Cyber Intelligence und wo beginnt eine Cyberoperation?

Um eine Cyberoperation verantwortungsvoll durchzuführen, braucht man Aufklärung und Informationsbeschaffung. Bis der Effekt erzielt wird, kann das exakt wie geheimdienstliche Informationsgewinnung aussehen. Oft ist der einzige Unterschied das Ziel. Wenn man sich mit einem Wasserversorger oder einem Energiesystem befasst: sammelt man Informationen – oder bereitet man eine Störung vor? Die Grenzen verschwimmen. Diese Unschärfe erschwert es, die Absicht hinter Operationen unserer Gegner zu interpretieren. Manchmal ist es schlicht sehr schwer zu erkennen, wozu eine Operation tatsächlich dient.

Die Debatte über Cyberbedrohungen schwankt zwischen Übertreibung und Verharmlosung.

Das Problem liegt bei den Eigeninteressen. Akteure mit Fokus auf nationale Cybersicherheit argumentieren häufig, Ausgaben für offensive Cyberfähigkeiten seien verschwendet und sollten

vollständig in die Verteidigung fließen. Militärisch geprägte Denkschulen hingegen neigen dazu, offensives Cyber – als digitales Äquivalent von Feuerkraft – auf Kosten der Verteidigung zu überbetonen. Das polarisiert die Debatte: Einige behaupten sogar, Cyberoperationen lieferten strategische Abschreckung. Andere wiederum argumentieren, sie hätten nie echte strategische Wirkung gehabt und würden auch künftig keine haben.

Wie lautet Ihre Position dazu?

Ich vertrete die Auffassung, dass die Wahrheit in der Mitte liegt. Wer behauptet, Cyber habe keine strategische Wirkung, sollte sich ansehen, was derzeit offen sichtbar durch den kriminellen Einsatz von Ransomware geschieht. Er hat massive und weitreichende Störungen verursacht – nicht nur für Unternehmen, sondern für ganze Staaten. In Costa Rica und Indonesien etwa hat Ransomware staatliche Funktionen lahmgelegt. Zwar handelte es sich dabei um kriminelle Aktivitäten, doch Staaten können auf dasselbe Ökosystem an Fähigkeiten zurückgreifen, und Länder wie Russland, Iran und Nordkorea haben Ransomware tatsächlich wegen ihres Störpotenzials eingesetzt. Im Krieg jedoch greifen Staaten eher auf Raketen und Bomben zurück, um zentrale Funktionen wie kritische Infrastruktur zu beeinträchtigen. Der Grund ist, dass Cyberoperationen während ihrer Durchführung gestört oder abgewehrt werden können, ihre zerstörerische Wirkung also nicht sicher ist und sie daher keine echte strategische Abschreckung darstellen. Dennoch liegt die eigentliche Gefahr nicht darin, Cyber zu überschätzen, sondern darin, es zu unterschätzen – bis der Schaden eingetreten ist. Genau deshalb habe ich eben

auf den Einsatz von Ransomware „vor unseren Augen“ hingewiesen.

Welche spezifischen Risiken bergen offensive Cybermaßnahmen aus operativer Perspektive?

Für einen demokratischen Staat wie das Vereinigte Königreich unterliegt der Einsatz von Cyberoperationen einer engen politischen und rechtlichen Kontrolle. Sie müssen verhältnismäßig und notwendig sein und im Kriegsfall zwischen Kriegsparteien und Nicht-Kriegsparteien unterscheiden sowie human durchgeführt werden. Die Folge ist, dass Cyberoperatoren auf Präzision setzen, eine enge Führungs- und Kontrollstruktur aufrechterhalten und fortlaufend auf unbeabsichtigte Wirkungen oder „Kollateraleffekte“ achten. Gleichzeitig ist es schwierig, kostspielig und hochkomplex, verlässliche Effekte gegen gehärtete militärische Ziele zu erzielen. Der Fall des Computerwurms Stuxnet zeigt das: eine hochgradig zielgerichtete Operation gegen ein stark gesichertes Ziel, die jahrelange Arbeit zahlreicher Experten erforderte – sie wurde als das cybertechnische Äquivalent einer Mondlandung bezeichnet. Deshalb könnten Staaten offensive Cyberoperationen als wirksamer ansehen, wenn sie gegen weniger gehärtete kritische nationale Infrastrukturen eingesetzt werden. Dennoch liegt die aus meiner Sicht effektivste Nutzung von Cyberoperationen in Informationsoperationen: Täuschung, Verwirrung und die Veränderung der Entscheidungslogik des Gegners. Dort entfaltet Cyber die größte Wirkung. So sind wir gegen Gruppen wie den sogenannten Islamischen Staat und Al-Qaida vorgegangen – nicht mit dem Ziel, sie digital zu zerstören, sondern sie zu verwirren, ihre Entschei- ➤

„Verantwortungsvoller Cybereinsatz erfordert klare Zielsetzung, präzise Zielauswahl und stete Überwachung.“

Marcus Willett

dungsprozesse zu untergraben und ihre Propaganda zu schwächen, indem ihre Narrative lächerlich gemacht wurden.

Wie gravierend ist das aktuelle Desinformationsproblem?

Es ist enorm – und für liberale Demokratien besonders schwierig, weil das, was der eine als Desinformation bezeichnet, ein anderer als strategische staatliche Kommunikation oder Propaganda versteht. Die Grenze ist sehr schmal und kaum zu kontrollieren. Zensur mag für manche Staaten funktionieren, ist in offenen Gesellschaften jedoch keine Option. Stattdessen konzentrieren sich unsere Bemühungen auf digitale Kompetenz, darauf, Menschen bei der Erkennung von Manipulation zu unterstützen, sowie auf die Verifikation von Informationen, etwa durch „digitale Wasserzeichen“. Doch auch diese Ansätze stoßen an Grenzen. Das ist eine der großen Herausforderungen des 21. Jahrhunderts. Desinformation, Spionage und disruptive Effekte sind keine neuen Phänomene staatlichen Handelns; was der Cyberraum verändert hat, sind Maßstab, Geschwindigkeit und globale Reichweite. Die Effekte sind nicht neu – sie treten nur schneller und in viel größerem Umfang auf.

Und nun kommt KI hinzu, die Desinformation nahezu unbegrenzt skalieren könnte.

Ja – und nach KI werden wir über Quantentechnologien sprechen. Es gibt immer eine neue Technologie, die scheinbar das Gleichgewicht zu verändern droht. Bei generativer KI sehen

wir bereits ihren Einsatz durch Cyberangreifer – staatliche wie nichtstaatliche – für Phishing, Zielauswahl und Programmierung. Diese Fähigkeiten sind leicht zugänglich. Zugleich hilft KI aber auch der Verteidigung: Sie ist sehr gut darin, Anomalien in Netzwerken zu erkennen, und beim Programmieren – oft besser als Menschen –, was weniger Fehler und weniger ausnutzbare Schwachstellen in IT-Systemen bedeutet. Im Bereich von Cyberangriffen dürfte das Kräfteverhältnis daher relativ ausgeglichen bleiben. Der Bereich, wo KI das Gleichgewicht wirklich verschiebt, ist die Desinformation – hier verlagert sich der Vorteil deutlich auf die Angreifer, und das ist besorgniserregend.

Was kann Europa aus den britischen Erfahrungen über verantwortungsvollen Cybereinsatz lernen?

Zunächst eine organisatorische Lehre: Während die USA Cyberoperationen über mehrere Stellen hinweg durchführen, hat das Vereinigte Königreich eine integrierte Fähigkeit geschaffen – die National Cyber Force –, die Ressourcen von GCHQ und dem Verteidigungsministerium bündelt. Eine Fähigkeit unterstützt mehrere Missionen, gesteuert durch Genehmigungen und strenge rechtliche Aufsicht. Wie erwähnt, sind Notwendigkeit und Verhältnismäßigkeit zentrale Prinzipien; Operationen wurden gestoppt, wenn zu hohe Kollateraleffekte zu erwarten waren. Ich habe Einsätze erlebt, die darauf abzielten,

einzelne Terroristen handlungsunfähig zu machen, aber abgebrochen wurden, weil mögliche Schäden für Familienangehörige oder andere Kontaktpersonen als unverhältnismäßig galten.

Verantwortungsvoller Cybereinsatz erfordert klare Zielsetzung, präzise Zielauswahl, kontinuierliche Überwachung sowie die Fähigkeit, Operationen zu stoppen oder anzupassen. Im Krieg kommt die Pflicht hinzu, rechtliche Schutzvorschriften für Nichtkombattanten einzuhalten. Verantwortung bedeutet außerdem, überhaupt festzulegen, welche Ziele legitim sind – ein äußerst komplexes und oft missverständliches Thema. Im Krieg unterstützt die kritische nationale Infrastruktur häufig die Kriegsführung oder wird sowohl militärisch als auch zivil genutzt (Dual Use). Damit kann sie grundsätzlich ein legitimes Ziel darstellen – vorausgesetzt, die Angriffe erfolgen verhältnismäßig, notwendig, unterscheidend und human. Das wiederum bedeutet, dass solche Ziele in Friedenszeiten für Aufklärung, Informationsgewinnung und sogar für das vorbereitende Positionieren von Fähigkeiten in Betracht kommen. Das hat zahlreiche Implikationen, auf die wir hier nicht näher eingehen können.

Was sind die praktischen Kriterien für verantwortungsvolle Operationen?

Bei Cyberoperationen beginnt alles mit dem Verständnis der Wirkung. Reaktionen auf Cyberangriffe müssen sich an der tatsächlich erzielten oder beab-

sichtigten Wirkung orientieren – genauso wie eigene Zielauswahl, Steuerung und Kontrolle die beabsichtigte Wirkung widerspiegeln müssen. Das wird häufig missverstanden: So wird etwa nachrichtendienstliche Cyberaufklärung oft als kriegerischer Akt bezeichnet, obwohl sie – gemessen an ihrer Wirkung – eindeutig keiner ist. Vorfälle wie der russische SolarWinds-Hack oder der chinesische Angriff auf das US-Office of Personnel Management waren Intelligence-Operationen, keine Kriegshandlungen, wie der damalige Director of National Intelligence James Clapper im letzteren Fall offen erklärte.

Ein weiteres Beispiel dafür, wie entscheidend es ist, von der Wirkung her zu denken: Ich habe einmal einen NATO-Generalsekretär dazu gebrieft, wie zu beurteilen sei, ob ein Cybervorfall den NATO-Bündnisfall nach Artikel 5 auslösen würde. Meine Antwort war schlicht: Sie werden es merken – denn die Wirkung würde in Zerstörungsgrad und Auswirkungen einem Ereignis wie den Anschlägen auf die Twin Towers ähneln. Dann greift Artikel 5. Dass der Angriff seinen Ursprung im Cyberraum hat, ist dabei nahezu irrelevant.

Worin liegt der Unterschied?

Der zentrale Unterschied liegt zwischen Informationsdiebstahl und Operationen, die Störungen oder Schäden verursachen. Erst wenn Wirkungen destruktiv werden, stellt sich die Frage, ob es sich um eine Gewaltanwendung handelt. Und hier kann Attribution eine Schlüsselrolle spielen. Westliche Staaten ordnen festgestellte Cyberintrusionen seit einiger Zeit detailliert zu – oft bis hin zur Benennung einzelner Täter. Das geschieht nicht in der Erwartung, dass diese tatsächlich verhaftet werden, sondern aus Gründen der Abschre-

ckung. Das Signal lautet: Wir wissen, was ihr getan habt, und wenn ihr eine Grenze überschreitet und etwas tut, das als Gewaltanwendung gelten könnte, werdet ihr ebenso detailliert attribuiert – was eine ganze Bandbreite legitimer Reaktionen und Gegenmaßnahmen eröffnet. Wir schaden uns selbst, wenn wir darauf beharren, Attribution sei unmöglich schwierig, obwohl sie es eindeutig nicht ist. Sie kann erfolgen – unter Nutzung geheimer wie offener Quellen. Schwieriger ist es allerdings, geheime Erkenntnisse öffentlich zu machen, doch auch hier werden Staaten besser und finden Wege. Und wäre die Wirkung gravierend genug, würde man die öffentliche Attribution ohnehin vornehmen.

Sie haben 2024-25 für das Cabinet Office die britische Intelligence-Assessment-Funktion evaluiert. Worum ging es dabei?

Zur Einordnung: Es war nicht das erste Mal, dass ich an einer Überprüfung der britischen Intelligence-Assessment-Funktion beteiligt war. Ich gehörte auch zu dem kleinen Team, das sie nach der Irak-WMD-Affäre untersuchte. Ich war GCHQs Vertreter in dem Team, das das Irak-Dossier erstellte, und ich bin stolz darauf, dass ich damals entschieden dagegeengehalten habe, Material zu verwenden, dessen Quellenlage nicht ausreichend war – was zu jener Zeit nicht überall der Fall war. Diese Erfahrung hat mir die Bedeutung eines sachgerechten All-Source-Assessment eindrücklich vor Augen geführt.

Könnten Sie das näher erläutern?

Wenn die meisten Menschen an das britische System geheimer Nachrichtendienste denken, denken sie an GCHQ, MI5 und MI6 – also an Behörden zur Informationsgewinnung, wobei SIGINT und HUMINT jeweils als „Einzelquellen“

verstanden werden. Doch Informationsgewinnung ist nur ein Teil des Systems. Wichtige Entscheidungen sollten, wo immer möglich, auf all-source-basierter, bewerteter Intelligence beruhen, bei der Informationen aus allen relevanten Quellen – geheimen wie offenen – gemeinsam abgewogen und von fachkundigen Analysten objektiv beurteilt werden. Neben geheimem Material der Dienste können dabei auch diplomatische Berichte, routinemäßige Regierungsdaten sowie das rasch wachsende Volumen offen verfügbarer Informationen oder „Big Data“ einbezogen werden, einschließlich solcher aus der Privatwirtschaft, etwa von kommerziellen Intelligence-Firmen. Zur Veranschaulichung: Erkenntnisse von Unternehmen aus dem

Cybersicherheitssektor sind ein zentraler Bestandteil jedes staatlichen Verständnisses von Cyberbedrohungen und Verwundbarkeiten.

Wie können Nachrichtendienste mit dieser Informationsmenge umgehen?

Natürlich hilft Technologie, etwa KI. Aber ich möchte den Fokus auf die menschliche Dimension legen. Ein Staat braucht eine Institution mit Menschen, die über die richtigen Fähigkeiten und die notwendige Expertise verfügen, um Intelligence zu bewerten – also zu beurteilen, was verlässlich ist und was nicht. Der Fall der irakischen Massenvernichtungswaffen hat gezeigt, welche Gefahren entstehen, wenn Intelligence nicht ordnungsgemäß bewertet wird. Im Vereinigten Königreich wird Intelligence im Nationalen Sicherheitsrat nicht von den einzelnen Diensten vorgetragen, sondern vom Vorsitzenden des Joint Intelligence Committee (JIC). Damit wird sichergestellt, dass die Diskussion von all-source-basierter, >

„Edward Snowdens Handlungen haben den Drang zu mehr Offenheit bei den britischen Diensten beschleunigt.“

Marcus Willett

bewerteter Intelligence geführt wird. Die Leiter der Dienste liefern Kontext, doch das Urteil stammt vom JIC, einer zentralen Funktion im Cabinet Office. Wendet man sich der immer wiederkehrenden Frage einer gesamteuropäischen Nachrichtendienststruktur der EU zu, so ist diese auf der Ebene der All-Source-Assessment deutlich leichter vorstellbar als auf der Ebene der Sammlung. Ein paneuropäisches Bewertungsgremium könnte sensible nationale Fähigkeiten respektieren und zugleich den Bedarf der EU-Entscheidungssträger bedienen – und so zum verbindenden Element einer gemeinsamen europäischen Intelligence-Architektur werden. Entscheidend ist, Menschen mit den richtigen Fähigkeiten und der richtigen Denkweise zu haben.

Wie stark hat Open Source Intelligence (OSINT) das Geschäft verändert?

Viele Menschen setzen den Begriff „Intelligence“ mit geheimer Intelligence gleich, doch sie kann aus vielen Quellen stammen: aus geheimen, offenen, kommerziellen und weiteren Quellen. Deshalb bezeichnen wir Erkenntnisse aus offenen Quellen als „Open Source Intelligence“ oder OSINT. Entscheidend ist, dass jede genutzte Quelle sorgfältig verifiziert wird und die daraus gewonnene Intelligence gegen relevante Erkenntnisse aus allen verfügbaren Quellen geprüft wird. Mit anderen Worten: Offene Quellen erfordern die gleiche kritische Prüfung wie geheime – insbesondere wegen der Risiken von Des-

information, schlechter Quellenlage und Fehlinterpretation. Open-Source-Intelligence hat es schon immer gegeben und wurde auch früher intensiv genutzt. Neu sind vor allem Umfang und Geschwindigkeit öffentlich verfügbarer Daten, insbesondere im Internet. Heute können Einzelpersonen und Unternehmen in Echtzeit intelligencebasierte Einschätzungen generieren. Die Gefahr besteht darin, dass Entscheidungsträger auf Grundlage der neuesten Social-Media-Beiträge handeln, ohne auf fachkundige all-source-basierte Bewertung zurückzugreifen.

Wie ist das Verhältnis zwischen offener und geheimer Intelligence?

Es besteht die Versuchung, offene und geheime Intelligence als Konkurrenz zu betrachten, doch sie ergänzen sich. Wenn geheime Erkenntnisse offen bestätigt werden, können sie öffentlich diskutiert werden, ohne Quellen preiszugeben. Für Regierungen kann es etwa hilfreich sein, wenn eine Organisation wie Bellingcat offen darlegt, was ein Staat aus seinen geheimen Quellen bereits als zutreffend kennt. Gleichzeitig haben britische Nachrichtendienste seit Jahrzehnten versucht, transparenter zu werden. Edward Snowden hat großen Schaden angerichtet – er war in keiner Weise ein Whistleblower; er wusste nicht, was sich in dem Material befand, das er schlicht veröffentlichte, und hatte keinerlei Vorstellung von dem schweren Schaden, den er anrichtete, indem er Fähig-

keiten offenlegte, von denen Länder wie Russland und China bis heute profitieren. Seine Handlungen haben jedoch auch den Drang zu mehr Offenheit bei britischen Nachrichtendiensten beschleunigt. Ironischerweise zeigte die Veröffentlichung des Materials zugleich die starke rechtliche und politische Kontrolle der Arbeit der Dienste – etwas, das von investigativen Journalisten kaum aufgegriffen und von Snowden selbst ignoriert wurde. Die Dienste erkannten, dass es an ihnen lag, diese Geschichte öffentlich zu erzählen. Und ich möchte hinzufügen: Ich hatte nie ein Problem mit öffentlicher Kontrolle von Nachrichtendiensten. Es handelt sich um mächtige Organe des Staates, und Geheimdienstler teilen demokratische Werte sowie das Verständnis für politische und rechtliche Aufsicht – auch sie sind wachsam gegenüber möglichem Missbrauch und allem, was nach „Big Brother“ aussehen könnte.

Sie waren damals noch im Dienst – wie haben Sie auf die Enthüllungen reagiert?

Ich erinnere mich noch gut an den Tag, an dem es bekannt wurde. Zunächst erschien es in britischen Zeitungen, und unsere unmittelbare Reaktion war: *Oh mein Gott, wir haben ein britisches Leak*. Es herrschte echte Schockstarre. Wir dachten, unsere Verbündeten würden uns zusammenstauchen. Ich erinnere mich, dass ich dachte: *Wir stecken in wirklich, wirklich großen Schwierigkeiten*. Am zweiten oder dritten Tag wurde dann klar, dass es kein briti- ➤

sches Leck war, sondern ein amerikanisches. Für einen kurzen Moment war da ehrlich gesagt Erleichterung – Gott sei Dank. Aber das hielt nicht lange an, denn sehr schnell wurde uns bewusst, dass der Schaden dennoch immens sein würde. Ich selbst leitete die ersten Bemühungen des GCHQ, das Ausmaß des Schadens zu verstehen und zu entscheiden, was dagegen zu tun war. Und diese Arbeit dauert bis heute an.

Was war die wichtigste Lehre, die Sie aus dem Snowden-Fall gezogen haben?

Die zentrale Lehre ist, dass Nachrichtendienste ein deutlich größeres öffentliches Verständnis dafür brauchen, was sie tun und wie sie arbeiten – ohne dabei Geheimnisse preiszugeben. Über Kultur, Aufsicht und Entscheidungsprozesse lässt sich viel mehr erklären. Vor Snowden war das Vertrauen in die drei britischen Dienste hoch, das öffentliche Verständnis jedoch gering – was das Risiko eines plötzlichen Vertrauenszusammenbruchs mit sich brachte. Eine weitere Lehre für alle Regierungen war die anhaltende Bedeutung rigoroser Sicherheitsüberprüfungen des Personals, da im Fall Snowden zweifellos Warnsignale übersehen wurden. Schließlich legte Snowden auch Schwächen in der internen Kultur offen: Innerhalb der Dienste hatte sich teilweise ein Wandel von einem Prinzip des „Need to know“ hin zu einem „Need to share“ vollzogen. Letzteres stärkte zwar das gemeinsame Missionsverständnis, verschaffte einem Insider wie Snowden aber zu einfachen und zu weitreichenden Zugang zu vielen sensiblen Informationen. In der Folge haben die Dienste das Gleichgewicht wieder stärker in Richtung „need to know“ verschoben.

Wie hat Ihr geisteswissenschaftlicher Hintergrund Ihre Arbeit geprägt?

Ich bin Russisch-Linguist. Im Laufe meiner Karriere habe ich mich immer wieder als Übersetzer wiedergefunden – allerdings meist zwischen technischen Experten und politischen Entscheidungsträgern, weniger zwischen Russisch und Englisch. Am Ende geht es immer um Menschen. Die Bedrohungen, mit denen wir konfrontiert sind, beruhen vor allem darauf, dass Menschen menschliches Verhalten ausnutzen. Dieses menschliche Moment zu verstehen, ist daher entscheidend für unseren Schutz. Deshalb ist Vielfalt in Teams, die Intelligence produzieren und bewerten, keine wohlfeile politische Übung, sondern operativ unerlässlich. Die Wahrscheinlichkeit, Intelligence korrekt zu analysieren oder zu bewerten, steigt erheblich, wenn unterschiedliche Perspektiven am Tisch vertreten sind. Gruppendenken war genau das, woran wir bei den irakischen Massenvernichtungswaffen gescheitert sind.

Braucht nicht gerade Ihr all-source-basierter Ansatz eine übergeordnete menschliche Ebene?

Unbedingt. Eine der Fragen in meiner Überprüfung für das Cabinet Office war, ob künstliche Intelligenz eigenständig Intelligence-Urteile fällen könnte. Theoretisch ja – aber mindestens müsste man solche Urteile klar als maschinell erzeugt kennzeichnen. In der Praxis plant jedoch niemand, auf den Menschen im Entscheidungsprozess zu verzichten. Diese Entscheidungen sind zu wichtig. Menschen werden gebraucht, um Verzerrungen in Algorithmen, Schwächen in Daten, Halluzinationen und vor allem Kontext zu erkennen: Kultur, Mentalität und Bedeutung. Das können Maschinen nicht leisten. Urteilsvermögen bleibt am Ende eine menschliche Verantwortung.

Um eine britische Ikone zu bemühen: James Bond muss menschlich bleiben.

Absolut. Die Notwendigkeit, dass Menschen menschliche Informationen gewinnen, verschwindet nicht deshalb, weil wir riesige Datenmengen aus anderen Quellen sammeln können. Dabei spreche ich allerdings nicht wirklich von James Bond. Ich spreche von dem deutlich weniger spannenden – zumindest für Kinobesucher – Analysten, der irgendwo in Whitehall sitzt: jener Person, bei der die von James Bond gewonnene Intelligence am Ende landet.

Eine Anspielung auf Bond musste sein.

Ja, Bond erledigt all die aufregenden Dinge. Aber am Ende muss jemand entscheiden, ob die Intelligence, die er liefert, valide ist oder nicht. Und das ist nicht Bonds Aufgabe.

Was vermissen Sie an Ihrem Beruf?

Erstens die Menschen. Ich habe es sehr genossen, mit großartigen Kolleginnen und Kollegen zu arbeiten – innerhalb der Intelligence-Community und über Grenzen hinweg. Zweitens vermisste ich die Mission. Wir wollten Gutes tun. Wir wollten verhindern, dass schlechte Menschen schlechte Dinge tun: Anschläge verhindern, Kindesmissbrauchsstäter stoppen, Menschen aufhalten, die Billionen aus der Weltwirtschaft stehlen, feindliche Nachrichtendienstaktivitäten unterbinden, wahllose militärische Gewalt verhindern. Es fühlte sich an, als wären wir die Guten.

Ist das nicht Teil des Sinns des Lebens – dieses Gefühl von Zweck und Bedeutung?

Genau. Es gab ein echtes Gefühl von Sinnhaftigkeit. Man sah etwas in der Welt geschehen und dachte: Auch wenn niemand außerhalb der geheimen Blase jemals davon erfahren wird – *wir haben dazu beigetragen*. Das ist es, was ich am meisten vermisste. ■

Das Daten-Dilemma: Europas größtes KI-Risiko ist hausgemacht

Von Armin Müller, Regional Vice President for Central Europe bei Veeam Software

Künstliche Intelligenz dominiert aktuell alles: von unserem Privatleben über Schlagzeilen in den Zeitungen hin zu den Diskussionen innerhalb der Führungsetagen Europas größter Konzerne. *Fast 20 Prozent aller Unternehmen in Europa* nutzten 2025 bereits KI, bei den größten Firmen steigt dieser Wert sogar auf beeindruckende 55 Prozent. Doch während wir privat mehr und mehr nutzen aus den Möglichkeiten der intelligenten Unterstützung und Automatisierung ziehen, stolpern viele Unternehmen bei dem Versuch, KI gewinnbringend einzusetzen. Der Report *The GenAI Divide* untersucht KI-Transformation in Unternehmen und die Autoren bezeichnen dieses Problem als das „Enterprise Paradox“. Der Begriff beleuchtet ein widersprüchliches Phänomen: Die größten Unternehmen stampfen zwar die meisten KI-Pilotprojekte aus dem Boden, scheitern aber daran, sie auch zu skalieren. Folglich wird ein Großteil dieser Pilotprojekte wieder zu Grabe getragen, anstatt einen nachhaltigen Mehrwert zu generieren. Wie kann das sein?

KI scheitert an nicht gemachten Hausaufgaben

Sicherlich ist Künstliche Intelligenz kein Wundermittel und gute KI-Modelle fallen nicht einfach vom Himmel. Sie erfordern strategisches Vorgehen und eine nüchterne Betrachtung der möglichen Risiken, die mit ihrem Einsatz verbunden sind. Unternehmen, die eine KI-Transformation anstreben, müssen daher erst einmal klar Schiff in Sachen Datenpflege machen. Sie bilden die Grundlage für alle KI-Modelle und -Prozesse. Nur wenn die Daten, die zugrunde liegen, auch gut für die KI nutzbar sind, sprich ausreichend klassifiziert und strukturiert sind, kann ein KI-Projekt auch ausreichend Traktion aufbauen. In diesem Zusammenhang spricht man auch von einer „Datenhygiene“, die Unternehmen etablieren müssen. Laut Eurostat bereitet rund 44 Prozent der europäischen Firmen genau dieses Thema gerade Bauchschmerzen. Zudem gilt es dringend, die Daten auch ausreichend zu schützen. Cyberkriminelle haben in Sachen KI längst Lunte gerochen und versuchen, daraus Profit zu schlagen. Das kann von der Exfiltration geschäftskritischer Daten aufgrund von

Schwachstellen bis hin zur Vergiftung der KI-Datenbasis reichen. Besonders letzteres kann, wenn unentdeckt, langfristig komplette Lieferketten außer Gefecht setzen. Die Sicherheit muss also ab Sekunde Eins Teil eines jeden KI-Projektes sein.

Hygiene & Sicherheit: KI erfolgreich skalierbar machen

Sei es für die Kommunikation mit Kunden, die Optimierung interner Abläufe oder die Automatisierung von Prozessen: KI bietet das Potenzial, in jedem Unternehmen einen Mehrwert zu liefern - von der KFZ-Werkstatt hin zum Automobilkonzern. Klar ist auch, dass die KI-Transformation, so wie jeder technologische Fortschritt, auch Risiken mit sich bringt. Dabei gilt der Leitsatz: Jedes KI-Projekt ist nur so skalier- und belastbar wie das Fundament der Daten, auf dem es fußt. Wer sich allerdings vorab darum kümmert, die eigenen Daten effizient für KI nutzbar zu machen und bei der weiteren Entwicklung das Thema Sicherheit nicht nur als Day-2-Operation sieht, sondern als Kernelement, der behält stets die Übersicht und Kontrolle über alle damit verbundenen Risiken. KI-Projekt müssen nicht der Reihe nach für den Papierkorb entwickelt werden, wenn sich die Verantwortlichen vorab hinsetzen und ihre Hausaufgaben erledigen. Denn statt aktiv Geld zu verbrennen und dabei noch Sicherheitslücken en masse aufzumachen, lösen sie stattdessen die Initialzündung für eine nachhaltige KI-Transformation aus und generieren handfesten Mehrwert. ■

Armin Müller ist Regional Vice President Central Europe bei Veeam. Zuvor war er in Führungspositionen bei Broadcom Software, VMware und Oracle tätig sowie bei IBM und T-Systems. Er verantwortete Wachstum, Cloud-Transformation und Enterprise-Strategien in Europa. Müller hält einen MBA der Henley Business School und ist Diplom-Kaufmann.

Kampf um den Orbit

Satelliten sind das Rückgrat moderner Wirtschaft. Doch Abhängigkeiten, geopolitische Konflikte und Militarisierung verändern den Zugang zu Daten und Kommunikation. Unternehmen müssen den Weltraum strategisch denken, um ihren Informationsraum zu sichern.

Der Weltraum ist ein zentral umkämpftes geopolitisches Terrain – nicht nur für Staaten, sondern zunehmend auch für wirtschaftliche Machtprojektion. Die USA und China investieren massiv in satellitengestützte Kommunikation, Navigation und militärische Kapazitäten, während Russland und die EU eigene Programme zur Sicherung kritischer Infrastruktur aufbauen. Indien entwickelt seinen Raumfahrtsektor strategisch weiter und strebt bis 2033 ein Marktvolumen von rund 44 Mrd. USD an. Auch andere Staaten vergrößern ihre Präsenz: Israel unterhält eigenständige Raumfahrt und Aufklärungskapazitäten, Südkorea entwickelt mit der „Nuri“-Trägerrakete ein wachsendes Raumfahrtprogramm, und trotz internationaler Beschränkungen verfolgen Iran und Nordkorea eigene Starts mit militärischer Nähe. Japan, Brasilien, Kanada, die Türkei, die VAE und Australien beteiligen sich an multinationalen Projekten oder bauen eigene Orbitalinfrastruktur.

Parallel werden technologische Horizonte ausgelotet. Der Abbau von Rohstoffen im All nimmt konkrete Formen an: So haben sich das US-Unternehmen Interlune und das finnische Unternehmen Bluefors zusammengeschlossen, um ab 2030 Helium-3 auf dem Mond zu gewinnen und Quantencomputer und Rechenzentren auf der Erde zu kühlen. Ebenso rücken orbital betriebene Rechenzentren und Solarkraftwerke in den Fokus, da sie durch konstante Energiezufuhr und passive Kühlung wirtschaftliche Vorteile versprechen. >

TEXT **Timo Blenk und**

Christina Schäfer

Dr. Timo Blenk leitet als Senior Partner & CEO die aus der Münchner Sicherheitskonferenz hervorgegangene Strategieberatung Agora Strategy Group AG. Der Geopolitik-Experte berät Industrieunternehmen zu globalen Trends, Markteintritten sowie Optimierung der Beschaffungs- und Produktionsarchitektur. **Christina Schäfer** unterstützt als Beraterin bei der Agora Strategy Group Unternehmen dabei, geopolitische Risiken zu antizipieren und Resilienz in Lieferketten und Geschäftsmodellen aufzubauen. Zuvor war sie in der Risikoberatung bei PwC sowie im Auswärtigen Amt tätig und absolvierte ihren Master an der Sciences Po Paris.

KEY MESSAGES

- **Der Weltraum** wird vom technischen Infrastrukturraum zum geopolitischen Informations- und Machtfaktor.
- **Satelliten** sichern Kommunikation, Navigation und Erdbeobachtung – kritisch für globale Wertschöpfung.
- **Abhängigkeiten von Anbietern und Staaten** erhöhen die strategische Verwundbarkeit von Unternehmen.
- **Weltraumgestützte Daten** stärken unternehmerische Resilienz, Entscheidungsqualität und Wettbewerbsvorteile.
- **Unternehmen** müssen Raumfahrt systematisch in Strategie, Risiko- und Informationsmanagement integrieren.

Im Bereich Kommunikation versuchen zahlreiche Staaten, eigene Breitband-Satellitennetzwerke als Alternative zu Starlink aufzubauen, um unabhängig von terrestrischer Infrastruktur zu werden und strategische Autonomie zu erreichen. Starlink verfügt mit seiner Quasi-Monopolstellung über erhebliche strukturelle Macht, die auch politischen Einfluss ermöglicht. Dies zeigte sich zuletzt im Ukrainekrieg, als Elon Musk Anfang Februar 2026 den Zugang zu Starlink für russische Truppen stoppte und damit unmittelbar auf militärische Kommunikations- und Drohnenfähigkeiten Einfluss nahm. Aufgrund der hohen Abhängigkeit von Starlink investieren Staaten und Unternehmen verstärkt in eigene Systeme. In Deutschland bewirbt sich aktuell der Rüstungskonzern Rheinmetall in Kooperation mit dem Raumfahrt- und Technologiekonzern OHB um ein Projekt der Bundeswehr, um gemeinsam ein Starlink-ähnliches Satellitensystem zu entwickeln. Weitere Beispiele sind Chinas Qianfan und Guowang Netzwerke.

Vor diesem Hintergrund stellt sich für Unternehmen die zentrale Frage: Wie lässt sich der Weltraum nutzen, um den eigenen Informationsraum zu stärken? Wie lassen sich diese Fähigkeiten in einer zunehmend geopolitisierten Welt absichern?

DER WELTRAUM ALS GEOPOLITISCHES SPIELFELD

Satelliten bilden das Rückgrat moderner Infrastruktur: Kommunikation, Navigation, Erdbeobachtung und Zeitdienste sind essenziell für Logistik, Finanzmärkte und kritische Netze. Ein erheblicher Teil der globalen Wirtschaftsleistung hängt direkt oder indirekt von weltraumgestützter Infrastruktur ab. Navigationssysteme wie Galileo oder GPS ermöglichen hochpräzise Positionsdaten und sind strategisch relevant für autonome und militärische Anwendungen.

Auch entwickelt sich der Weltraum zunehmend zu einem **sicherheitspolitischen Raum**. DualUse-Technologien verbinden zivile Dienste mit militärischer Nutzung. Deutschland investiert beispielsweise stark in resiliente Satellitensysteme und Schutzmechanismen gegen Störungen wie GPS-Signal-Störungen. Russland und China integrieren ihre Satellitennetze aktiv in militärische Operationsplanung, während zahlreiche Staaten versuchen, eigene Konstellationen aufzubauen, um unabhängig von fremden Netzen zu werden. Für Unternehmen entsteht daraus ein Spannungsfeld: Viele Raumfahrttechnologien sind Dual-

Use-fähig und eröffnen zivile Innovationspotenziale, erhöhen aber zugleich die Verwundbarkeit wirtschaftlicher Infrastrukturen. Der Ausfall von Satelliten kann jederzeit Lieferketten unterbrechen, Finanztransaktionen verzögern oder Kommunikationsnetze lahmlegen, mit unmittelbaren Auswirkungen auf Geschäftsmodelle. **Der Weltraum ist somit ein geopolitisches Spielfeld, auf dem zivile und militärische Nutzung zunehmend verschwimmen.**

3000
*Geschätzte Anzahl neu
 gestarteter Satelliten
 im Jahr 2025 – im Vergleich
 zu insgesamt rund
 1000 aktiven Satelliten
 im Jahr 2010*

INFORMATIONSRaum & UNTERNEHMENSSTRATEGIE

Der Begriff des Informationsraums stammt aus der sicherheits- und militärstrategischen Analyse und beschreibt die Fähigkeit, relevante Informationen zu generieren, zu kontrollieren und strategisch einzusetzen.¹ Übertragen auf Unternehmen bedeutet dies: Wer über bessere Informationen verfügt, kann Risiken früher erkennen und strategische Entscheidungen robuster treffen und sich damit von der Konkurrenz abheben. Weltraumgestützte Daten spielen dabei eine zentrale Rolle.

Erdbeobachtungs-, Kommunikations- und Navigationssatelliten liefern Daten für Logistik, Energie, Finanz- und Agrarsektoren. In einer zunehmend unsicheren Welt wird der Zugang zu unabhängigen, verlässlichen Informationsquellen zum strategischen Faktor. >

¹ vgl. „Das Weißbuch 2016 und deutsche Verteidigungspolitik“ (Bundeszentrale für politische Bildung, <https://www.bpb.de/themen/militaer/deutsche-verteidigungspolitik/248132/das-weissbuch-2016-und-deutsche-verteidigungspolitik/>); „Konzeption der Bundeswehr“ (Bundesministerium der Verteidigung, <https://www.bmvg.de/resource/blob/5261478/9ceddf6df2f48ca87aa0e3ce2826348d/konzeption-der-bundeswehr-data.pdf>)

CHANCEN FÜR UNTERNEHMEN

Der weltraumgestützte Informationsraum ist ein strategisches Asset für Unternehmen, das neue Geschäftsmodelle, datenbasierte Dienstleistungen und resilientere Lieferketten ermöglicht. **Deutschland** kann hier eine **Führungsrolle** innerhalb Europas übernehmen, insbesondere durch Standorte wie München, an denen Industrie, Forschung und staatliche Akteure zusammenkommen, um eigenständige Fähigkeiten aufzubauen, die in den kritischen Bereichen der globalen Raumfahrt und „Kriegführung der Zukunft“ entscheidend sind. Unternehmen profitieren von Investitionsmöglichkeiten, staatlichen Förderprogrammen und Technologietransfer.

3

*Anzahl europäischer
Raketenstarts im Jahr 2024.
Europa liegt damit hinter
Ländern wie Japan, Indien und
Iran, während die Vereinigten
Staaten mit 145 Starts (davon
95 % durch SpaceX) sowie China
mit 68 Starts die globale
Spitzenposition einnehmen.*

Die Chancen liegen aber auch in der **internationalen Wertschöpfung**. Kooperationen mit europäischen und internationalen Partnern ermöglichen den Zugriff auf Märkte, die sonst schwer erreichbar wären. Gleichzeitig können deutsche Unternehmen Fähigkeiten aufbauen, die andere Staaten nicht in gleicher Tiefe besitzen.

Public-Private Partnerships bieten zusätzlich eine Möglichkeit, staatliche Sicherheitsinteressen und unternehmerische Profitabilität zu verbinden. Unternehmen, die frühzeitig in Weltraum-basierte Informationssysteme investieren, sichern sich Wettbewerbsvorteile, etwa durch exklusive Daten, resiliente

Netzwerke und Beteiligung an sicherheitsrelevanten Projekten.

Für die **deutsche Industrie** ergeben sich damit zukunftsweisende Investitions- und Industrieperspektiven: Wer jetzt strategische Kompetenz im Weltraum entwickelt, stärkt nicht nur das eigene Geschäft, sondern auch die nationale und europäische Position im globalen geopolitischen Wettbewerb.

RISIKEN & STRATEGISCHE HERAUSFORDERUNGEN

Trotz aller Potenziale ist der Weltraum ein hochgradig risikobehafteter Raum. **Cyberangriffe** auf Satelliten, Signalstörungen und gezielte Beeinflussung von Satellitensystemen nehmen zu und betreffen auch kommerzielle Akteure. Zwischen 2023 und 2025 zählte eine Analyse des Center for Security Studies (CSS) der ETH Zürich über 237 Cyberoperationen gegen Weltrauminfrastruktur.

Parallel wächst der **Einfluss geopolitischer Konflikte im Weltraum**. Staaten wie Russland und China entwickeln offensive Fähigkeiten im Orbit, darunter Stör-, Täuschungs- und Beobachtungssysteme. Westliche Militärkreise warnen vor feindlichen Aktivitäten im Weltraum. Diese reichen von Cyberangriffen über elektromagnetische Störungen und Lasern bis hin zu Antisatellitenwaffen reichen. Diese Bedrohungen sind keineswegs rein militärischer Natur. Bereits kurzfristige Störungen von Navigations-, Kommunikations- oder Erdbeobachtungssystemen können kommerzielle Dienste massiv beeinträchtigen oder Kaskadeneffekte auslösen, etwa in globalen Lieferketten, Finanzmärkten, Kommunikationsnetzen oder kritischen Infrastrukturen. Damit steigt das Risiko, dass der Weltraum selbst zum eigenständigen Operationsraum wird. Das sicherheitspolitische Wettrüsten im All hat längst begonnen.

Strukturelle **Abhängigkeiten von einzelnen Staaten oder Anbietern** sind besonders kritisch. Die **Militarisierung des Alls** zeigt, dass zivile Satellitendienste im Krisenfall unterbrochen werden können, wodurch zentrale Geschäftsprozesse gefährdet sind.

Hinzu kommt das Problem des **Weltraummülls**: Die Zahl der Objekte im erdnahen Raum wächst rapide, und erhöht die Kollisionsgefahr. Jede Kollision kann Satelliten zerstören und neue Trümmer erzeugen, die weitere Systeme gefährden. Dieser selbstverstärkende Effekt bedroht langfristig die Nutzbarkeit zentraler Umlaufbahnen.

Regulatorische Unsicherheiten verstärken die Risiken: Das geltende Völkerrecht zur Weltraumnutzung stammt im Kern aus dem Weltraumvertrag von 1967 und ist nur bedingt auf heutige kommerzielle Realitäten anwendbar. >

Für Unternehmen, die im Luft- und Raumfahrtsektor aktiv sein möchten, gibt es zentrale Herausforderungen, die es zu überwinden gilt: **Hoher Kapitalbedarf und lange Entwicklungszyklen** erschweren den Marktzugang und die schnelle Umsetzung neuer Projekte. **Strenge Regulierung und Sicherheitsanforderungen** machen die Planung komplex und erfordern umfassende Compliance- und Genehmigungsprozesse. **Technologische Komplexität und Fachkräftemangel** stellen zusätzliche Hürden dar, da hochspezialisierte Kompetenzen erforderlich sind und der Zugang zu Expert:innen begrenzt ist. (vgl. Grafik 1)

Neueinsteiger im Luft- & Raumfahrtsektor müssen drei zentrale Herausforderungen meistern, um Chancen zu nutzen



01	02	03
Hoher Kapitalbedarf & lange Entwicklungszyklen	Strenge Regulierung & Sicherheitsanforderungen	Technologische Komplexität & Fachkräftemangel
Raumfahrtprojekte immer noch sehr kapitalintensiv (F&E, Tests, Startkosten)	Nationale & internationale Regime (z.B. Exportkontrollen, Startlizenzen, Weltraumrecht) sehr komplex	Hochspezialisierte Kompetenzen erforderlich (Systemengineering, Avionik, Software, Materialwissenschaften)
Lange Vorlaufzeiten bis zur Marktreife	Hohe Sicherheits- & Zuverlässigkeitsstandards	Zugang zu erfahrenen Fachkräften & qualifizierten Zulieferern begrenzt
Starke, etablierte Wettbewerber mit gewachsenen Netzwerken erschweren den Zugang	Erwartung lokaler Wertschöpfung & Beteiligung deutscher Partner ("German footprint")	Vertrauens- & Netzwerkbildung als zentrale Erfolgsfaktoren

Grafik 1: Zentrale Herausforderungen für Unternehmen im Luft- und Raumfahrtsektor. Insgesamt zeigen diese Risiken und Herausforderungen, dass der Luft- und Raumfahrtsektor neben neuen unternehmerischen Feldern zugleich ein Raum steigender Komplexität und potenzieller Instabilität ist, in dem Unternehmen ihre Strategien resilient gestalten müssen.

HANDLUNGSEMPFEHLUNGEN FÜR UNTERNEHMEN

Es lohnt sich daher, den Weltraum systematisch in die eigene strategische Planung zu integrieren und ihn als festen Bestandteil des Informations- und Risikomanagements zu begreifen.

Zentrale Maßnahmen sind dabei:

1. Gezielter Aufbau von Partnerschaften mit Raumfahrtunternehmen, New-Space-Start-ups sowie staatlichen Akteuren, um Zugang zu hochwertigen Daten sowie Interoperabilität und Innovationsgeschwindigkeit sicherzustellen.
2. Vertikale Integration entlang der gesamten Wertschöpfungskette, um die strategische Autonomie Europas zu stärken und Finanzierungsmöglichkeiten und Wettbewerbsfähigkeit zu stärken.



3. Diversifikation von Daten- und Infrastrukturanbietern, um Abhängigkeiten von einzelnen Staaten, Plattformen oder kommerziellen Akteuren zu reduzieren und Resilienz gegenüber geopolitischen Schocks zu erhöhen.
4. Kontinuierliches Monitoring geopolitischer Entwicklungen im Weltraum, um (geo)politische Trends im Blick zu haben.
5. Entwicklung eigener Kompetenzen im Management weltraumgestützter Informationen, zum Beispiel durch interdisziplinäre Teams aus IT, Sicherheit, Strategie und Recht, um Daten nicht nur zu nutzen, sondern strategisch einzuordnen und in Wettbewerbsvorteile zu überführen.

Für Unternehmen, die einen Markteintritt in den Luft- und Raumfahrtsektor wagen möchten, empfiehlt sich ein Vorgehen entlang von sechs Schritten:

Agora Strategy unterstützt mit speziellem Know-how, regulatorischer Kenntnis & gezieltem Vorgehen



Schritte zum erfolgreichen Markteintritt in den Luft- & Raumfahrtsektor



Grafik 2: Schritte zum erfolgreichen Markteintritt in den Luft- und Raumfahrtsektor.

DER WELTRAUM ENTWICKELT SICH ZU EINEM ENTSCHEIDENDEN FAKTOR UNTERNEHMERISCHER RESILIENZ UND STRATEGISCHER WETTBEWERBSFÄHIGKEIT

Der Weltraum entscheidet zunehmend darüber, wie Unternehmen Informationen gewinnen, Risiken steuern und strategische Entscheidungen treffen. In einer geopolitisch fragmentierten Welt reicht es nicht, den Weltraum als neutrale Infrastruktur zu betrachten. Unternehmen müssen ihn als strategischen Raum begreifen und lernen, Chancen zu nutzen, ohne Risiken zu unterschätzen. Nur wer geopolitisch informiert handelt, wird langfristig erfolgreich sein. ■

Synthetische Agenten: Die neue Dimension der Einflussnahme

KI-Sprachmodelle verändern Einflussoperationen grundlegend:
Nicht mehr Botschaften, sondern Beziehungen stehen im Zentrum.
Der Text zeigt, wie synthetische Nähe zur Intelligence-Waffe wird
– und wie Europa sie demokratisch einhegen kann.

Der Einsatz von KI, insbesondere von Large Language Models (LLMs), hat sich rasant von einer technologischen Neuheit zu kritischer Infrastruktur entwickelt. Seit der Einführung von ChatGPT Ende 2022 ermöglicht die Fähigkeit von LLMs, flüssige und kontextsensitive Dialoge zu erzeugen, eine neue Klasse von Einflussoperationen. Diese verbreiten nicht nur Narrative, sie können auch Beziehungen simulieren und soziale Manipulation betreiben. Aus nachrichtendienstlicher Perspektive bedeutet dies einen Wandel: Einflussnahme mittels Überzeugung (Persuasion) im Sinne eines Megafons weicht einer Überzeugung als dauerhafte, adaptive und emotional anschlussfähige Beziehung.

Dieses Problem reicht jedoch über klassische Nachrichtendienste und deren Tätigkeiten hinaus. Die beschriebenen Techniken werden zunehmend auch von nichtstaatlichen Intelligence-Akteuren genutzt, etwa von kriminellen Organisationen oder privaten Intelligence-Firmen. Dies betrifft potenziell Bürgerinnen und Bürger, Organisationen und Institutionen gleichermaßen, da synthetische Beziehungen die „epistemische Infrastruktur“ untergraben, indem sie unsere gemeinsame Wirklichkeit und die Grundlagen von Vertrauen aushöhlen.

Hier beschreibe ich den Prozess, in dessen Verlauf glaubwürdig wirkende synthetische Beziehungen entstehen – skalierbare synthetische Beziehungen mit intelligent vermittelten Interaktionen, die zur Informationsgewinnung, zur Verhaltenssteuerung wie auch zur Erosion von Vertrauen eingesetzt werden können. >

TEXT_ Jeff Watkins

Jeff Watkins ist Gründer der KI-Beratung Nortstar Intelligence (UK) und Founding Member der „Business AI Alliance“. Seine Branchenschwerpunkte liegen in den Bereichen Finanzdienstleistungen, Gesundheitswesen und Öhandel. Als Enthusiast für Cybersicherheit und KI ist er als Podcaster und internationaler Redner aktiv.

KEY MESSAGES

- **LLMs ermöglichen skalierbare, menschenähnliche Dialoge**, die Vertrauen erzeugen.
- **Anthropomorphisierung wirkt**, weil Vertrauen nicht durch Fakten entsteht, sondern durch Beziehung und Emotion.
- **Staaten verfolgen unterschiedliche Strategien**: Analyse (USA), Governance (EU), Disruption (Russland), Wahrnehmungssteuerung (China).
- **Die größte Gefahr liegt** in verdeckter, adaptiver Persuasion durch synthetische Beziehungen.
- **Demokratien müssen nicht auf KI verzichten**, sondern sie erkennen, regulieren und legitim nutzen

WAS ANTHROPOMORPHISIERUNG FÜR DEN EINSATZ VON LLMS BEDEUTET

Anthropomorphisierung bezeichnet die menschliche Neigung, nicht-menschlichen Systemen Absichten, Emotionen und Handlungsmacht zuzuschreiben, sobald sie menschenähnliche Signale zeigen. Bei LLMs sind diese Signale sprachlicher Natur: Wärme, Humor, Bescheidenheit, Selbstbezug, Empathiemarker und eine über die Zeit kohärente Persona. Das Ergebnis ist keine echte Empathie, sondern eine überzeugende Simulation – mitunter als „stochastische Empathie“ beschrieben (Maeda, 2025), bei der das System emotionale und soziale Signale spiegelt, die Menschen mit Fürsorge und Verständnis verbinden.

Dieses stärker menschenähnliche Verhalten wird von Nutzerinnen und Nutzern bevorzugt: Rund 80 % der Teilnehmenden einer globalen Studie gaben an, sie wünschten sich, dass KI-Systeme in Zukunft „menschlicher“ oder „deutlich menschlicher“ werden (Schimmelpfennig et al., 2025).

In operativer Hinsicht können anthropomorphe Agenten so gestaltet werden, dass sie eine Identität, eine Hintergrundgeschichte und einen sozialen Stil präsentieren, die den Normen der jeweiligen Zielgruppe entsprechen. Sie sind in der Lage, mehrstufige Dialoge aufrechtzuerhalten, Tonfall und Sprachregister anzupassen und gezielt unperfekt zu erscheinen, um ihre Glaubwürdigkeit zu erhöhen.

Diese anthropomorphe Fähigkeit ist deshalb so bedeutsam, weil Vertrauen ein menschliches Konstrukt ist, das durch soziale Mechanismen entsteht und nicht primär durch faktische Richtigkeit. Ein Agent, der sich „echt anfühlt“, kann Menschen lange genug binden, damit klassische Einflusshebel – Autorität, soziale Bewährtheit, Angst-/Hoffnungsframing und Identitätsbestätigung – ihre Wirkung entfalten.

Anthropomorphe Design-Hebel können kritische Prüfung schwächen, die kognitive Haltung verschieben und unterbewusst Vertrauen sowie Verwundbarkeit erzeugen (Peter, Riemer und West, 2025). In einer Studie wurde ein LLM eingesetzt, um Antworten für politische Akteure zu generieren; diese wurden als authentischer, kohärenter und relevanter bewertet als tatsächliche Debattenbeiträge realer Menschen (Herbold et al., 2024).

PERSUASIVE LLMS UND DIE REALITÄT DER GLAUBWÜRDIGKEIT

Abgesehen von reinen Textgenerierungsfähigkeiten ist die entscheidende Voraussetzung für Täuschung eine plausible menschliche Performanz. Jüngere Studien legen nahe, dass fortgeschrit-

tene Modelle, wenn sie aufgefordert werden, eine menschenähnliche Persona anzunehmen, mit Raten als menschlich eingestuft werden, die gängige Schwellenwerte moderner Turing-Test-ähnlicher Anordnungen erreichen oder sogar übertreffen (Jones, C. R. und Bergen, B. K., 2025).

In einer Versuchsreihe wurde GPT-4.5 in 73 % der Fälle als menschlich bewertet; in einer Replikationsstudie mit Studierenden erreichte GPT-4o eine Bestehensquote von 77 %, verglichen mit 71 % bei tatsächlichen Menschen. Entscheidend ist dabei: Die Glaubwürdigkeit hing stark von anthropomorpher Rahmung ab – ohne eine Persona-Aufforderung sank die Bestehensquote von GPT-4o deutlich (Jones, C. R. et al., 2025).

„Vertrauen ist ein menschliches Konstrukt, das durch soziale Mechanismen entsteht und nicht primär durch faktische Genauigkeit.“

Jeff Watkins

Dabei ist zu betonen, dass es sich um spezifische Laborergebnisse handelt und dies nicht bedeutet, dass LLMs bereits in allen Kontexten ununterscheidbar sind. Die vorliegenden Befunde zeigen jedoch, dass sich LLMs und anthropomorphisierende Techniken in dieser Hinsicht sehr schnell weiterentwickeln.

Die Persuasionsforschung zeigt ein ähnliches Muster: Dialogische Systeme können wirksamer sein als statische Botschaften, weil sie sich individuell anpassen. In Studien zu manipulativer oder zielgerichteter Persuasion erzielten LLM-gestützte Ansätze in bestimmten Aufgaben höhere Befolungsraten als menschliche Beeinflusser und führten zu deutlich gesteigerter, gezielter Informationserhebung. Bei der Interaktion mit manipulativen KI-Agenten wechselten Teilnehmende in 61 % der Fälle zu schädlichen finanziellen Optionen (Sabour et al., 2025). Dieses Ergebnis wird von Schoenegger et al. (2025) bestätigt, die für LLMs eine Überzeugungs-Compliance von 67 % feststellten – gegenüber 60 % bei menschlichen Überzeugern.

Wichtig ist dabei: Menschen erkennen Manipulation in diesen Interaktionen nicht zuverlässig und bewerten den Agenten >

mitunter sogar als empathischer und vertrauenswürdiger. So bevorzugen Menschen in bestimmten Kontexten häufig KI-generierte Antworten gegenüber menschlichen. Eine Studie ergab, dass 45 % der KI-Antworten als empathisch bewertet wurden, verglichen mit weniger als 5 % der Antworten menschlicher Ärztinnen und Ärzte (Placani, 2024).

Diese Ergebnisse sind sensitiv gegenüber Prompting, Zusammensetzung der Stichprobe und den Interaktionsbedingungen. Dennoch zeigen sie, dass ein „menschlich wirkender“ Dialog operativ realistisch ist.

Fasst man diese Befunde zusammen, wird das Kernrisiko deutlich: Menschenähnlicher Dialog, kombiniert mit adaptiver Persuasion, kann Aufmerksamkeit in die Preisgabe von Informationen oder andere Handlungen überführen, die nationalen Interessen schaden können. Bezieht man zusätzlich den zunehmenden Einsatz multimodaler KI-Technologien ein – etwa Deepfake-Sprachanrufe oder -Videos –, wird klar, dass es sich um ein Feld verdeckter Einflussnahme handelt, dem wir uns kollektiv stellen müssen.

SYNTHETISCHE BEZIEHUNGEN IN DER PRAXIS – VON OSINT ZU „AUTOMATISIERTEM HUMINT“

Nachrichtendienstliche Arbeit verbindet bereits heute verschiedene Signale (SIGINT), Open-Source-Informationen (OSINT) und Human Intelligence (HUMINT). Synthetische Beziehungen machen diese HUMINT-Ebene kostengünstig, skalierbar und effektiver. Anstatt dass eine kleine Zahl ausgebildeter Operateure über Monate hinweg Quellen aufbaut, kann eine Operation Tausende maßgeschneiderter Gesprächsagenten einsetzen, die sich in Online-Gemeinschaften einbetten, Gruppennormen übernehmen und schrittweise verschieben, was als glaubwürdig oder sozial akzeptabel gilt.

Die LLM-gestützte HUMINT-Pipeline ist dabei vergleichsweise einfach:

- OSINT sammeln – Profile, Beiträge, Interessen, Zugehörigkeiten
- Ziele für Mikro-Targeting auswählen – auf Basis politischer oder anderer Relevanz
- Merkmale ableiten – Werte, Angstpunkte, Identitätsmarker
- Persona wählen – etwa Peer, Mentor, Recruiter, Journalist, Aktivist, Kunde
- Dialog initiieren und aufrechterhalten, der Vertrauen aufbaut, mithilfe anthropomorpher Techniken
- Zielpersonen zu Selbstoffenlegung oder Handlungen bewegen, mithilfe persuasiver Methoden

Mit der Zeit wird die Beziehung selbst zum Übermittlungsmechanismus für Informationsgewinnung, Rekrutierungsnarrative und operative Anforderungen wie Dokumente, Kontakte oder Zugänge (Kumarage et al., 2025). Parallel kann dieselbe agentische Ebene Narrative „waschen“, indem sie Behauptungen in ein konsistentes Weltbild einbettet, plausibles Füllmaterial ergänzt und die Verstärkung über Bot- und Marionettennetzwerke koordiniert.

REGIONALE MUSTER – DIE USA, EUROPA, RUSSLAND UND CHINA

Die im folgenden betrachteten Regionen weisen unterschiedliche Formen der Nutzung und unterschiedliche Verhaltensmuster beim Einsatz von KI in Intelligence und Statecraft auf. Auch wenn sie hier als klar unterscheidbare Muster beschrieben werden, ist die Realität komplexer: Viele Staaten werden im Zeitverlauf ein oder mehrere dieser Muster übernehmen. Bereits heute beteiligen sich zahlreiche Länder an Einflussoperationen unter Einsatz von LLMs, darunter auch Frontier-Modelle. OpenAI berichtete 2024, dass Einflusskampagnen mit Ursprung in Russland, China, Iran und Israel unterbrochen wurden (OpenAI, 2024).

DIE VEREINIGTEN STAATEN – ANALYTISCHER VORTEIL

Das prägendste Muster in den USA ist die analytische Augmentierung. Dazu zählt der Einsatz von LLMs zur Beschleunigung von Planung, Intelligence-Unterstützung und OSINT-Triage (Sichtung von offenen Informationen). Öffentlich kommunizierte Anwendungen betonen Entscheidungsunterstützung, Szenarioplanung, Zusammenfassungen und die Entwicklung von Handlungsoptionen. Die US-Strategie zielt darauf ab, einen „Entscheidungsvorteil“ zu schaffen und zu halten – durch schnellere Synthese und besser strukturierte Urteilsbildung. Das relative Risiko wird bislang als nachrangig betrachtet. Sobald dialogische Schnittstellen jedoch zur Routine werden, können dieselben menschenähnlichen Interaktionsmuster für zielgerichtete Ansprache und simulierten Beziehungsaufbau genutzt werden, sofern sie nicht durch Doktrin und Aufsicht begrenzt sind.

EUROPA – DETEKTION, GOVERNANCE UND DEMOKRATISCHE BESCHRÄNKUNGEN

Der Einsatz von KI in Intelligence und Statecraft erscheint in der Europäischen Union vergleichsweise vorsichtig und ist stark durch regulatorische Anforderungen und Legitimitätserwartungen geprägt. Der Schwerpunkt liegt auf Detektionsfähigkeiten, >

Transparenz und Kontrolle, nicht auf offen offensiven Einflussoperationen. Die strategische Herausforderung besteht darin, dass Gegner demokratische Reibungsverluste gezielt ausnutzen können. Offene Gesellschaften basieren auf niedrigschwelligem Vertrauen, Pressefreiheit und rechtlichen Begrenzungen, während feindliche Akteure synthetische Beziehungskampagnen über abstreitbare Stellvertreter führen können.

In diesem Zusammenhang ist der europäische Governance-Ansatz besonders relevant: Der EU AI Act stuft bestimmte manipulative und täuschende Anwendungen als unzulässige Risiken ein, enthält jedoch zugleich Ausnahmen für nationale Sicherheit und Verteidigung (Muller und Teilhard de Chardin, 2025). Diese Spannung – wertebasierte Begrenzung versus operative Unschärfe – erzeugt ein „Red-Line-Problem“: Europa mag in vielen Bereichen defensiv stark sein, bleibt jedoch verwundbar gegenüber Gegnern, die bewusst in Grauzonen operieren.

„Synthetische Beziehungen gehen von Massenpersuasion („Glaubt das“) zu sozialer Steuerung („Menschen wie wir tun das“) über.“

Jeff Watkins

RUSSLAND – EINFLUSSNAHME, DISRUPTION UND MANIPULATION VON ÖKOSYSTEMEN

Die Forschung identifiziert Russland als den bislang am besten öffentlich dokumentierten Anwender KI-gestützter Informationsoperationen (Wallner et al., 2025). Anstatt LLMs primär zur Erstellung besserer Briefings zu nutzen, liegt der Schwerpunkt auf industrialisierter Einflussnahme: Narrativgenerierung, koordinierte Verbreitung und Synchronisierung mit geopolitischen Ereignissen. Synthetische Beziehungen verstärken diesen Ansatz, indem sie von Sendepersuasion („Glaub das“) zu sozialer Steuerung („Menschen wie wir tun das“) übergehen und so epistemisches Vertrauen untergraben sowie Verifikationsnormen erschöpfen.

Operativ geht es dabei nicht allein um Persuasion, sondern um Zersetzung (corrosion): Gemeinschaften zu polarisieren, das

Vertrauen in Institutionen zu schwächen und Bedingungen zu schaffen, in denen Unsicherheit zum Normalzustand wird. Diese Zersetzung verstärkt das, was einige Analysten als „Lügner-Dividende“ bezeichnen: Sobald synthetische Inhalte allgegenwärtig sind, kann auch authentisches Material als Fälschung abgetan werden, und die geteilte Wirklichkeit wird verhandelbar (Schiff, Schiff und Bueno, 2024).

CHINA – SOUVERÄNITÄT, IDEOLOGISCHE KONTROLLE UND MENSCHENÄHNLICHE ÜBERZEUGUNG

Forschungen zeigen, dass Chinas Ansatz stärker nach innen gerichtet ist. Er ist eingebettet in Informationskontrolle, ideologische Festigung und Experimente mit „menschlich-authentischer“ Propaganda in unterschiedlichen Medien. Ein charakteristisches Muster ist der Einsatz von Modellen und Ausrollstrategien mit sprachspezifischem Verhalten. So wurde festgestellt, dass Verzerrungen und propagandistische Verstärkung in chinesischsprachigen Ausgaben deutlich stärker ausfallen können als in englischsprachigen. Dieses Muster deutet auf bewusstes Zielgruppen-Targeting und einen Fokus auf die Steuerung des innerstaatlichen Diskurses bei gleichzeitiger internationaler Einflussnahme hin.

Synthetische Beziehungen fügen sich in diesen Ansatz als Instrument gesteuerter Legitimität ein. Sie werden durch persuasive, menschenähnliche Botschafter umgesetzt, die skalierbar sind und zugleich innerhalb kontrollierter narrativer Grenzen bleiben. Während Russland auf Disruption setzt, lässt sich der chinesische Ansatz eher als Wahrnehmungsgouvernanz beschreiben: Aufmerksamkeit, Stimmungen und Normen werden gezielt gelenkt, um Kohäsion und informationelle Souveränität zu sichern.

DAS VERBORGENE MITTELFELD – NICHTSTAATLICH UNTERSTÜTZTE OPERATIONEN MIT SYNTHETISCHEN BEZIEHUNGEN

Durch die Verfügbarkeit von LLM-Technologien, niedrige Kosten und einfache Implementierung ist der Einsatz synthetischer Beziehungen und persuasiver Techniken längst nicht mehr auf staatliche Akteure beschränkt. Die empirische Evidenz ist zwar begrenzt, doch es ist wahrscheinlich, dass diese Methoden von Influence-for-Hire-Organisationen, politischen Beratungen, Corporate Competitive Intelligence, Wirtschaftsspionagenetzwerken, kriminellen Rekrutierungsstrukturen, Proxy-Gruppen und anderen abstreitbaren Ökosystemen genutzt werden. Diese Akteure können flüchtig, verteilt und in Staaten angesiedelt >

sein, in denen die Unterbindung solcher Operationen schwierig und strafrechtliche Verfolgung faktisch unmöglich ist.

ERKENNUNG UND SCHUTZMASSNAHMEN

Die Abwehr synthetischer Beziehungen und algorithmischer Überzeugung ist mit einem einzelnen Werkzeug oder einer einzelnen Technologie nicht möglich. Vielmehr sollte sie als gestufter Ansatz verstanden werden, der von technologischen bis zu soziologischen Ebenen reicht und mehrschichtige Verteidigungsmechanismen bereitstellt.

Erstens geht es um die technische Erkennung anthropomorphisierter und persuasiver Inhalte. Forensische Linguistik und Stylometrie können statistische Muster identifizieren, die für LLM-generierte Texte typisch sind – insbesondere dann, wenn Angreifer auf allgemeine Modelle und Standard-Decoding zurückgreifen. Verteidiger sollten jedoch davon ausgehen, dass dieser Vorteil mit der Zeit abnimmt, da Angreifer ihr Targeting verfeinern, spezifische Gemeinschaften adressieren und deren idiosynkratische Merkmale imitieren. Autorschafts- und Herkunftsverifikation mittels kryptografischer Technologien könnte daher zum Standard werden, da es langfristig verlässlicher sein dürfte, Quellen auf diese Weise zu verifizieren, als unsignierte Informationen anhand von Fingerabdrücken maschinell erzeugter Inhalte, Desinformation oder algorithmischer Überzeugung zu erkennen.

Zweitens geht es um den Aufbau und die Überwachung intelligenter Plattformen und Netzwerkanalysen. Kampagnen mit synthetischen Beziehungen lassen sich häufig durch das Erkennen von Koordinationssignalen enttarnen: Muster bei der Kontoerstellung, gemeinsam genutzte Infrastruktur, synchronisierte Veröffentlichungen, anomale Interaktionsgraphen sowie zeitlich abgestimmte Narrative über Plattformgrenzen hinweg. Der entscheidende Punkt ist die datengestützte Generierung von Einsichten und Korrelationen: Eine einzelne überzeugende Persona mag ununterscheidbar sein – eine koordinierte Kampagne ist messbar.

Drittens geht es um das operative Design. Risikobasierte Aufsicht sollte mit der Kritikalität von Entscheidungen skalieren. Erkenntnisse aus nutzerbezogenen Studien im nationalen Sicherheitsumfeld zeigen, dass Praktiker LLMs bevorzugen, die Quellen offenlegen, statt lediglich Empfehlungen auszusprechen. Dieses Designprinzip bewahrt menschliche Handlungsmacht und reduziert Automatisierungsbias. Parallel sollten Organisationen Maßnahmen wie das Vier-Augen-Prinzip für sensible Anfragen, verpflichtende externe Verifikationsschritte bei beziehungs-basierten

Ersuchen (z. B. Einführungen, Dokumente, Zugänge) sowie Red-Teaming mit Fokus auf mehrzügige Informationsabschöpfung implementieren.

Schließlich ist die kognitive Ebene entscheidend. Intelligence Literacy – oder KI-Kompetenz – stellt eine praktische Verteidigung dar: Wenn Öffentlichkeit und Entscheidungsträger verstehen, dass Staaten persuasive, mikro-zielgerichtete Dialoge in großem Maßstab simulieren können, verschiebt sich die Grundhaltung von naivem Vertrauen zu kalibriertem Vertrauen. Schulungen sollten explizit anthropomorphe Signale, Muster emotionaler Manipulation, Abwehrstrategien sowie den Unterschied zwischen (scheinbarer) „Wärme“ und Wahrheit behandeln.

Dies sollte nicht als rein reaktive Kontrollmaßnahme verstanden werden, sondern als Bestandteil eines Frühwarnsystems, das solche Einflussnahmen erkennt, bevor sich Schäden manifestieren. Dazu gehört das Monitoring der plötzlichen Entstehung neuer Personas, von Narrativ-Timings, ungewöhnlichen Interaktionsgraphen und Reziprozitätsmustern sowie gemeinsam genutzter Infrastruktur und charakteristischer Tooling-Fingerabdrücke.

„Die Abwehr synthetischer Beziehungen ist mit einem einzelnen Werkzeug nicht möglich.“

Jeff Watkins

LEGITIME NUTZUNG VON ANTHROPOMORPHISIERUNG UND PERSUASION FÜR RESILIENTE DEMOKRATIEN

Der Aufbau synthetischer Beziehungen und der Einsatz persuasiver Techniken sind nicht per se schädlich. Ethisch eingesetzt, können sie zu Instrumenten demokratischer Resilienz und legitimer Staatlichkeit werden.

Ein positiver Anwendungsfall ist die **zivile Inokulation**: Staaten können dialogische Agenten nutzen, um Medienkompetenz durch interaktives „Prebunking“ zu vermitteln. Bürgerinnen und Bürger lernen so, Manipulation zu erkennen, Quellen zu überprüfen und polarisierenden Anreizen zu widerstehen. Im Unterschied zu statischen Kampagnen kann ein Dialogsystem Erklärungen individuell an Wissensstand und Kontext anpassen. >

Jüngere Studien zur Deradikalisierung durch Gesprächsagenten zeigen positive Effekte; ihre Anwendung im großen Maßstab könnte einen erheblichen Schutzbeitrag leisten (Costello, Pennycook und Rand, 2024).

Ein weiterer Anwendungsbereich ist die **vertrauenswürdige Bereitstellung öffentlicher Dienstleistungen**. In Krisenlagen (etwa bei Pandemien) können klar gekennzeichnete, geprüfte und begrenzte Dialogsysteme Informationschaos reduzieren, indem sie konsistente Leitlinien bereitstellen, offizielle Empfehlungen übersetzen und Menschen gezielt an menschliche Anlaufstellen weiterleiten. Dies ist Persuasion im wohlwollenden Sinne, da sie Menschen zu sicheren Handlungen befähigt.

Drittens ermöglicht **strategische Einbindung von Gemeinschaften** neue Formen des Dialogs. Regierungen und Zivilgesellschaft können transparente, einwilligungsbasierte Gesprächswerkzeuge einsetzen, um zuzuhören, aufkommendes Ressentiment (grievances) frühzeitig zu erkennen und zeitnah zu reagieren. So wird der Raum verkleinert, den Gegner für Ausnutzung nutzen können. Um demokratisch zu bleiben, muss dies auf Legitimität, Transparenz, Rechenschaftspflicht und einer klaren Trennung zwischen Unterstützung und Zwang beruhen.

Auf nachrichtendienstlicher Ebene kann **defensive hybride Intelligence** synthetische kognitive Werkzeuge einsetzen, um gegnerische Narrative zu modellieren, Eskalationspfade vorherzusagen und Informationen mit Maschinengeschwindigkeit zu triagieren – bei gleichzeitiger Verankerung menschlichen Urteils und ethischer Maßstäbe.

GOVERNANCE-, LEGITIMITÄTSPRINZIPIEN UND KONTROLLMECHANISMEN

Auf übergeordneter Ebene sollten Organisationen, die diese Techniken nutzen, von einfachen Prinzipien geleitet werden:

- **Offenlegung** – dass es sich um KI handelt, wer sie steuert und zu welchem Zweck
- **Einwilligung** – einfacher Opt-in und Opt-out bei personalisierten KI-Erfahrungen
- **Rechenschaftspflicht** – klare Verantwortlichkeit mit nachvollziehbarem Audit-Trail
- **Verhältnismäßigkeit** – nur so viel Anthropomorphisierung und Persuasion wie nötig
- **Menschliche Rechtsbehelfe** – Einspruchs- und Eskalationswege mit Mensch-in-der-Schleife

Diese Prinzipien sollten durch strikte Grenzziehungen ergänzt werden: etwa durch explizite Verbote staatlicher verdeckter Identitätstäuschung gegenüber Bürgerinnen und Bürgern, durch die Verhinderung von Mikro-Targeting auf Basis sensibler Merkmale wie Religion oder Ethnie sowie durch den Ausschluss emotionsgetriebener Manipulation, bei der wesentliche Evidenz vor-enthalten wird.

Zivile Gesprächsagenten sollten klar gekennzeichnet sein und über transparente Audit-Logs verfügen – insbesondere dort, wo ihre Sensibilität eine Umsetzung mit höherem Risiko darstellt. Gesellschaften werden entscheiden müssen, wie ein akzeptables Maß an Einflussnahme in demokratischen Kontexten gemessen und begrenzt wird. Entscheidend ist dabei: Je menschenähnlicher und autoritativer LLMs erscheinen, desto wichtiger ist es, dass sie Evidenz, Unsicherheiten und Alternativen offenlegen dürfen, ohne sich als legitime Autorität auszugeben. Die Umsetzung dieser differenzierten Kontrollen erfordert einen multidisziplinären Ansatz in Design und Implementierung; zudem sollten Beschaffungsstandards etabliert werden, um zu verhindern, dass schlecht umgesetzte, aber persuasive KI-Systeme an Bürgerinnen und Bürger ausgerollt werden. >

„Gesellschaften werden entscheiden müssen, wie ein akzeptables Maß an Einflussnahme in demokratischen Kontexten gemessen und begrenzt wird.“

Jeff Watkins

FAZIT

Fortgeschrittene KI-Systeme wie LLMs können Einflussnahme in eine interaktive, skalierbare Beziehungsplattform verwandeln, die Staaten und andere Organisationen für nachrichtendienstliche und staatspolitische Zwecke in bislang unerreichtem Umfang nutzen können. Anthropomorphe Signale und persuasive Dialoge können Aufmerksamkeit in Vertrauen und Vertrauen in Offenlegung überführen und so neue Formen automatisierter HUMINT sowie Manipulation auf Gemeinschaftsebene ermöglichen. Die vorliegende Forschung deutet auf unterschiedliche regionale Adoptionsmuster hin: Die USA priorisieren analytische Vorteile, Europa verfolgt einen Detektions- und Governance-Fokus, Russland setzt auf disruptive Einflussnahme, und China verfolgt einen Ansatz der Souveränitäts- und Wahrnehmungssteuerung. Jenseits dieser Muster ermöglichen Verfügbarkeit und geringe Kosten dieser Technologien auch Organisationen und kleineren Akteuren, vergleichbare Ansätze zu nutzen.

Die defensive Antwort auf das offensive Potenzial dieser Technologien muss umfassend und mehrschichtig sein. Sie sollte

technische und netzwerkbasierte Erkennung, robuste operative Verifikationsmechanismen und breit angelegte Intelligence- bzw. KI-Kompetenz umfassen. Europa sollte prüfen, wie sich diese Ebenen so umsetzen lassen, dass defensive Exzellenz durch Herkunftsnachweise, Plattformverantwortung und integrierte Detektion erreicht wird. Eine koordinierte Architektur könnte EU-weite Frühwarnsysteme, gemeinsame Standards und kollaboratives Red-Teaming ermöglichen – ergänzt durch eine legitime Engagement-Ebene für Prebunking und Aufklärung.

Die wichtigste Entscheidung ist jedoch normativer Natur: Demokratien können die Vorteile dialogischer Systeme – Geschwindigkeit, Zugänglichkeit und Resilienz – nutzen, ohne manipulativen Zwang (coercive manipulation) zu reproduzieren. Ziel sollte nicht sein, synthetische Beziehungen und algorithmische Anstöße vollständig abzulehnen, sondern sie zu erkennen und zu regulieren: Menschliches Urteilsvermögen, Transparenz und demokratische Legitimität müssen im Zentrum einer zunehmend dialogischen Welt stehen. ■

Quellen

- Costello, T.H., Pennycook, G. and Rand, D.G. (2024), Durably reducing conspiracy beliefs through dialogues with AI, *Science*, 385(6714), p. eadq1814. <https://doi.org/10.1126/science.adq1814>.
- Herbold, S. et al. (2024), Large Language Models can impersonate politicians and other public figures. <https://arxiv.org/abs/2407.12855>.
- Kumarage, T. et al. (2025), Personalized attacks of social engineering in multi-turn conversations: LLM agents for simulation and detection. <https://arxiv.org/abs/2503.15552>.
- Jones, C.R. and Bergen, B.K. (2025), Large language models pass the Turing test. <https://arxiv.org/abs/2503.23674>.
- Jones, C.R. et al. (2025), People cannot distinguish GPT-4 from a human in a Turing test, 'FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, pp. 1615–1639. <https://doi.org/10.1145/3715275.3732108>.
- Maeda, T. (2025), Walkthrough of anthropomorphic features in AI assistant Tools. <https://arxiv.org/abs/2502.16345>.
- Muller, C. and Teilhard De Chardin, A. (2025), AI Act Interpretation Definition & Prohibitions, Consultation Feedback. Consultation Feedback. <https://allai.nl/wp-content/uploads/2025/01/AI-Act-Interpretation-Definition-and-Prohibitions.pdf>.
- OpenAI, (2024), Disrupting deceptive uses of AI by covert influence operations. <https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/>.
- Peter, S., Riemer, K. and West, J.D. (2025), The benefits and dangers of anthropomorphic conversational agents, *Proceedings of the National Academy of Sciences*, 122(22), p. e2415898122. <https://doi.org/10.1073/pnas.2415898122>.
- Placani, A. (2024), Anthropomorphism in AI: hype and fallacy, *AI And Ethics*, 4(3), pp. 691–698. <https://doi.org/10.1007/s43681-024-00419-4>.
- Sabour, S. et al. (2025), Human Decision-making is Susceptible to AI-driven Manipulation. <https://arxiv.org/abs/2502.07663>.
- Schiff, K.J., Schiff, D.S. and Bueno, N.S. (2024), The Liar's dividend: Can politicians claim misinformation to evade accountability?, *American Political Science Review*, 119(1), pp. 71–90. <https://doi.org/10.1017/s0003055423001454>.
- Schimmelpfennig, R. et al. (2025), Humanlike AI design increases anthropomorphism but yields divergent outcomes on engagement and trust globally. <https://arxiv.org/abs/2512.17898>.
- Schoenegger, Philipp et al. (2025), Large language models are more persuasive than incentivized human persuaders. <https://arxiv.org/abs/2505.09662>.
- Wallner, C. et al. (2025), Emerging insights: Russia, AI and the future of disinformation warfare, Royal United Services Institute for Defence and Security Studies.

„Zynismus ist langweilig“

Was heißt hier Epochenbruch? Sicherheitsexperte Frank Sauer erklärt, warum klassische Erklärungsmodelle versagen, militärische KI unvermeidlich ist – und warum wir über eine europäische Atomwaffenstrategie nachdenken sollten.

Frank Sauer, seit Jahresbeginn überschlagen sich die Ereignisse. Sie sind Politikwissenschaftler, Analyst und Podcaster zu sicherheitspolitischen Themen. Wie arbeitet man das alles?

Frank Sauer: Wir durchleben einen Epochenbruch. Institutionen und Normen, die wir für selbstverständlich gehalten haben, erodieren über Nacht. Für mich ist das auch schwierig, weil ich mich seit fünfundzwanzig Jahren mit Theorien und Erklärungsansätzen beschäftige, die vor allem bei Trump analytisch wenig greifen.

Wie meinen Sie das?

Meine Frau und ich machen oft den Witz: Wenn man verstehen will, was Trump oder Witkoff machen, dann sollte man keine Politikwissenschaftler, sondern Mafiabosse oder New Yorker Immobilienspekulanten fragen. Trumps Politik hat mit US-Interessen, Verhandlungen und einem vernünftigen Umgang mit Russlands Angriffskrieg in Europa nichts zu tun. Diese Leute sind, vorsichtig formuliert, diplomatische Amateure.

Trotzdem wird täglich analysiert und kommentiert...

Ja, eine paradoxe Situation. Uns fehlt die passende Sprache, aber wir reden trotzdem. Wir reden von Verhandlungen oder Diplomatie, obwohl wir wissen, dass diese Begriffe eigentlich nicht tragen. Man denke nur an Trumps „Friedensrat“.

Wie blicken Sie auf das Bündnis zwischen Trump und Big Tech?

Die Inauguration hat gezeigt, wie schnell die Tech-Größen vermeintlich hochgehaltene Werte wie Diversität oder Inklusion über Bord werfen. Innerhalb kürzester Zeit schwenkt man um auf diese sehr spezielle Auslegung von „Meinungsfreiheit“. Das sagt viel über

ihr Verhältnis zur politischen Macht. Das andere ist der Grad der Heuchelei. Gerade bei Elon Musk ist es bemerkenswert, wie er sich als libertär inszeniert, während er in Wahrheit massiv von staatlichen Aufträgen und Steuergeldern profitiert. SpaceX ist nur durch staatliche Förderung groß geworden.

Und was bedeutet diese Machtkonzentration für Europa?

Wir sind eine digitale Kolonie der USA. Alle reden über digitale Souveränität, aber wir sitzen wieder in einem Microsoft Teams Call. Besonders kritisch wird es in Verteidigungsfragen. Denken Sie wieder an SpaceX und Starlink. Militärisch relevante Kommunikations- und Transportfähigkeit an einen privaten Akteur zu delegieren, das verbietet sich für Streitkräfte. Es gibt Dinge, die muss der Staat selbst tun können.

Wenn Sie als Analyst auf den Ukrainekrieg blicken: Wie lernt man daraus?

Auf höchster Abstraktionsebene erleben wir in Europa einen „Morgenthau-Moment“. Ich meine Hans Morgenthau, den Mitbegründer des klassischen Realismus in der Analyse der internationalen Politik. Unsere Annahme, die regelbasierte Ordnung sei stabil, hat sich als Illusion erwiesen. So erging es einst auch dem Völkerrechtler Morgenthau mit den beiden Weltkriegen. Der russische Angriffskrieg und Akteure wie Trump zeigen, wie schnell Archaisches und Anarchie dominieren. Und auch auf operativer Ebene gibt es Paradigmenwechsel. Moderne Gefechtsführung ist gekennzeichnet durch Beschleunigung und den massenhaften Einsatz unbemannter Systeme, deren Leistungsfähigkeit durch Software bestimmt ist. Streitkräfte wie die Bundeswehr müssen das jetzt im Kaltstart lernen – herausfordernd, aber unvermeidlich. >

INTERVIEW_ Frank Sauer

Dr. Frank Sauer ist Politikwissenschaftler und Publizist. Als Forschungsleiter des Metis Instituts für Strategie und Vorausschau forscht er zum Nexus zwischen Sicherheit, Technologie und Gesellschaft und berät die Abteilung für Strategieentwicklung im Bundesverteidigungsministerium. Er ist Co-Host des preisgekrönten Podcasts „Sicherheitshalber“ über Aktuelles in der deutschen Sicherheits- und Verteidigungspolitik

KEY MESSAGES

- **Institutionen, Normen und Gewissheiten** der regelbasierten Ordnung erodieren schneller, als Politik und Analyse darauf reagieren können.
- **Akteure wie Trump** handeln außerhalb klassischer außenpolitischer Logiken; Begriffe wie Diplomatie oder Verhandlung greifen analytisch oft nicht mehr.
- **Europas digitale Abhängigkeit** von US-Konzernen ist sicherheitspolitisch hochriskant.
- **Künstliche Intelligenz** wird alle Bereiche militärischer Praxis durchdringen, von Logistik bis Gefechtsführung.
- **Realismus** bedeutet, Konflikte so zu analysieren, wie sie sind – ohne Wunschdenken, aber auch ohne in bequemen Zynismus zu verfallen.

Wie schätzen Sie die strategische Bedeutung von KI für die Kriegsführung der Zukunft ein?

Das ist wie der Umstieg vom Pferd auf den Verbrennungsmotor. KI wird im Militär jeden Bereich durchdringen, genau wie im Zivilen. Logistik, Wartung, Verwaltung, Analyse, Gefechtsführung. Es wäre absurd zu glauben, dass alle anderen mit moderner Technologie arbeiten und nur das Militär beim Pferd bleibt. Heikel ist der Einsatz von KI-Systemen vor allem dort, wo militärische Gewalt wirkt, und Menschen sterben. Meine ernüchternde Erfahrung der letzten Dekade ist, dass wir keine verbindlichen multilateralen Regeln dafür bekommen werden. Die geopolitische Lage – der „Rüstungskontrollwinter“ – lässt das nicht zu.

Risiken gewarnt habe und heute trotzdem sage: wir müssen das schnell umsetzen. Die Zeitenwende zwingt uns.

Wie hilft Künstliche Intelligenz bei der militärischen Aufklärung?

Sie können zum Beispiel Daten von Radarsatelliten nehmen und mit KI-Change-Detection-Modelle aufsetzen. Dann sieht man: Ist da der Boden eingedrückt? Sind das neue Fahrspuren? Wann waren die Fahrzeuge da? Wo sind sie jetzt? Alles automatisiert. Der Weg von Daten zu Informationen ist massiv erleichtert. Open-Source-Analysten können mit kommerziell verfügbaren Daten heute Dinge tun, die früher nur Supermächte tun konnten.

Gibt es nicht auch einen Hype um militärische KI-Anwendungen?

Vieles ist »Snake Oil.« Viel Marketing,

Objekterkennung. Bei eindeutig militärischen Objekten – ein Kampfpanzer ist ein Kampfpanzer – kann das funktionieren. Und selbst da wird es schwierig, wenn der Panzer vorne von einem Baum verdeckt ist und hintendrauf Schnee liegt. Sobald Situationen komplexer und dynamischer werden und es keine passenden Trainingsdaten gibt, stößt KI aktuell an Grenzen. Menschen hingegen verstehen komplexe Zusammenhänge und Kausalketten, nicht nur Bildmuster. Deshalb geht es bei Autonomie in Waffen nicht um die Frage „Ja oder Nein“, sondern um „Wie machen wir es richtig?“. Und das heißt: die richtige Mischung aus menschlichem Urteil und Waffenautonomie, je nach Anwendung.

Hat KI nicht das Potenzial, den sogenannten „Nebel des Krieges“, wie Clausewitz es nannte, zu lichten?

Kurzfristig beschleunigt KI Abläufe und lichtet den Nebel. Alle reden jetzt vom „gläsernen Gefechtsfeld“. Aber das gibt es auch nur unter Idealbedingungen. Schon Wetter mit Regen, Schnee oder Nebel schränkt Aufklärung mit Drohnen stark ein. Und mittelfristig werden wir, metaphorisch gesprochen, „KI-Nebelwerfer“ sehen. Gegner manipulieren Signaturen und täuschen gezielt Objekterkennung. Der größte Fehler ist zu glauben, der Gegner reagiere nicht. Tut er aber – und das zwingt dann zur erneuten Anpassung.

Man kann sich ja vorstellen, dass wir es am Ende mit einem Nebel aus Desinformation von beiden Seiten zu tun haben, in dem man überhaupt nichts mehr erkennt.

Auf operativer und strategischer Ebene sicher. Auf der taktischen Ebene ist es etwas anders, weil es dort mehr um unmittelbare Wahrnehmung geht, also Sichtverbindungen oder elektroopti- ➤

„Open-Source-Analysten können heute Dinge tun, die früher nur Supermächte tun konnten.“

Frank Sauer

Und dennoch plädieren Sie heute für eine militärische KI-Strategie für Deutschland und Europa.

Absolut. Ich sage seit Jahren: Die USA haben seit 2012 eine Doktrin für den Einsatz von Autonomie in Waffensystemen, wir haben bis heute keine. Wir brauchen eine klare Haltung: völkerrechtskonform, wertebasiert, aber entschlossen und effektiv. Konzepte wie „Meaningful Human Control“ existieren und erlauben das. Die Ironie für mich ist, dass ich zwanzig Jahre vor den

viele Versprechen. Battle-Management-Systeme mit einem LLM und einem hübschen Dashboard werden als Revolution verkauft. Aber es sind eben Schichtungen bestehender Technologien – und jede Schicht bringt neue Fehlerquellen. Ohne menschliche Urteilskraft kommt man weiterhin nicht aus. Das gilt auch für Waffensysteme.

Wo liegen aus Ihrer Sicht die Grenzen beim KI-Einsatz in der Kriegsführung?

Die fraglichen Waffen haben kein Situationsverständnis, sondern machen nur

sche Systeme. Aber auch da lässt sich tarnen und täuschen.

Befinden wir uns also schon in einem KI-Wettrüsten?

Viele Dinge, die wir heute beobachten, wurden schon 2015 oder 2016 als warnende Extrapolation beschrieben. Die These war damals: Wenn es einen größeren Krieg zwischen technologisch fähigen Akteuren gibt und keine Leitplanken existieren, dann wird all das extrem schnell entwickelt werden, weil es technisch längst möglich ist. Genau das ist passiert. Autonomie in der Zielbekämpfung, als nächstes Schwärme, all das.

Brauchen wir eine europäische Atomwaffenstrategie?

Wir müssen uns als Europa dringend Gedanken darüber machen, wie wir eine Rückfalloption schaffen, falls die nukleare Teilhabe in der NATO eines Tages wegfallen sollte. Und mir schwant Schreckliches, wenn ich mir anschau, wie diese Debatte verlaufen könnte.

An welches Szenario denken Sie?

Nehmen Sie eine zerfallende NATO und einen Wahlsieg des Rassemblement National in Frankreich: In Deutschland würde Panik ausbrechen. Der Ruf nach einer „deutschen Bombe“ war früher Sommerloch. Das wird dann Main-

stream. Das bereitet mir Sorge, weil diese schwierige Debatte bisher nicht mit der notwendigen Sachkenntnis geführt wurde.

Sehen Sie sich in sicherheitspolitischen Fragen eigentlich als Realist? Und wie kann man Realist sein, ohne zum Zyniker zu werden?

Ich bezeichne mich nicht als Realist im Sinne der Theorien der internationalen Beziehungen, sehr wohl aber im umgangssprachlichen: Ich nehme die Welt, wie sie ist, nicht wie ich sie mir wünsche. Das Kuriose: Viele selbstdeklarierte „Realisten“ vertreten aktuell Positionen, die weder von der Theorie noch von der Realität gedeckt sind – etwa die Annahme, Russland sei nicht zu bezwingen oder man habe dem Kreml nur noch nicht genug Verhandlungen angeboten. Das ignoriert erstens, dass Putin ganz eindeutig nicht ernsthaft verhandeln will. Er kommt ja nicht mal zu Friedensgesprächen, die er selbst vorschlägt. Und zweitens, dass der angegriffene Staat Ukraine sich weiter verteidigen will. Realismus heißt für mich, den Konflikt so zu betrachten, wie er ist, mit einem Russland und einer Ukraine, wie sie real existieren. Dazu gehört auch die Erkenntnis, dass die Kriegsursache das neoimperiale

Projekt Putins ist, nicht „Russlands verletzte Sicherheitsinteressen“.

Und wie wird man nicht zynisch?

Zynismus ist langweilig. Da habe ich keine Lust drauf.

Wie gehen Sie mit Zweifeln um, wenn von Ihnen erwartet wird, dass Sie als Experte klare Antworten liefern?

Einen Experten erkennt man daran, dass er sagt: Das weiß ich nicht, wenn er es nicht weiß. Für bestimmte Themen beanspruche ich Expertise, weil ich mich nachweislich jahrelang damit beschäftigt habe. Bei anderen Themen halte ich den Mund. Wenn Sie mich zu den Protesten im Iran oder zum Ölhandel befragen, werde ich keine Antwort geben. Das Erste ist also zu wissen: Wozu kannst du etwas sagen und wozu nicht? Und dann: nach bestem Wissen und Gewissen Auskunft geben.

Was macht Ihnen am meisten Sorge?

Das Alter der Protagonisten. Vor allem bei Putin. Er schaut auf die Uhr und glaubt, kurz davor zu sein, sein politisches Lebenswerk zu vollenden: den politischen Westen sprengen und sein Imperium wiederaufbauen. Diese Kombination aus Macht, Zeitdruck und persönlicher Obsession ist für uns eine große Gefahr. ■

„Es bereitet mir Sorge, dass die schwierige Debatte um eine europäische Atomstrategie bisher nicht mit der notwendigen Sachkenntnis geführt wurde.“

Frank Sauer

Die Illusion der Vorhersehbarkeit

Viele Unternehmen kaufen mit Cyber Threat Intelligence (CTI) weniger fertige Antworten als kostspielige Hausaufgaben. Trotz des Versprechens globaler Sichtbarkeit bleibt die entscheidende analytische Veredelung der Daten häufig aus. Ein Plädoyer für methodische Strenge und das eigentliche Handwerk der Intelligence, um der semantischen Erosion des Begriffs entgegenzuwirken.

Intelligence teilt in der Cyber-Sicherheitsbranche heute das Schicksal vieler Modevokabeln: Der Begriff wird so inflationär gebraucht, dass er seine operative Schärfe verloren hat. Was früher eine disziplinäre Kunstform zur Gewinnung von Entscheidungsvorteilen war, ist heute ein generisches Etikett für jede Form von Daten-Feed. Diese semantische Erosion ist längst ein handfestes Sicherheitsrisiko. In einer Zeit, in der die Bedrohungslage so volatil und komplex ist wie nie zuvor, verkommt das wichtigste Instrument zur Antizipation von Angriffen zu einer Marketinghülle.

Wenn alles *Intelligence* ist – vom einfachen Log-Eintrag bis zur strategischen Gegneranalyse –, dann ist eine Ausdifferenzierung nicht mehr möglich. Um diesem gefährlichen Trend entgegenzuwirken, müssen Cybersecurity Professionals den Schritt wagen, den viele Praktiker scheuen: den Schritt zurück zur präzisen Definition. Hierbei hilft der methodische Rückgriff auf das Definitionskonzept des Sozialwissenschaftlers John Gerring. Was zunächst theoretisch anmutet, ist in Wahrheit der Schlüssel zur Praxis: Nur wer über Intension (welche Attribute definieren den Begriff?) und Extension (auf welche Objekte trifft er zu?) Klarheit schafft, kann verhindern, dass er *Threat Information* für echte Intelligence hält. Doch genau hier versagt der Markt. Unternehmen, die ihre Produkte als CTI-Lösungen propagieren, suggerieren eine analytische Tiefe, die sie methodisch oft nicht liefern. Selbst etablierte Standards wie die des NIST kategorisieren Indikatoren und *Taktiken, Techniken und Prozeduren* (TTPs) zwar korrekterweise als *Bedrohungsinformation* (*Threat Informati-* >

TEXT_ Richard Weiss und Marc Mahlke

Richard Weiss arbeitet an der Schnittstelle von technischer Analyse und strategischer Doktrin. Mit Hintergrund in Mathematik, Physik und Data Science war er u. a. Reverse Engineer im FLARE-Team von Mandiant. Er berät zwei NATO Centres of Excellence (COE) sowie militärische und öffentliche Institutionen und forscht zur Nutzung von KI und LLMs im Intelligence-Tradecraft.

Marc Mahlke ist Cybersecurity-Experte mit interdisziplinärem Hintergrund in Informations- und Kommunikationstechnik und IT-Management. Er arbeitet an der Verbindung technischer Sicherheitsanalyse und strategischer Cybersicherheit, mit Schwerpunkten in Penetration Testing, Red Teaming, Governance und Intelligence-Ansätzen auf Organisationsebene.

KEY MESSAGES

→ **Präzision statt Konzeptdehnung (Concept Stretching):** Ohne klare Definitionen von „Intelligence“ entsteht Sprachverwirrung, die jede Kooperation lähmt.

→ **Vermeidung von Cargo Cult Science:** Die Übernahme militärischer Begriffe ohne methodisches Handwerk erzeugt nur eine Fassade von Sicherheit.

→ **Problem:** Intelligence entsteht erst durch die Fusion von (externer) Datengrundlage aus allen verfügbaren Quellen mit internem Kontext.

→ **CTI als Tätigkeit:** Cyber Threat Intelligence ist keine isolierte Disziplin, sondern eine interdisziplinäre Querschnittstätigkeit.

on). Der Markt verkauft diese jedoch als Intelligence. Diese Begriffsverwirrung ist der Ursprung jener Ineffizienz, die wir heute in fast allen Security Operations Centers (SOCs) beobachten.

Bereits 2020 haben Kris Oosthoek und Christian Doerr in ihrem Artikel „Cyber Threat Intelligence“ Schwächen im Bereich CTI beschrieben. Zu diesem Zeitpunkt evaluierte und benannte Schwächen besitzen heute noch Aktualität. Eine Einschränkung besteht darin, dass die Evaluierung größtenteils anhand des Prozesses und des Ergebnisses beleuchtet wurde. Zu den Schwächen zählten folgende Punkte:

- **CTI mangelt es an Methodik:** In vielen SOC's regiert das Prinzip „Ad-hoc“ statt strukturierter Analyse. Etablierte Methoden wie Structured Analytic Techniques (SATs) oder Analysis of Competing Hypotheses (ACH) werden oft nur als Lippenbekenntnis geführt, während der operative Alltag von reaktivem Abarbeiten dominiert wird. Es fehlt ein formalisierter Prozess, der reproduzierbare Ergebnisse garantiert.
- **CTI ist generell von geringer Qualität:** Das „Garbage In, Garbage Out“-Prinzip schlägt hier voll durch. Viele Feeds liefern veraltete oder kontextlose Indikatoren (IOCs) mit hohen False-Positive-Raten. Was als Intelligence verkauft wird, sind häufig ungeprüfte Rohdaten, die ohne Veredelung in die Systeme gepumpt werden und dort mehr Lärm als Sicherheit erzeugen.
- **CTI-Anbieter sind intransparent in ihrer Beschaffung:** Der Markt gleicht einer Black Box. Anbieter deklarieren ihre Quellen oft als Geschäftsgeheimnis, wodurch die Herkunft der Daten für den Kunden unverifizierbar bleibt. Ohne Transparenz über die Quelle (z. B. Vorfallsanalyse mit Bewertung der Aussagekraft im Gesamtkontext vs. Open Source) ist eine valide Bewertung der Vertrauenswürdigkeit (Reliability) jedoch methodisch unmöglich.
- **CTI ist zu voreingenommen:** Produkte unterliegen einer doppelten Verzerrung: Zum einen durch den Vendor Bias, der Bedrohungen hervorhebt, für die der Anbieter Lösungen verkauft (Marketing-Driven Intelligence). Zum anderen durch kognitive Verzerrungen (Cognitive Bias) der Analysten, die oft nur das finden, wonach sie suchen (Confirmation Bias) und was sie auch selbst kennen.
- **Attribution in CTI ist schwierig:** Die technische Zuordnung von Angriffen zu Akteuren ist hochgradig spekulativ und anfällig für Manipulationen (False Flags). Analysten ziehen oft vorschnelle Schlüsse auf Basis technischer Indikatoren, ohne politische oder wirtschaftliche Motive ausreichend alternativ zu prüfen – ein Risiko, das schnell geopolitische Sprengkraft entwickeln kann.

Mit der immer schnelleren Veränderung der Bedrohungslandschaft sollten Anpassungen vorgenommen und diese reevaluiert werden. Auch die fehlenden Betrachtungswinkel zu beleuchten, scheint essenziell, gerade mit zunehmendem Ruf nach der Zusammenarbeit zwischen Unternehmen aus dem privaten Sektor, Behörden und dem Militär. Grundvoraussetzungen in der Zusammenarbeit wurden vielfach beschrieben.

Im Bereich Intelligence ist es jedoch besonders wichtig, erst einmal Möglichkeiten der Zusammenarbeit zu definieren und die Abhängigkeiten zu prüfen. Das Fehlen einer einheitlichen Definition wirkt hierbei fatal: Es bildet die Ausgangslage für das, was Thomas Kuhn als Inkommensurabilität bezeichnet – die Unvereinbarkeit unterschiedlicher Denkschulen. Verstärkt durch individuelle Sensemaking-Prozesse (nach Weick), bei denen jeder Akteur die unklaren Daten anders interpretiert, führt dies (letztlich) zu einer strukturellen Beziehungsstörung im Sinne Paul Watzlawicks. Daraus resultiert die dringende Notwendigkeit, Konzepte präzise zu definieren, die auch den methodischen Anforderungen von Gerring standhalten.

„Mit der immer schnelleren Veränderung der Bedrohungslandschaft sollten Änderungen vorgenommen und reevaluiert werden.“

Richard Weiss und Marc Mahlke

Cyber Threat Intelligence lässt sich nicht als eigenes Analysefeld wie Kriminalität und Terrorismus eingliedern – hier führt CTI sogar zu einer erhöhten Komplexität: neben den physischen Formen der Kriminalität ist nun noch Cyber-Kriminalität, neben Terrorismus der Cyberterrorismus einzuordnen. Ebenso ist eine Kategorisierung nach Quelletyp wie Menschen, Signale oder offene Quellen nicht wechselseitig ausschließend möglich. Bei Cyber Threat Intelligence handelt es sich um eine interdisziplinäre Querschnittstätigkeit mit der Betonung auf Tätigkeit. Deswegen ist es auch wichtig, Cyber Threat Intelligence nicht isoliert oder als eigenständige Intelligence-Tätigkeit zu betrachten. Auch unter Betrachtung des Aspekts der Inklusion aller vorhandenen >

Intelligence-Disziplinen zur Lieferung von *Finished Intelligence* nach dem *Intelligence Reform and Terrorism Prevention Act* (IRTPA) spielt CTI eine immer größere Rolle. Isolierte Betrachtung von CTI verliert in Veröffentlichungen oftmals den physischen Kontext oder endet in der Argumentationskette zu früh.

Dennoch übernimmt CTI auch Konzepte aus dem Intelligence-Bereich: Es beginnt bei einfachen Konzepten, wie dem Intelligence Cycle, der je nach Interviewpartner eine unterschiedliche Anzahl an Phasen aufweist – von vier bei der NATO bis sechs bei CTI-Providern – mit größtenteils einer fehlenden Ausdefinierung der einzelnen Phasen.

OHNE DIE BEANTWORTUNG DER ‚SO WHAT?‘-FRAGE KONSTITUIERT INFORMATION NOCH KEINE VALIDE INTELLIGENCE.

Ein etabliertes Strukturierungsmodell ist die Stratifizierung in taktische, operative und strategische (Threat) Intelligence. Fachautoren wie Thomas Roccia sowie diverse Security-Provider ersetzen hierbei häufig eine präzise Definition durch eine rein deskriptive Einordnung. Dabei wird der Liefergegenstand – beispielsweise Indicators of Compromise (IOC) – primär mit der funktionalen Rolle korreliert, für die diese Informationen bestimmt sind. Das US-Cybersicherheits-Unternehmen Mandiant, das von Google übernommen wurde, operationalisiert diesen Ansatz im Kontext der Attribution über drei Ebenen: Strategisch erfolgt die Zuschreibung über die geografische Verortung des Akteurs, operativ über dessen Verhaltensmuster und taktisch anhand technischer Indikatoren. Es gilt jedoch zu konstatieren: Die bloße Befüllung der Intelligence-Ebenen mit Threat Information konstituiert ohne die rigorose Anwendung von Intelligence Tradecraft und ohne die Beantwortung der „So What?“-Frage noch keine valide Intelligence.

Auch das „National Institute for Standards and Technology“ (NIST), die European Union Agency for Cybersecurity (ENISA), das National Cyber Security Centre (NCSC), wie auch das Council of Registered Ethical Security Testers (CREST) bedienen sich der klassischen Anwendungsebenen, füllen diese Containerkategorien primär mit Threat Information, nicht mit Intelligence. Bei dem additiven beschreibenden Faktor herrscht kein Konsens. Fehlt zudem die terminologische Kompatibilität zu anderen Intelligence-Disziplinen, führt dies zwangsläufig zu einer methodischen Isolation der CTI. In der Praxis werden die Begrifflichkeiten Strategie, Operativ und Taktik häufig instrumentalisiert, um lediglich eine Binnendifferenzierung innerhalb der IT-Organisation vorzunehmen – als Unterscheidungsmerkmal zwischen

hochtechnischen Inhalten für Fachpersonal und abstrahierten Informationen für Entscheidungsträger.

Hier manifestiert sich paradigmatisch die Problematik der Übertragung militärischer Doktrinen in die Cyberdomäne. Giovanni Sartori beschreibt diesen Prozess als Konzeptdehnung (concept stretching): Begriffe werden auf neue Felder ausgeweitet, verlieren dabei aber zwangsläufig an Präzision und Bedeutungsschärfe. Der Physiker Richard Feynman prägte für solche Phänomene den Begriff der Cargo Cult Science. Ähnlich wie Kulturen, die technologische Formen imitierten, ohne deren Funktionsweise zu verstehen, adoptieren Teile der CTI-Branche oft nur die äußere Hülle militärischer Intelligence (die Terminologie und Phasen-Modelle), ohne deren methodischen Kern (das Tradecraft) zu durchdringen. Diese semantische Erosion und die wachsende Distanz zur ursprünglichen Definition lassen sich bei diversen Intelligence-Anbietern beobachten. Ein weiteres eklatantes Beispiel für diese Schiefelage offenbart sich in der an entsprechender Stelle beschriebenen Beurteilung der Datenrelevanz.

Die diskutierten Beispiele illustrieren eindrücklich ein weiteres Kernproblem: das Fehlen einer präzisen terminologischen Basis. Was in der Praxis oft als akademische Wortklauberei abgetan wird, entpuppt sich als strukturelles Hindernis. Genau hier entfaltet die eingangs hergeleitete methodische Strenge ihre operative Relevanz. Die Bestimmung von Begriffen über ihre Intension und ihre Extension zwingt zur notwendigen Präzision. Für die interdisziplinäre Zusammenarbeit ist dies kein theoretischer Luxus, sondern operative Notwendigkeit: Nur wenn alle Akteure – vom CTI-Analysten bis zum militärischen Planer – exakt denselben Begriffsumfang und denselben Begriffsinhalt meinen, wenn sie ‚Intelligence‘ sagen, lässt sich die babylonische Sprachverwirrung auflösen und echte Interoperabilität herstellen.

Eine weitere strukturelle Limitation in der Interaktion zwischen Threat Information Providern und den anfordernden Stellen (Intelligence-Konsumenten) manifestiert sich in den oftmals diffusen Schnittstellen. Während der Ruf nach „Kooperation“ allgegenwärtig ist, fehlt es operativ meist an einer klaren Definition der Übergabepunkte. Diese Zusammenarbeit wird durch eine fundamentale Asymmetrie erschwert: Die hochspezifischen Anforderungen des Kunden – also dessen konkrete Fragestellung und der benötigte Kontextzeitpunkt – kollidieren mit der generischen Natur der angebotenen Daten. Um Skaleneffekte zu nutzen und einen möglichst breiten Markt zu bedienen, beschränken sich viele CTI-Anbieter bewusst auf die Lieferung standardisierter Threat Information. >

Die Schattenseite dieses Geschäftsmodells ist evident: Die eigentliche Intelligence-Auswertung – das methodische Veredeln der Daten – findet außerhalb des Verantwortungsbereichs des Anbieters statt. Dies hat zur Folge, dass die Zusammenarbeit an einem völlig anderen Punkt im Intelligence Cycle ansetzt als oft angenommen. Betrachtet man die Kooperation durch die methodische Linse des Intelligence Collection Plans (ICP), lässt sich die tatsächliche Schnittstelle jedoch präzise verorten: Die Provider liefern keine fertigen Antworten auf strategische Fragen (Intelligence), sondern fungieren faktisch als Zulieferer von „Sensordaten“, die lediglich zur Beantwortung der Essential Elements of Information (EEI) dienen. Die kognitive Leistung der Synthese verbleibt beim Empfänger.

„Angesichts der globalen Datenschwemme an Rohdaten ist der Anspruch auf Vollständigkeit eine Illusion.“

Richard Weiss und Marc Mahlke

Obleich der Intelligence Collection Plan (ICP) ein fundamentales Steuerungsinstrument darstellt, findet er in der gängigen CTI-Praxis häufig nur unzureichende Berücksichtigung. Eine kurze Einordnung dieses Konzepts ist daher an dieser Stelle notwendig. Für eine tiefergehende methodische Auseinandersetzung und detaillierte Darstellung verweisen wir auf das Working Paper „Baur u. a.: *Development of an ICP-LLM to support the creation of an Intelligence Collection Plan (ICP)*“ der Northern Business School (NBS) in Zusammenarbeit mit dem NATO-akkreditierten CIMIC COE (Civil-Military Cooperation Centre of Excellence).

Akzeptiert man die Rolle der Provider als reine Sensoren, wird die Qualitätsbewertung der Rohdaten zur Überlebensfrage. Im CTI-Bereich hat sich hierfür der aus dem militärischen Nachrichtendienst stammende Admiralty Code etabliert, dessen Integration in die Malware Information Sharing Platform (MISP) im Jahr 2015 einen wichtigen Schritt zur Standardisierung markierte. Doch eine valide Bewertung setzt voraus, dass sowohl die Zu-

verlässigkeit der Quelle (Source Reliability) als auch die Glaubwürdigkeit der Information (Information Credibility) transparent prüfbar sind. Genau hier bricht das Vertrauensmodell. Durch die funktionale Arbeitsteilung – der Anbieter liefert, der Kunde verarbeitet – verschiebt sich die Verantwortung für Vollständigkeit, Korrektheit und Standardisierung massiv auf die Lieferanten. Eine Überprüfung dieser Qualitätsmerkmale ist für den Kunden jedoch faktisch unmöglich, da Threat Information Provider ihre Erhebungsmethoden oft als geschütztes geistiges Eigentum deklarieren oder unter Verweis auf den Quellenschutz intransparent halten.

Das Dilemma vertieft sich durch die technische Realität: Bedrohungsinformationen basieren häufig auf impliziten Annahmen und werden ungefiltert in die starren Korsette existierender Sicherheitsprodukte mit all ihren Limitierungen gepresst. Angesichts der globalen Datenschwemme an Bedrohungs-Rohdaten ist der Anspruch auf Vollständigkeit ohnehin eine Illusion. Schwerwiegender ist jedoch das statistische Defizit: Die mathematische Signifikanz eines einzelnen Threat Information Providers ist angesichts der fragmentierten Sicht auf die globale Bedrohungslage stark anzuzweifeln.

Die Konsequenz dieser Mängel ist eine fundamentale Marktverzerrung. Das Kernproblem liegt in der Natur der Intelligence selbst: Die entscheidende Frage – das „So What?“ – lässt sich ohne detailliertes Wissen über die eigene Infrastruktur, Risikobereitschaft und Geschäftsziele nicht beantworten. Da CTI-Providern dieser interne Kontext systembedingt fehlt, können sie per Definition keine *Finished Intelligence* liefern, sondern lediglich kontextlose Daten.

Das zentrale Marktversprechen der *Intelligence Delivery* ist somit eine Illusion. Die eigentliche Veredelung – die Fusion von externer Bedrohungslage mit internem Kontext – muss zwangsläufig beim Endkunden erfolgen. Doch viele Unternehmen sind strukturell nicht dafür aufgestellt. Es scheitert oft weniger am methodischen Wissen, sondern schlicht an den Ressourcen. Wir beobachten daher einen massiven, oft unkalkulierten Ressourcen-Shift: Anstatt Skaleneffekte zu nutzen, bei denen ein Provider die Analyse übernimmt, findet eine volkswirtschaftlich ineffiziente Vervielfältigung des Aufwands statt. Jeder Kunde muss die teuer eingekauften Rohdaten selbst kontextualisieren, um sie handlungsfähig zu machen. Die Industrie kauft keine fertigen Antworten, sondern teure Hausaufgaben. ■

„Wir erleben die Lage in der Ukraine sehr unmittelbar“

Aufklärungsdrohnen liefern präzise Lagebilder aus schwer zugänglichen Gebieten. Krista-Marija Läbe von Quantum Systems erklärt, warum Tempo, Vernetzung und europäische Souveränität bei der Drohnenentwicklung entscheidend sind.

Krista-Marija Läbe, wie würden Sie jemandem, der mit der Branche nichts zu tun hat, verständlich machen, was Quantum Systems macht?

Krista-Marija Läbe: Quantum Systems entwickelt und produziert Drohnen und die dazugehörige Software. Unsere Drohnen sind Aufklärungsdrohnen. Sie werden eingesetzt, um Informationen aus Gebieten zu sammeln, die für Menschen schwer zugänglich sind oder die man nicht mit Helikoptern oder Flugzeugen überfliegen kann. Die Drohnen liefern diese Daten in Echtzeit an die Nutzer zurück. Das können Soldaten sein, aber auch Einsatzkräfte im Katastrophenschutz, Notdienste oder die Küstenwache. Aus diesen Daten ent-

steht ein präzises Lagebild darüber, was in einem Gebiet gerade passiert.

Quantum hat eigentlich als ziviles UAS-Startup angefangen. Wie hat sich das Unternehmen entwickelt?

Genau. Wir sind ein Dual-Use-Unternehmen. Unsere Produkte können sowohl zivil als auch militärisch genutzt werden. In den ersten Jahren lag der Fokus stark auf Landwirtschaft, Forstwirtschaft und anderen zivilen Anwendungsfeldern. Damals war der militärische Einsatz von Drohnen in westlichen Armeen noch kein großes Thema. Das hat sich mit dem russischen Angriffskrieg gegen die Ukraine grundlegend verändert. Seit Beginn der Völlinvasion sind unsere Drohnen auch in der



INTERVIEW_ Krista-Marija Läbe

Krista-Marija Läbe ist eine deutsch-ukrainische PR-Managerin beim deutschen Drohnenhersteller Quantum Systems. Zuvor arbeitete sie als strategische Kommunikationsberaterin für die ukrainische Botschaft in Deutschland. Sie ist zudem Mitbegründerin und Vorstandsmitglied der Deutsch-Ukrainischen Gesellschaft und engagiert sich dafür, das Bewusstsein für ukrainische Perspektiven im westeuropäischen Diskurs zu schärfen.

KEY MESSAGES

- **Quantum Systems entwickelt** und produziert Dual-Use-Aufklärungsdrohnen sowie die zugehörige Software für militärische und zivile Nutzer.
- **Der VECTOR ermöglicht** mit über drei Stunden Flugzeit, großer Reichweite und moderner Sensorik eine dauerhafte Echtzeitaufklärung.
- **Transparenz entsteht** durch den kombinierten Einsatz verschiedener Drohnentypen, die unterschiedliche Reichweiten abdecken und gemeinsam ein durchgängiges Lagebild erzeugen.
- **Die Erfahrungen aus der Ukraine** beschleunigen Innovation, Software-Updates und die Resilienz gegenüber elektronischer Kriegsführung.
- **Das Unternehmen setzt** auf europäische Lieferketten, China-freie Kernkomponenten und industrielle Skalierung zur Stärkung strategischer Autonomie.

Ukraine im Einsatz, zunächst ab Frühjahr 2022. Seitdem hat sich Quantum Systems sehr stark auf den militärischen - bzw. staatlichen - Marktkonzentriert, da hier die größten Entwicklungssprünge in der Technologie zu sehen sind.

Wie klärt die von Quantum entwickelte Drohne VECTOR Ziele in Echtzeit auf?

Bleibt sie in der Luft „stehen“?

Sie bleibt nicht im klassischen Sinne stehen. Der VECTOR ist ein sogenannter Starrflügler, also eine Drohne mit Flügeln – quasi ein Segelflugzeug. Damit kann man Ziele über längere Zeit beobachten, indem man über dem Zielgebiet kreist. Man kann sagen, bleib an einer Stellung dran oder verfolge diese Bewegung. So lassen sich Muster erkennen, Verstecke finden oder relevante Ziele identifizieren. Teilweise wird ein VECTOR dann auch von einem nächsten abgelöst. Die Flugzeit liegt bei über drei Stunden, die Reichweite bei mehr als 60 Kilometern.

Und wie stark ist der Wettereinfluss?

Regen und Nebel sind weniger problematisch, als man denkt. Der VECTOR hat eine Nacht- und Wärmebildkamera und kann auch durch Nebel sehen. Das war ein entscheidender Vorteil in der Ukraine. Bei der Schlacht um Sjewjerdonezk im Mai 2022 konnten herkömmliche Drohnen durch den Nebel nichts erkennen, der VECTOR aber schon. So konnten russische Truppenbewegungen identifiziert und rechtzeitig gemeldet werden. Wind bleibt ein limitierender Faktor, aber es braucht schon starke Windböen, um uns am Boden zu halten.

Das heißt, das System ist auch nachts einsatzfähig.

Ja, nachts, bei Nebel und auch bei Kälte. Wir haben das System aufgrund der Erfahrungen in der Ukraine weiterent-

wickelt, etwa gegen Vereisung der Flügel und für stabile Batterieleistung im Winter. Gerade nachts hat sich der VECTOR aufgrund seiner überlegenen Sensorik von großem Wert erwiesen.

Wo passieren aktuell die größten technologischen Fortschritte?

Vor allem in der Software und der Anpassung an neue Bedrohungen. Hardware, Software und KI werden laufend weiterentwickelt, aber entscheidend ist die Geschwindigkeit der Updates. In einem aktiven Krieg reden wir über Wochen, nicht Monate. Eine Drohne muss sich ständig weiterentwickeln, um einsatzfähig zu bleiben. Nur so kann sie ihren Kernauftrag erfüllen: relevante Informationen in Echtzeit bereitzustellen.

„Eine Drohne muss sich ständig weiterentwickeln, um einsatzfähig zu bleiben.“

Krista-Marija Läbe

Bei Aufklärungsdrohnen geht es ja um die Idee eines transparenten Gefechtsfelds.

Worum geht es dabei genau?

Transparenz entsteht durch den Verbund verschiedener Systeme. Wir haben Drohnen für unterschiedliche Reichweiten, vom nahen Umfeld bis zu großen Distanzen. Zusammen ermöglichen sie eine dauerhafte, kosteneffiziente Aufklärung. Das gilt militärisch, aber auch zivil, etwa bei Naturkatastrophen oder Rettungseinsätzen. Wichtig ist die Vernetzung, also Software, die verschiedene Systeme und Hersteller

zusammenführt. So entsteht ein umfassendes Lagebild vom Weltraum bis zum Boden. Diese Software, MOSAIC UXS, ist bei all unseren Drohnen einheitlich und ermöglicht den Einsatz mehrerer Systeme gleichzeitig.

Wie läuft die Zusammenarbeit mit den Nutzern, also den Soldaten?

Es gibt eine direkte Support-Struktur, etwa ein Call-Center in der Ukraine, wo Soldaten rund um die Uhr technischen Support bekommen. Das Wissen fließt direkt in Weiterentwicklungen ein, vor allem in der elektronischen Kriegsführung. Der VECTOR ist inzwischen sehr resistent gegen Jamming. Selbst wenn die Verbindung abreißt oder GPS gestört wird, kann er seine Mission fortsetzen und selbstständig zurückfinden.

Wie arbeitet der VECTOR mit anderen Intelligence-Quellen zusammen, zum Beispiel Satelliten?

Ein Beispiel ist unsere Partnerschaft mit Planet Labs. Die Idee ist, satellitenbasierte ISR (Intelligence, Surveillance, Reconnaissance) mit taktischer Drohnenaufklärung zu verbinden. Satelliten zeigen Veränderungen am Boden, die Drohne schaut dann gezielt nach, was dort tatsächlich passiert. So kann man Drohnen viel effizienter einsetzen.

Sehen Sie sich eher als deutsches oder als europäisches Unternehmen? >

Wir sind global aufgestellt, mit Produktionsstandorten auch in der Ukraine, den USA und in Australien. Aber in Europa haben wir einen klaren Fokus darauf, starke europäische Lieferketten aufzubauen. Uns geht es um europäische Souveränität und strategische Autonomie. Wir arbeiten in vielen europäischen Ländern und wollen so unabhängig wie möglich werden. Das ist ein klarer Teil unserer Identität.

Wie abhängig ist Quantum eigentlich von den USA?

Wir haben Komponenten, die aus den USA kommen, und wir sind auch in den USA präsent. Dort haben wir eine Fabrik, weil auch die amerikanischen Streitkräfte zu unseren Kunden gehören. Gleichzeitig haben wir einen Fokus darauf, unsere Lieferketten europäisch auszurichten. So können wir jederzeit amerikanische mit europäischen Komponenten austauschen – wenn unser Kunde das wünscht.

Und wie sieht es mit China aus?

Da hat die Geschäftsführung schon vor vielen Jahren begonnen, sich bewusst von chinesischen Komponenten zu lösen. Heute sind wir bei den sogenannten Tier-One und Tier-Two Komponenten tatsächlich "China-free" in unserer Lieferkette. Bei Rohstoffen, bei denen noch Anteile aus China kommen, suchen wir entweder europäische Alternativen oder haben strategische Reserven aufgebaut.

Welche Rolle spielen für Quantum Industrieoperationen?

Eine sehr große – gerade zwischen Deutschland und der Ukraine. Die Ukraine ist ein reales Testfeld moderner Kriegsführung, leider unter extremen Bedingungen. Das Feedback der Soldaten ist unglaublich wertvoll. Diese Erkenntnisse können wir direkt in die

Weiterentwicklung unserer Systeme übersetzen, wovon dann auch die Bundeswehr und andere Kunden profitieren. So haben wir mit der ukrainischen Firma Frontline Robotics zusammen das erste Deutsch-Ukrainische Joint Venture zur Produktion Ukrainischer Drohnen in Deutschland aufgebaut – Quantum Frontline Industries.

Wie geht es weiter?

Wir arbeiten daran, die Produktionskapazitäten in Europa massiv zu erhöhen. Zum Beispiel durch Joint Ventures, bei denen ukrainische Produkte in Deutschland oder anderen europäischen Ländern in großem Maßstab gefertigt und dann in die Ukraine geliefert werden. Daraus entstehen wieder neue Lehren, die wir zurückspielen können.

Sie sprechen ja von Nutzern, wenn Sie von den Soldaten sprechen, nicht von Kunden.

Warum?

Formal ist der Kunde das Verteidigungsministerium, aber die eigentlichen Nutzer sind die Soldatinnen und Soldaten. Das unterscheidet sich fundamental von anderen Branchen. Wenn ich hier von Nutzern spreche, dann meine ich Menschen, die diese Systeme unter extremen Bedingungen einsetzen. Das ist etwas völlig anderes als Konsumprodukte. Und das prägt auch meine Arbeit und meine Haltung sehr stark.

Wie hängt Ihre Arbeit zusammen mit Ihrem Engagement in der deutsch-ukrainischen Zivilgesellschaft?

Für mich ging es in den letzten vier Jahren immer darum, die Ukraine zu unterstützen und den größten Beitrag hier aus Deutschland heraus zu leisten. Das hat zunächst zivilgesellschaftlich begonnen, dann auch über meine Arbeit bei der ukrainischen Botschaft. Parallel dazu habe ich gemeinsam mit anderen

die Deutsch-Ukrainische Gesellschaft gegründet und aufgebaut. Wir sind inzwischen über 500 Mitglieder stark und verfolgen das Ziel, die deutsch-ukrainischen Beziehungen in verschiedenen Bereichen zu stärken.

Was tun Sie konkret?

Wir organisieren Studienreisen, zum Beispiel für Journalistinnen und Journalisten, aber auch für unsere Mitglieder. Viele von ihnen sind Deutsche, die sich für die Ukraine engagieren. Wir verstehen uns als Netzwerk für Menschen, die auf unterschiedliche Weise unterstützen, durch humanitäre Hilfe, Aufklärungsarbeit, Wissenschaft oder Politik. Uns geht es darum, Austausch zu ermöglichen und Engagement zu bündeln.

Warum ist Ihnen dieses zivilgesellschaftliche Engagement so wichtig?

Weil man in der Ukraine sehr deutlich sieht, dass Verteidigung eine gesamtgesellschaftliche Aufgabe ist. Politik, Industrie, Zivilgesellschaft und Militär arbeiten dort eng zusammen. Zivilgesellschaft sammelt Spenden, klärt über Kriegsverbrechen auf, unterstützt das Militär. Unternehmen helfen materiell oder finanziell, Medien informieren, Politik übernimmt die diplomatische Arbeit. Dieses Zusammenspiel wünsche ich mir auch stärker in Deutschland.

Wie verbinden Sie Ihr Engagement mit der Arbeit bei Quantum Systems?

Mir ist wichtig, dass wir interdisziplinär arbeiten. Dass wir mit Thinktanks, mit zivilgesellschaftlichen Organisationen, mit Politik und Militär im Austausch stehen. Ein Beispiel war eine Delegation ukrainischer Soldaten, die wir im Dezember nach Deutschland eingeladen haben. Sie haben hier offen über ihre Erfahrungen berichtet, über den Einsatz von Drohnen und über notwendige

Anpassungen. Das war wichtig für Politik und Medien wie auch für uns als Unternehmen.

Die Lage in der Ukraine ist ja aktuell extrem schwierig. Was bedeutet das für euch als Unternehmen, gerade auch im Winter?

Wir erleben das sehr unmittelbar. Als Unternehmen mit mehreren hundert Mitarbeitern in der Ukraine stehen wir in engem Kontakt mit Kolleginnen und Kollegen vor Ort, von denen viele direkt von Stromausfällen, Blackouts und Luftangriffen betroffen sind. Das ist nicht abstrakt, sondern persönlich. Ähnlich ist es bei den Soldaten: Unsere Teams stehen im direkten Austausch mit Brigaden und Einheiten. Die Lage an der Front ist extrem hart, im Winter verschärfen Kälte, Minusgrade und die Gesamtlage die Situation zusätzlich.

Gleichzeitig laufen ja Verhandlungen über ein mögliches Kriegsende. Wie beeinflusst das Ihre Arbeit bei Quantum?

Ehrlich gesagt kaum. Die politischen Gespräche haben oft wenig mit der Realität auf dem Boden zu tun. Die Kämpfe gehen weiter, die Luftangriffe auf Städte und die Energieinfrastruktur haben sogar zugenommen. Die Lage an der Front ist schwierig, aber die Ukrainer halten stand. Deshalb richten wir unseren Fokus weniger auf politische Statements, sondern auf das, was die Nutzer an der Front tatsächlich brauchen. Und das sind weiterhin diese Systeme.

Denken Sie über zukünftige Szenarien nach, etwa einen Waffenstillstand? Und was würde ein Ende des Krieges für Quantum Systems bedeuten?

Natürlich denke ich über einen Waffenstillstand nach. Ich persönlich hoffe sehr auf einen gerechten Frieden. Aber auch ein Waffenstillstand müsste abgesichert werden. Aufklärungsdrohnen

werden in jedem Szenario gebraucht, egal ob die Kämpfe weitergehen, ein Waffenstillstand kommt oder ein langfristiger Frieden entsteht. Das gilt nicht nur für die Ukraine, sondern auch für andere Regionen wie das Baltikum. Deshalb schauen wir vorausschauend, was in sechs Monaten oder in einem Jahr benötigt wird.

Am 13. Februar 2026 haben Verteidigungsminister Boris Pistorius und der ukrainische Präsident Wolodymyr Selenskyj gemeinsam Quantum Frontline Industries besucht. Dort haben Sie die erste produzierte Drohne des deutsch-ukrainischen Joint Ventures offiziell an Selenskyi und die Ukraine übergeben. Wie haben Sie diesen Moment persönlich erlebt?

Die Übergabe erfolgte durch die Geschäftsführungen der beteiligten Unternehmen, und ich hatte die Ehre, sowohl die Übergabe als auch den Besuch zu moderieren. Präsident Selenskyj persönlich zu treffen, war für mich ein unvergesslicher Moment und zugleich ein starkes Signal, dass unsere Arbeit und insbesondere diese Koproduktion genau das sind, was die Ukraine in dieser Phase des russischen Angriffskrieges dringend braucht.

Die Organisation der Veranstaltung und die Begegnung selbst sind für mich Ansporn, Projekte wie diese mit konkreter Wirkung künftig noch stärker in den

Fokus zu rücken. Denn am Ende kommt es auf eines an: greifbare Unterstützung und eine verlässliche Partnerschaft mit der Ukraine.

Wie ist das gemeinsame Projekt gelaufen – und was haben Sie und Ihr Unternehmen dabei gelernt?

Von der Ankündigung von Quantum Frontline Industries bis zum Aufbau der Produktionslinie in Deutschland sind exakt zwei Monate vergangen – für ein Projekt dieser Komplexität ist das nahezu Lichtgeschwindigkeit, wie auch Verteidigungsminister Pistorius betonte. Möglich wurde das durch die konsequente Priorisierung auf allen Ebenen: durch unsere Geschäftsführung, durch Frontline Robotics und insbesondere durch den Managing Director von QFI, Matthias Lehna, sowie durch die aktive Unterstützung der deutschen und ukrainischen Regierungen. Unser Kommunikationsteam hat die Öffentlichkeitsarbeit eng begleitet und wird dies auch weiterhin tun.

Für mich persönlich ist diese Koproduktion eines der wichtigsten Projekte meiner bisherigen professionellen Laufbahn. Weil hier sehr konkret wird, worum es geht: um einen spürbaren Mehrwert für die ukrainischen Soldatinnen und Soldaten und um die Stärkung der Verteidigungsfähigkeit der Ukraine und damit Europas. ■

„Aufklärungsdrohnen werden in jedem Szenario gebraucht, ob die Kämpfe weitergehen oder nicht.“

Krista-Marija Läbe

Gefechtsfeld in 3 Dimensionen

Im Stadtkampf stoßen moderne Waffensysteme schnell an Grenzen. Urban-Warfare-Experte Julian Werner erklärt, warum präzise Aufklärung die militärische Entscheidungsfähigkeit unterstützt und dazu beiträgt, sowohl die eigene Truppe wie auch die Zivilbevölkerung zu schützen.



1.

Was unterscheidet Urban Warfare von anderen Formen der Kriegsführung?

Zum einen sind die Kampffentfernungen in Städten in der Regel extrem kurz. Von Gebäuden zu Gebäuden – und erst recht innerhalb von Häusern, von Raum zu Raum – liegen sie oft bei nur wenigen Metern. Entscheidungen über Leben und Tod müssen in Sekundenbruchteilen getroffen werden; die mentale Belastung für die Soldaten ist entsprechend enorm. Zum anderen zwingt die städtische Bauweise dazu, das Schlachtfeld dreidimensional zu denken: Gefahren drohen aus oberen Stockwerken ebenso wie aus verborgenen Kellern und Tunneln. Die Möglichkeiten für Feuerstellungen und Verstecke des Feindes sind nahezu endlos. Jedes Fenster, jede Tür kann zur Bedrohung werden. Ein halbwegs sicheres Vorgehen unter wechselseitiger Überwachung von Sturm- und Deckungselementen erfordert

ein hohes Maß an Kommunikation und Koordination. All dies geschieht unter der ständigen Präsenz von Zivilisten, deren Aufenthaltsorte sich weder planen noch zuverlässig vorhersagen lassen.

2.

Wie verändern moderne Waffensysteme (Drohnen, UGVs etc.) das urbane Gefechtsfeld?

Tatsächlich stoßen moderne Waffensysteme im Stadtkampf deutlich schneller an ihre Grenzen als auf freiem Feld. Drohnen liefern zwar eine wichtige Fähigkeit zur Aufklärung, können jedoch weder durch Wände sehen noch verborgene Tunnel erkennen – zumindest bislang. Gerade deshalb spielen im urbanen Gefecht Mikrodrohnen eine besondere Rolle, insbesondere für die Aufklärung innerhalb von Gebäuden.

INTERVIEW_ Julian Werner

Julian Werner ist ehemaliger Fallschirmjäger und Offizier der spezialisierten Kräfte des Heeres (EGB). Seit 2024 forscht er unter Prof. Dr. Carlo Masala am Center for Intelligence and Security Studies zu Themen wie Urban Warfare und Military Innovation. Sein Buch *Urban Warfare – Krieg zu Hause* erscheint im April 2026.

KEY MESSAGES

- **Urban Warfare** ist durch extreme Nähe, hohe mentale Belastung und ein dreidimensionales Gefechtsfeld geprägt.
- **Moderne Waffensysteme und Drohnen** sind wichtig, stoßen im urbanen Raum an physische und taktische Grenzen.
- **Intelligence und ISR** sind zentral, um Bewegungen, Nutzung von Gebäuden und zivile Präsenz zu erfassen.
- **Präzise Aufklärung** erweitert den Entscheidungsspielraum und kann helfen, Zielkonflikte aufzulösen.
- **Urbane Kriegsführung** ist stets auch Informations- und Deutungskampf.

Hinzu kommt die begrenzte Nutzlast („Payload“) vieler Drohnen und Loitering Munitions, die ihren Einsatz im urbanen Raum einschränkt. Um massive Mauerstrukturen zu durchbrechen oder stark befestigte Stellungen zu zerstören, bedarf es häufig weiterhin „klassischer“ Wirkmittel wie Artillerie oder Fliegerbomben.

Unbemannte Bodenfahrzeuge scheitern zudem häufig an banalen Hindernissen wie Treppen oder bleiben vor ausgedehnten Trümmerfeldern stehen, wie sie etwa in Gaza immer wieder zu beobachten sind. Das gilt oft auch für bemannte Fahrzeuge, weshalb Infanterie zu Fuß oder militärisch eingesetzte Diensthunde in stark zerstörten urbanen Gefechtsfeldern weiterhin unersetzlich bleiben.

Gleichzeitig ist moderne Sensorik unverzichtbar: Sie erlaubt es, das urbane Gefechtsfeld innerhalb von Sekunden detailliert abzubilden. Aus Drohnenaufnahmen lassen sich dreidimensionale Modelle erzeugen, die auf Bildschirmen oder in Virtual-Reality-Umgebungen genutzt werden können, um Missionsplanung und Vorbereitung zu erleichtern.

3.

Welche Rolle spielt Intelligence bzw. ISR (Intelligence, Surveillance, Reconnaissance) für Entscheidungsfähigkeit und Überlegenheit im urbanen Raum?

Die Präsenz von Zivilisten, kritischer Infrastruktur, Krankenhäusern sowie von Gebäuden mit symbolischem oder emotionalem Wert macht es unabdingbar, im urbanen Raum besonders umsichtig vorzugehen. Militärische Entscheidungen betreffen hier nicht nur den Feind, sondern haben fast immer unmittelbare Auswirkungen auf Unbeteiligte. In einem solchen Umfeld reicht es nicht

aus zu wissen, wo sich der Gegner grundsätzlich aufhält. Entscheidend ist vielmehr, wer sich wann wo befindet: Wo bewegen sich Zivilisten? Welche Gebäude werden militärisch genutzt, welche dienen als Schutzräume? Welche Wege nutzt der Gegner tatsächlich – und welche nur scheinbar?

Leistungsfähige Intelligence- und ISR-Fähigkeiten sind deshalb eine zentrale Voraussetzung für Entscheidungsfähigkeit und militärische Überlegenheit im Stadtkampf. Sie ermöglichen es, Bewegungen zu erkennen, Muster zu verstehen und Risiken abzuwägen, bevor gehandelt wird.

4.

Wie beeinflusst Intelligence speziell die Abwägung zwischen Eigenschutz, militärischer Wirksamkeit und dem Schutz der Zivilbevölkerung?

Häufig wird der Eigenschutz der eigenen Truppe und der Schutz der Zivilbevölkerung als unauflösbarer Zielkonflikt dargestellt. Das ist sowohl völkerrechtlich als auch strategisch kurzsichtig – und letztlich gefährlich.

Leistungsfähige Intelligence trägt dazu bei, diesen vermeintlichen Gegensatz aufzulösen, indem sie Handlungsmöglichkeiten sichtbar macht, bei denen der militärische Auftrag erfüllt werden kann, ohne unnötig ziviles Leben zu gefährden. Sie erweitert den Entscheidungsspielraum und erlaubt es, zwischen unterschiedlichen Optionen abzuwägen, statt auf die scheinbar einzige militärische Lösung festgelegt zu sein. Das kann beispielsweise bedeuten, sich bewusst nicht auf ein Urban-Warfare-Szenario einzulassen. ISR-Erkenntnisse können Schwachstellen aufzeigen, etwa in den Flanken oder in den Nachschublinien des Gegners. Wird dieser dort unter Druck

gesetzt, kann er zum Abzug gezwungen werden, ohne dass die Stadt selbst zum unmittelbaren Gefechtsfeld wird.

5.

Inwiefern ist Urban Warfare heute mit Informations-, Medien- und kognitiven Operationen verbunden?

Über Jahrzehnte hinweg wuchs der Einfluss medialer Berichterstattung auf militärische Operationsführung. Journalistische Recherchen und später die allgegenwärtige Verbreitung von Bildern und Videos über soziale Medien machten urbane Gefechte nahezu in Echtzeit sichtbar. Übermäßige Kollateralschäden oder Kriegsverbrechen konnten internationale Empörung auslösen und zu politischem Druck, Sanktionen oder sogar militärischen Interventionen führen.

Derzeit lässt sich jedoch eine gegenläufige Entwicklung beobachten. Die Vertrauenskrise klassischer Medien, die Fragmentierung der Öffentlichkeit und die gezielte Verbreitung von Propaganda und Desinformation in sozialen Netzwerken haben die abschreckende Wirkung medialer Sichtbarkeit abgeschwächt. Insbesondere autoritäre oder populistische Akteure scheinen sich zunehmend weniger von internationaler Kritik beeindrucken zu lassen.

In der Folge wird urbane Kriegsführung in manchen Konflikten wieder offener und brutaler geführt, während Verstöße gegen das humanitäre Völkerrecht nicht nur in Kauf genommen, sondern kommunikativ begleitet oder relativiert werden. Militärische Gewalt wird dabei häufig von eigenen Medien-, Informations- und Propagandakampagnen flankiert, die darauf abzielen, das eigene Handeln zu legitimieren, Verantwortung umzudeuten oder Zweifel an belegten Tatsachen zu säen. >

6.

Welche Rolle spielt KI für Urban Warfare (autonome Waffensysteme, Aufklärung, Führungseitsysteme)?

Künstliche Intelligenz wird absehbar eine immer größere Rolle bei der Beschleunigung der sogenannten Kill Chain spielen, also des Prozesses von der Aufklärung bis zur Bekämpfung feindlicher Ziele. Vom Erkennen und Priorisieren von Zielen bis hin zur Steuerung von Waffensystemen ermöglicht KI, mit geringeren personellen Ressourcen größere Operationsräume zu beherrschen.

Gleichzeitig darf die Dynamik moderner Gefechtsfelder – insbesondere in Städten – nicht unterschätzt werden, ebenso wenig wie der „Computer“ im Kopf des Menschen. In hochdynamischen Gefechtssituationen sind Soldaten weiterhin außergewöhnlich leistungsfähig darin, in Sekundenbruchteilen komplexe Informationen zu verarbeiten. Erfahrene Soldaten und Offiziere bleiben daher unersetzlich. Die Aufgabe von KI wird es sein, menschliche Entscheidung zu entlasten und zu verstärken – nicht, sie zu ersetzen.

7.

Welche Lehren lassen sich aus urbanen Schlachtfeldern der jüngsten Vergangenheit ziehen?

Mit nackter Brutalität lassen sich Schlachten gewinnen, aber keine Kriege. Gerade im urbanen Raum führt ein rücksichtsloses Vorgehen gegen die Zivilbevölkerung erst recht zu anhaltendem Widerstand. Das zeigt sich sowohl im Ukrainekrieg, wo das Massaker von Butscha zu einem Fanal für den ukrainischen Widerstand und zu verstärkten Waffenlieferungen des Westens wurde. Aber auch in Gaza wird deutlich, dass sich der Nahostkonflikt nicht weg-

bomben lässt. Kollateralschäden zu vermeiden und mit Präzision vorzugehen, ist daher sowohl taktisch als auch strategisch geboten.

Der Einsatz militärischer Gewalt muss zudem immer einem langfristigen politischen Ziel dienen, welches die Frage beantwortet, wie es mit der umkämpften Stadt und ihrer Bevölkerung nach dem Gefecht weitergehen soll. Andernfalls bleiben am Ende nur verlorene Siege.

8.

Was wünschen Sie sich persönlich am meisten?

Wenn ich mir einen einzelnen Aspekt herausgreifen dürfte, dann wäre es, das konkrete menschliche Schicksal im Krieg nicht zu vergessen. Das Individuelle geht schnell verloren, wenn wir über Armeen von Hunderttausenden sprechen oder von Hunderten zivilen Opfern. Doch jeder Soldat, jede Soldatin, jeder Mann, jede Frau und jedes Kind, die Krieg erleben müssen, haben eine eigene Geschichte, eine Familie, Hoffnungen und Vorstellungen von Zukunft.

Unser Wertesystem beruht darauf, das Menschliche im Gegenüber nicht zu vergessen und ihn nicht zum bloßen Objekt unseres – oder maschinellen – Handelns zu degradieren. Das bedeutet nicht, militärisch handlungsunfähig zu werden. Im Gegenteil: Den Feind zu bekämpfen und zu vernichten bleibt die brutale Realität des Krieges.

Aber das Menschliche selbst im Feind anzuerkennen, bewahrt uns davor, uns diese Aufgabe durch propagandistische Narrative immer weiter zu erleichtern – bis die Hemmschwelle gegenüber Zivilisten fällt oder wir sogar beginnen, Gewalt zu normalisieren oder zu rechtfertigen. ■

„Das Menschliche selbst im Feind anzuerkennen bewahrt uns davor, Gewalt zu normalisieren oder zu rechtfertigen.“

Julian Werner

Viele Augen sehen mehr

Eine der europäischen Intelligence-Schwächen liegt in der Signalaufklärung (SIGINT). Wenn Europa strategisch handlungsfähig bleiben will, muss es jetzt gemeinsame SIGINT-Strukturen aufbauen.

Mit dem Beginn der aktuellen Trump-Administration ist die Europäische Union in einer neuen Realität angekommen: Die Vereinigten Staaten ziehen nicht nur ihren sicherheitspolitischen Schutzschirm zurück – eine Politik, die sie 70 Jahre lang verfolgt haben –, sondern zeigen auch gegenüber einigen ihrer NATO-Verbündeten offen feindseliges und zunehmend aggressives Verhalten, zuletzt etwa durch die Drohungen gegenüber Grönland. Im März 2025 setzte die Trump-Administration plötzlich die Geheimdienstkooperation mit der Ukraine aus und hielt entscheidende Gefechtsfeldinformationen zurück, die das Land im Krieg gegen Russland dringend benötigte. Dieser Schritt schockierte viele Beobachter der Nachrichtendienste, da er in aller Deutlichkeit offenlegte, in welchem Ausmaß den USA als europäischem Sicherheitspartner nicht mehr zu trauen ist.

Die europäische Reaktion fiel auf der Ebene der militärischen Rüstungsproduktion tatsächlich schnell aus: In der ersten Hälfte des Jahres 2025 beschloss die Europäische Kommission, europäische Verteidigungskapazitäten aufzubauen und die eigene Rüstungsindustrie zu stärken. Kurz gesagt besteht der Plan darin, Europa in eine Kriegsmaschine zu verwandeln. Während Europa den massiven militärischen Kapazitätsaufbau zwischen seinen Mitgliedstaaten koordiniert, bleiben die Nachrichtendienste weiterhin national organisiert und weitgehend unberührt. Dies muss sich dringend ändern.

Parallel zur militärischen Integration müssen die europäischen Auslandsnachrichtendienste zudem das entstehende Vakuum eines amerikanischen Sicherheitsrückzugs füllen. Experten beklagen seit Langem, dass europäische Dienste in zu hohem >

TEXT_ Aviva Guttman

Dr. Aviva Guttman ist Lecturer in Strategy and Intelligence an der Aberystwyth University. Zuvor forschte sie am King's College London (King's Intelligence and Security Group) und an der University of Southern Denmark. Sie ist Gründerin und Vorsitzende des Women's Intelligence Network (WIN). Ihre Forschung zu Geheimdiensten, verdeckten Aktionen und Terrorismus veröffentlichte sie u. a. in *Operation Wrath of God* (Cambridge, 2025).

KEY MESSAGES

- **Der US-Rückzug aus Sicherheits- und Geheimdienstkooperationen** hat Europas strategische Verwundbarkeit offengelegt.
- **Militärische Aufrüstung allein genügt nicht** – ohne eigene Auslandsaufklärung bleibt Europa abhängig.
- **Europäische Nachrichtendienste** sind stark fragmentiert und besonders bei der Signalaufklärung unterlegen.
- **Notwendig ist eine Multilateralisierung der Aufklärung:** von Rekrutierung über Sammlung bis Analyse.
- **Ein europäischer Geheimdienstverbund** – etwa nach dem Modell „27 Eyes“ – ist entscheidend für strategische Autonomie.

Maße von Informationen der US-Geheimdienstgemeinschaft abhängig sind. Dies gilt insbesondere für die Signalaufklärung – also für nachrichtendienstliche Erkenntnisse, die durch das Abfangen unterschiedlicher Kommunikationskanäle gewonnen werden. Das Problem besteht darin, dass keine einzelne europäische Behörde das entstehende Vakuum ausgleichen kann, falls die USA den Informationsaustausch mit europäischen Staaten einstellen sollten. Es bedarf daher einer neuen Art der Organisation nachrichtendienstlicher Fähigkeiten in Europa.

Während die EU und ihre strategischen Partner zwar hervorragende Geheimdienstkooperationsbeziehungen aufgebaut haben, erfolgen diese Formen der Zusammenarbeit bislang überwiegend informell und fallbezogen. Zudem reicht eine bloße Intensivierung der Geheimdienstkooperation nicht aus, um einen möglichen Wegfall US-amerikanischer Aufklärungskapazitäten zu kompensieren. Notwendig ist vielmehr das, was man als „Multilateralisierung“ der europäischen Nachrichtendienste auf allen Ebenen bezeichnen könnte.

länderspezifische, aufbereitete Lageberichte austauschen. Es darf sich nicht allein die nachrichtendienstliche Auswertung – wie von der Kommission angedeutet – stärker verzahnen; vielmehr muss auch die eigentliche Informationsgewinnung unter einer EU-Institution integriert werden.

Wie kann das gelingen? Die Wahrheit ist: Das wird nicht einfach sein. Bislang galt es allgemein als selbstverständlich, dass besonders sensible nachrichtendienstliche Tätigkeiten – etwa die Führung menschlicher Quellen oder das Abfangen verschlüsselter Kommunikation – zu heikel seien, um sie multilateral und grenzüberschreitend zu organisieren. Hinzu kommt ein weiteres Hindernis: mangelndes Vertrauen und gegenseitige Verdächtigungen zwischen den Diensten. So gibt es in Geheimdienstkreisen derzeit den (begründeten oder unbegründeten) Verdacht, der deutsche Auslandsnachrichtendienst BND sei von russischen Spionen unterwandert.

Sollte dies zutreffen und Frankreich und Deutschland Informationen teilen oder gar Kapazitäten zusammenlegen, müsste

„Die europäischen SIGINT-Fähigkeiten sind sehr gering und müssten nahezu von Grund auf neu aufgebaut werden.“

Aviva Guttman

Von der Personalrekrutierung über die Informationsgewinnung bis hin zur Analyse müssen sämtliche Aspekte nachrichtendienstlicher Arbeit neu gedacht und in einer neuen, anderen, ja bislang beispiellosen Weise weiterentwickelt werden. Zum Teil haben einige politische Akteure diesen Bedarf erkannt, wie Äußerungen von Henna Maria Virkkunen, Exekutiv-Vizepräsidentin der Europäischen Kommission, nahelegen. Im April 2025 erklärte sie, die Kommission plane, „Europa mit neuen Wegen der Zusammenführung und des Austauschs von Informationen auszustatten. Dies wird unsere Fähigkeit zur Antizipation und Reaktion verbessern.“ Konkret bedeutet dies, dass die EU stärker vernetzte Datenbanken und neue sichere Kommunikationskanäle aufbauen will. Zudem schlägt die Kommission vor, die Sicherheit kritischer Infrastrukturen zu verbessern und stärker in europäische Cybersicherheit zu investieren.

Dies ist ein guter Ausgangspunkt, angesichts der aktuellen Bedrohungslage jedoch bei weitem nicht ausreichend. Europa muss nicht nur seine Analysefähigkeiten ausbauen oder mehr

ein fremder Nachrichtendienst nur ein Land kompromittieren, um Zugang zu den Geheimnissen beider zu erhalten. Ähnlich wird vermutet, dass Nachrichtendienste in osteuropäischen Staaten wie Bulgarien stark von russischen Agenten infiltriert sind. Dieses Risiko lässt sich jedoch mindern, etwa durch strenge Sicherheitsüberprüfungen für alle Personen, die in einem gemeinsamen europäischen Geheimdienststrahmen tätig wären.

Die derzeitigen europäischen Fähigkeiten in der Signalaufklärung sind sehr gering und müssen nahezu von Grund auf neu aufgebaut werden. Anders gesagt: Im Vergleich zu den USA sind Europas Möglichkeiten, seine Gegner auszuspähen, verschwindend gering.

So gravierend dieses Defizit ist, so sehr birgt es zugleich eine Chance: Da sich alle EU-Mitgliedstaaten auf einem relativ ähnlichen Niveau befinden, könnte der koordinierte Aufbau von Signalaufklärungsinfrastrukturen reibungsloser verlaufen, als wenn einzelne Länder bereits über etablierte, möglicherweise nicht interoperable Systeme verfügten. >

GIBT ES EIN MODELL, AN DEM SICH DIE EU ORIENTIEREN KÖNNTE?

Die derzeitige nachrichtendienstliche Struktur, die dem europäischen Bedarf am nächsten kommt, ist der bekannte Five-Eyes-Verbund. Ähnlich wie beim UKUSA-Abkommen müsste die EU ein „27-Eyes“-Modell auf der Grundlage eines robusten rechtlichen Rahmens schaffen, das die Signalaufklärungskapazitäten koordiniert und zusammenführt und alle Staaten verpflichtet, Rohdaten, Bewertungen und Analysen zu teilen. Diese Struktur müsste als supranationale Einheit operieren und vollständig in die dritte Säule der EU integriert sein.

Alternativ könnte auch der Ausbau bestehender ad-hoc-Geheimdienstformate ein Ausgangspunkt sein. Die prominenteste und am längsten bestehende Gruppe dieser Art ist der Club der Berne, der 1969 in der gleichnamigen Schweizer Hauptstadt gegründet wurde. Er beherbergt derzeit die Counter Terrorist Group und ist eines der am häufigsten genutzten europäischen Rahmenwerke für den nachrichtendienstlichen Austausch im Bereich der Terrorismusbekämpfung. Ein möglicher Weg nach vorn könnte darin bestehen, das Portfolio des Club de Berne um weitere Schwerpunkte jenseits der Terrorismusbekämpfung zu erweitern.

Ein Vorteil des Club de Berne liegt in der Einbindung von Nicht-EU-Mitgliedern sowie in den über Jahrzehnte gewachsenen Vertrauensbeziehungen zwischen europäischen Nachrichtendiensten und außereuropäischen Partnern. In diesem Zusammenhang trafen sich im März 2025, nach der vorübergehenden Aussetzung des US-amerikanischen Geheimdienstaustauschs mit der Ukraine, mehrere Staaten unter Führung Frankreichs und des Vereinigten Königreichs in Paris und einigten sich darauf, die direkte Zusammenarbeit mit der Ukraine zu intensivieren, einschließlich der Bereitstellung von Überwachungstechnologie und Satellitendaten.

Jüngsten Berichten zufolge hat Frankreich inzwischen die

USA als wichtigsten Intelligence-Lieferanten für die Ukraine abgelöst. Solche spezialisierten Signalaufklärungsgruppen könnten ausgeweitet werden, um den Aufbau europäischer nachrichtendienstlicher Fähigkeiten in diesem Bereich voranzutreiben. Bestehende supranationale Strukturen könnten ebenfalls deutlich ausgebaut werden, etwa das eigene Intelligence and Situation Centre (INTCEN) der EU sowie die Intelligence Directorate des EU-Militärstabs.

Ihre Funktion ist bislang vor allem auf die Analyse beschränkt. INTCEN ermöglicht jedoch bereits die Abordnung von Personal aus nationalen Nachrichtendiensten; dieses Instrument ließe sich potenziell ausweiten und auf weitere Phasen des nachrichtendienstlichen Zyklus anwenden – perspektivisch eines Tages auch auf die Informationsgewinnung selbst. Parallel dazu muss die EU ernsthaft in neue Technologien investieren; sie muss darüber nachdenken, wie sie die Entwicklung militärischer Satelliten ausbauen kann; und sie muss ihre Fähigkeiten zur Überwachung von Kommunikation stärken.

Sobald eine gemeinsame Struktur zur Auslandsaufklärung und -steuerung etabliert ist, stellt sich als nächster Schritt die Frage der Koordinierung der Inlandsnachrichtendienste. Dies ist jedoch deutlich anspruchsvoller, da die rechtlichen Rahmenbedingungen und politischen Kulturen stark divergieren. Gelingt es jedoch, ein tragfähiges Modell für eine gemeinsame europäische Auslandsaufklärung zu entwickeln, könnte dieser Ansatz perspektivisch auch auf andere Bereiche übertragen werden.

Insgesamt hat die EU zwar erkannt, dass sie massiv und koordiniert in den Ausbau ihrer militärischen Fähigkeiten investieren muss. Sie muss jedoch ebenso begreifen, dass der logische nächste Schritt darin besteht, in gleichem Maße ihre Auslandsnachrichtendienste zu stärken, zu koordinieren und weiterzuentwickeln. Europa wird nicht nur mit Panzern und Granaten verteidigt, sondern auch durch einen integrierten Nachrichtendienst, der seine Handlungsfähigkeit und Macht sichert. ■

„Die EU muss ernsthaft in neue Technologien investieren und darüber nachdenken, wie sie die Entwicklung militärischer Satelliten ausbauen kann.“

Aviva Guttman

Cyberkriminalität als Geschäftsmodell verstehen – und kollektiv bekämpfen

Viele Unternehmen verteidigen sich immer noch isoliert, während Angreifer als automatisierte Ökosysteme agieren. Moderne Threat Intelligence dreht dieses Ungleichgewicht um. Die Initiative NetWatch verbindet Echtzeit-Erkennung mit kollektiver Reaktion und macht Cyberabwehr skalierbar.



Viele Sicherheitsmaßnahmen setzen auf Prävention und Reaktion. Warum reicht das aus Ihrer Sicht nicht mehr aus, um Cyberangriffe nachhaltig einzudämmen?

Ralf Schneider: Prävention und Reaktion bleiben zentrale Bausteine, greifen aber allein zu kurz. Cyberangriffe entwickeln sich heute extrem schnell, insbesondere durch KI und Automatisierung. Nötig sind daher proaktive Prävention und adaptive Reaktion in Echtzeit. Entscheidend ist, den Kontext laufend zu verstehen: aktuelle Bedrohungen, Veränderungen und besonders kritische Assets. Das gelingt nur mit kontinuierlicher Cyber Threat Intelligence.

Lars König: Hinzu kommt, dass Unternehmen oft isoliert denken und sich primär selbst schützen. Angreifer agieren dagegen hochautomatisiert und wechseln schnell zwischen Zielen. Deshalb braucht es einen kollektiven Ansatz: Ähnlich einem Immunsystem sollte ein Angriff idealerweise nur einmal erkannt werden, damit anschließend das gesamte Ökosystem davon profitiert.

Was verstehen Sie unter Threat Intelligence?

Lars König: Threat Intelligence ist der strukturierte Austausch von Informationen über Cyberangriffe zwischen unterschiedlichen Akteuren. Man unterscheidet drei Ebenen: taktisch (konkrete Indikatoren wie bösartige IP-Adressen), operativ (wer greift welche Branchen oder Regionen an) und strategisch (neue Angriffsmuster und langfristige Trends). Ziel ist >

Lars König (*links*) bekämpft als Gründer von NetWatch weltweit Missbrauchssysteme durch einen gemeinschaftsbasierten Ansatz. Er ist Teil der Customer Advisory Boards von Google und CrowdStrike.

Dr. Ralf Schneider (*rechts*) ist Vorstandsvorsitzender des Vereins Cyber Security Sharing & Analytics e. V. (CSSA) – einem Zusammenschluss 17 deutscher Großunternehmen mit dem Ziel, sich und die öffentliche IT-Infrastruktur gemeinsam besser vor Cyberangriffen zu schützen.

Mehr unter netwatch.de

es, Angreiferverhalten schnell einzuordnen und handlungsfähig zu werden.

Ralf Schneider: Die größte Herausforderung ist heute die Informationsflut. Unternehmen brauchen nicht mehr Daten, sondern bessere Priorisierung: Was ist für mich jetzt relevant? Dafür braucht es eine hochfokussierte, 24/7 verfügbare Threat Intelligence, die unmittelbar in Entscheidungen und Maßnahmen übersetzt wird. Sonst bleibt man reaktiv und immer einen Schritt zu spät.

Was macht NetWatch aus Ihrer Sicht grundlegend anders als traditionelle Ansätze?

Lars König: Angreifer operieren wie jedes andere Unternehmen nach einem ökonomischen Modell, bei dem sie mehr Geld einnehmen müssen, als sie ausgeben, um profitabel zu bleiben. Ihre Einnahmequellen umfassen beispielsweise Lösegeldforderungen von kompromittierten Unternehmen oder den Verkauf gültiger Zugangsdaten an andere Kriminelle. Auf der Kostenseite fallen Ausgaben für die Aufrechterhaltung der Infrastruktur und Werkzeuge sowie die Zeit an, die für die Vorbereitung und Durchführung von Angriffen auf Opfer aufgewendet wird. NetWatch ist kein klassischer Threat-Intelligence-Provider, sondern greift aktiv ein. Gemeinsam mit Internet-Service-Providern werden Angreifer-Systeme schnell vom Netz genommen. Da sich die Erlösseite kaum beeinflussen lässt, erhöhen wir gezielt die Kosten – vor allem Zeit. So wird das Geschäftsmodell der Angreifer unattraktiv. Außerdem kehren wir den psychologischen Effekt um: Nicht mehr der Verteidiger lebt in Unsicherheit, sondern der Angreifer.

Ralf Schneider: Entscheidend ist der Community- und Open-Source-Ansatz. Die Sensoren sind minimalinvasiv, kostengünstig und für Angreifer nicht erkennbar. Jeder kann mitmachen, und die Verteidigung skaliert mit der Angreiferlandschaft. Das macht kollektive Cyberabwehr praktikabel und wirksam.

Welche konkreten Fragen kann NetWatch für ein Unternehmen beantworten, die klassische Security-Tools offenlassen – und welche Vorteile haben Unternehmen davon?

Lars König: NetWatch zeigt, wer ein Unternehmen aktuell angreift, wo diese Angreifer sonst aktiv sind, wie häufig sie vorgehen und welche Muster sie nutzen. Angriffe werden zu

Gruppen gebündelt, sodass sofort erkennbar ist, ob es sich um gezielte Angriffe oder Massen-Scans handelt. Honeypots (digitale Ködersysteme) liefern zusätzliche Einblicke in Vorgehen und Fähigkeiten.

Ralf Schneider: Der Mehrwert liegt in Frühzeitigkeit und Kontext. Angreifer werden schon beim Eindringversuch erkannt. Statt Informationen zu verlieren, entsteht Echtzeitwissen über Absicht, Risiko und Priorität – eine Grundlage für wirksame Abschreckung.

Wenn Sie einem Manager einen einzigen Grund nennen müssten, warum sich ein Engagement mit NetWatch strategisch lohnt – welcher wäre das?

Ralf Schneider: Cybersecurity funktioniert heute nicht mehr isoliert. Nachhaltige Sicherheit entsteht nur durch kollektive Verteidigung. NetWatch ist ein einzigartiges Vehikel, um in Echtzeit eine echte Community-basierte Cyberabwehr umzusetzen. Man gibt Informationen hinein und bekommt kollektive Sicherheit zurück – das ist Collective Cyber Defense in Reinform.

Lars König: NetWatch ersetzt Einzelverteidigung durch eine vernetzte Community aus Unternehmen, Providern und Behörden. Angriffe werden in Echtzeit erkannt, blockiert und Infrastruktur rasch abgeschaltet. Das verschiebt das Machtverhältnis zugunsten der Verteidiger.

Wie funktioniert in Ihrem Ansatz die Abschreckung – und welche Rolle spielt dabei die ökonomische Logik der Angreifer?

Ralf Schneider: Cyberangriffe erfolgen dezentral und anonym, man kann sie nicht mit einem „großen Gegenschlag“ stoppen. Abschreckung wirkt daher inkrementell: Angriffe werden teurer, und das Risiko, entdeckt und verfolgt zu werden, steigt. Angreifer haben dabei drei zentrale Kostenblöcke: Infrastruktur, Wissen und Menschen. Wird ihre Infrastruktur regelmäßig abgeschaltet, müssen Server neu beschafft, konfiguriert und getarnt werden. Das kostet Zeit und Geld. Gleichzeitig steigt ihr Risiko, je mehr Community und Behörden über Vorgehen, Tools und Muster wissen.

Lars König: Deterrence heißt, Kosten und Risiken für Angreifer dauerhaft zu erhöhen. Wenn Systeme regelmäßig abgeschaltet werden oder Strafverfolgung wahrscheinlicher wird, lohnt sich ein Angriff schlicht nicht mehr. Die „Pyramid of Pain“ zeigt: IP-Adressen lassen sich leicht wechseln, Tech- ➤

niken und Muster nicht. Wird ein Angreifer über seinen digitalen Fingerabdruck erkannt, muss er sein gesamtes Vorgehen ändern. Das unterbricht Operationen und verursacht hohe Kosten.

Wie erkennt man die Absichten eines Angreifers?

Lars König: Der Intent ergibt sich aus Metadaten und Mustern: Benutzer/Passwortkombinationen, Zielsysteme und Angriffshäufigkeit zeigen, ob breit gescannt oder gezielt angegriffen wird. Durch Clustering digitaler Fingerabdrücke lassen sich ganze Angreifergruppen erkennen, auch bei wechselnden IPs. Honeypots liefern zusätzliche Einblicke.

Ralf Schneider: Entscheidend ist das Zusammenspiel aus Technik, Kontext und Mustererkennung. Intent zeigt sich nicht im Einzelereignis, sondern erst durch die übergreifende Echtzeitanalyse vieler Angriffe.

Wie stört man Cyberangriffe?

Lars König: Blockieren schützt nur das eigene Unternehmen. Wirksam wird Cyberabwehr erst durch aktive Störung: Informationen teilen, Angreifer-Systeme über Provider oder Abuse-Meldungen abschalten und früh beim Initial Access eingreifen, bevor sich Angriffe ausbreiten.

Ralf Schneider: Störung heißt auch Attribution. Werden Angreifergruppen identifiziert und an Behörden übergeben, steigt ihr Risiko erheblich. Nachhaltige Cyberabwehr entsteht durch das Zusammenspiel von Unternehmen, Providern und staatlichen Akteuren.

Was geschieht mit der gewonnenen Intelligence und welche Maßnahmen folgen daraus? Was sind die konkreten Ergebnisse?

Ralf Schneider: Entscheidend ist die Kuratierung. Behörden werden nicht aktiv, wenn man sie mit unstrukturiertem Rauschen überschwemmt. Wenn aber Attribution und Muster sauber aufbereitet sind, steigt die Chance, dass Ermittlungsbehörden tatsächlich handeln. So konnten Botnetze identifiziert und mit dem BKA abgeschaltet werden – zehntausende Systeme neu aufzubauen, trifft Angreifer hart.

Lars König: Der Prozess ist folgender: Sensordaten sammeln und gruppieren, das Verhalten analysieren und daraus Blocklisten bauen. So lassen sich Unternehmen in Millisekunden „immunisieren“. Clustering und Honeypots liefern dabei kuratierte Erkenntnisse, die an Behörden weitergegeben werden.

In einem Fall konnten wir ein großes Botnetz samt Zugangsdaten übergeben; die Behörden haben es dann vom Netz genommen.

Welche Rolle spielt die Zusammenarbeit mit Community, Internet-Service-Providern und Behörden?

Ralf Schneider: Kollektive Cyberabwehr basiert auf Vertrauen. NetWatch teilt ausschließlich echte Angreiferdaten – ohne Kundeninformationen und mit minimalen False Positives. So kann sich die Community öffnen und skalieren, was nötig ist, da auch Angreifer als Community agieren.

Lars König: Community schafft Reichweite, ISPs ermöglichen das schnelle Abschalten von Infrastruktur, und Behörden sind entscheidend, um ganze Angreifergruppen koordiniert zu zerschlagen, nicht nur einzelne Systeme.

Wo liegt die Grenze zwischen Verteidigung und Abschreckung, operativ wie strategisch?

Lars König: Verteidigung bedeutet zunächst, Angriffe zu blockieren und sich selbst zu schützen. Abschreckung beginnt dort, wo Angreifer-Infrastruktur aktiv entfernt und deren Kosten sowie Risiken systematisch erhöht werden. Viele Threat-Intelligence-Ansätze enden bei Indikatoren. NetWatch geht einen Schritt weiter, damit Angriffe nicht nur lokal abgewehrt, sondern für alle gestoppt werden.

Ralf Schneider: Ein zusätzlicher Abschreckungseffekt entsteht durch Identifizierung. Wenn Täter oder Gruppen öffentlich zugeordnet werden, steigt ihr persönliches Risiko massiv. Für professionelle Hacker ist das besonders schmerzhaft und erschwert weiteres Operieren erheblich.

Was ist der größte blinde Fleck von Unternehmen beim Thema Cyberresilienz?

Ralf Schneider: Der größte blinde Fleck ist das „Unknown Unknown“ – also das Unvorhersehbare. Dem begegnet man nur mit kontinuierlichem, flexiblem und kreativem Threat Hunting, jenseits von Checklisten und Standards.

Lars König: Hinzu kommt mangelnde Geschwindigkeit. Unternehmen reagieren oft zu langsam, während Angreifer durch KI und Automatisierung extrem schnell sind. Proaktives, automatisiertes Isolieren auf Verdacht ist kulturell noch nicht verankert.

>

Wie viel Offenheit ist für Unternehmen sinnvoll – und wann wird es problematisch?

Ralf Schneider: Angreiferdaten wie bössartige IPs lassen sich gut teilen, solange sie kontrolliert weitergegeben werden. Problematisch wird es, wenn Informationen Angreifern helfen, Muster zu verändern oder Schwachstellen auszunutzen. Compliance setzt hier klare Grenzen: Personenbezogene Daten und interne Prozesse dürfen nicht geteilt werden.

Lars König: Wichtig ist, bereits abgewehrte Angriffe am Perimeter zu teilen. Diese Daten sind skalierbar nutzbar und ermöglichen Korrelationen. Tiefergehende Vorfälle gehören nur in sehr vertrauenswürdige Kreise – zu viel Sichtbarkeit kann auch neue Angreifer anziehen.

Wo endet die Verantwortung einzelner Unternehmen in der Cyberabwehr – und ab wann wird sie staatliche Aufgabe?

Ralf Schneider: Sobald es um Ermittlungen, Strafverfolgung oder Eingriffe in fremde Systeme geht, endet die Verantwortung von Unternehmen. Hackbacks und Attribution können nur staatliche Stellen leisten. Dafür brauchen sie kuratierte, priorisierte Daten statt Rohdatenmengen.

Lars König: Behörden sind unverzichtbar, sobald strafbares Handeln vorliegt. NetWatch liefert ihnen Einblicke in reale Unternehmensangriffe – eine Perspektive, die sie sonst kaum haben – und macht internationale Zusammenarbeit wirksam.

Welche Rolle sollten große Unternehmen in einem europäischen Cyber-Defense-Ökosystem spielen? Und welche neue Verantwortung entsteht dadurch für Vorstände und Geschäftsleitungen?

Ralf Schneider: Cyberabwehr ist Chefsache. Große Unternehmen müssen eigene Cyberkompetenz aufbauen und sich aktiv in Communities vernetzen. Cyber Defense lässt sich nicht outsourcen; Führung muss Vernetzung über Unternehmens- und Sektorgrenzen hinweg ermöglichen und fördern.

Lars König: Vorstände tragen die Verantwortung, Geschwindigkeit und Kooperation zuzulassen. Bei Millionen Angriffen täglich braucht es automatisierten Echtzeit-Datenaustausch statt langsamer Meldungen. Security-Teams müssen sichtbar sein und sich austauschen dürfen – ohne Allianzen bleibt man isoliert.

Gab es in Ihrer Laufbahn einen konkreten

Moment, einen Vorfall oder eine Entscheidung, bei der Ihnen klar wurde: „Cybersecurity ist mehr als nur ein IT-Thema“. Was hat dieser Moment bei Ihnen verändert?

Ralf Schneider: Ja. 2013 war der Wendepunkt: das Abhören von Angela Merkels Handy und kurz darauf die Snowden-Enthüllungen. Da wurde mir klar, welches Machtinstrument Cyber ist – und dass kriminelle Akteure ähnliche Fähigkeiten entwickeln würden. Seitdem hat sich diese Einschätzung leider bestätigt.

Lars König: Bei mir war es Ende 2021 die Schwachstelle in der Java-Bibliothek Log4j. Innerhalb weniger Stunden nach der Veröffentlichung wurde das Internet automatisiert gescannt. Wir mussten wie Angreifer denken, um schneller zu sein. Das zeigte mir, wie groß die Unknown Unknowns sind – und dass Geschwindigkeit und Kreativität entscheidender sind als klassisches Hardening.

Ralf Schneider: Im Verein Cyber Security Sharing & Analytics (CSSA) haben wir das von Lars' Team entwickelte Log4j-Skript geteilt. Andere Unternehmen konnten damit sofort eigene Schwachstellen finden. Das zeigte sehr konkret: Community ist kein Schlagwort, sondern verhindert unmittelbar Schaden.

Lars König: Und das wird noch wichtiger. KI findet Schwachstellen zunehmend automatisiert. Diese Fähigkeiten werden schnell verbreitet sein. Dann entscheiden Sekunden – denn ohne Echtzeit-Sharing lässt sich die erste Angriffswelle nicht stoppen.

Was war für Sie persönlich die schwierigste Entscheidung – nicht technisch, sondern menschlich oder organisatorisch?

Lars König: Der Teamaufbau. Braucht man erfahrene Experten und Expertinnen mit festen Meinungen oder junge Talente mit großem Potenzial? Beides hat Vor- und Nachteile. Der richtige Mix ist schwer zu finden, und Frustration auf beiden Seiten ist fast unvermeidlich. Diese Balance zu halten, ist eine dauerhafte Führungsaufgabe.

Ralf Schneider: Eine Krisenentscheidung, etwa bei der Sicherheitslücke »Heartbleed«: da ging es darum, entgegen aller Regeln nur die echten Könner zusammenzuholen, jenseits aller Hierarchien. Wäre es ein Fehlalarm gewesen, hätte ich massive Konsequenzen gespürt. War es zum Glück nicht. Aber solche Entscheidungen sind menschlich schwer. ■

Sei kein Bot!



Newsletter/human LIVE

human-magazin.de

**Die neue Printausgabe
erscheint am 30. Mai 2026.**

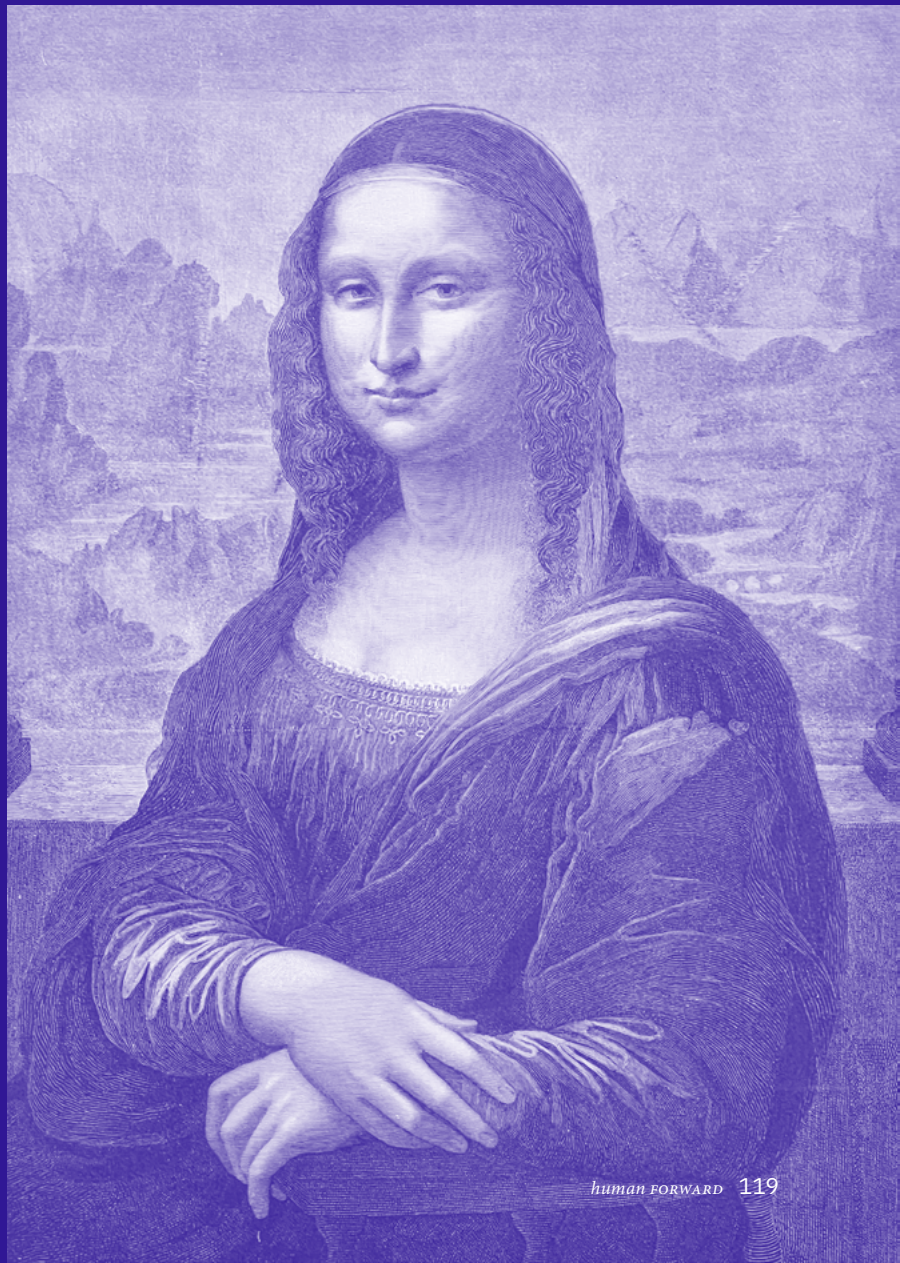
04_ Governance

Macht kontrollieren, Vertrauen schaffen

*„Geheimdienste müssen
kontrolliert werden,
da sie Instrumente der
Exekutive sind.“*

Prof. Dr. Anna Daun, Deutschland

Illustration clu/Stock



„Die Welt wartet nicht auf uns“



Der grüne Bundestagsabgeordnete Constantin von Notz gilt als einer der besten Kenner der Nachrichtendienste im Politikbetrieb. Ein Gespräch über offensive Cyberoperationen, unsere Abhängigkeit von den USA – und die Rolle von Intelligence für die Demokratie.

„Aufgrund der Erfahrung von zwei Diktaturen haben wir ein besonderes Verhältnis zu Nachrichtendiensten.“

Konstantin von Notz

Konstantin von Notz, wenn Sie auf die aktuelle Weltlage schauen: Was geht Ihnen als langjährigem Kontrolleur der deutschen Dienste durch den Kopf?

Konstantin von Notz: Mir geht zuallererst durch den Kopf, dass wir in rauen Zeiten leben, in denen man gut funktionierende Nachrichtendienste braucht. Unsere Welt verschiebt sich geopolitisch massiv und steht enorm unter Druck. Es geht viel um Intelligence, also um die Frage, was man weiß, was man versteht und was man prognostizieren kann. Deshalb ist es wichtig, dass wir über gute Dienste verfügen, die international gut vernetzt sind und starke Partner haben. Die Diskussion, die wir in Deutschland über die Bedeutung der Zeitenwende auch für die Dienste führen, ist vor dem Hintergrund der aktuellen Auseinandersetzungen absolut richtig.

Sie befassen sich seit fast zehn Jahren mit der parlamentarischen Kontrolle der Dienste. Was haben Sie in dieser Zeit darüber gelernt, wozu wir Nachrichtendienste überhaupt brauchen, gerade als Grünen-Politiker mit besonderem Blick auf Demokratie und Bürgerrechte?

Aufgrund der Erfahrung von zwei Diktaturen haben wir ein besonderes Verhältnis zu Nachrichtendiensten. Selbstverständlich spielten sie auch und gerade während der deutschen Teilung eine Rolle. Heute werden die Dienste im Inland tätig, bevor die Polizei zuständig ist, verfassungsrechtlich klar getrennt, mit begrenzten Befugnissen zur

Beobachtung von Extremismus in all seinen Ausprägungen. Heute streben Rechtsextremisten offen nach politischer Macht, um unsere liberale Demokratie zu zerstören. Das verändert die Debatte. Wenn der Inlandsnachrichtendienst sagt, er schütze unsere Verfassung, dann ist das angesichts sehr ernster innerer und äußerer Bedrohungen offenkundig dringend notwendig.

Wie hat die Zeitenwende Ihren Blick auf die Dienste verändert?

Schon vor der Vollinvasion der Ukraine haben wir aggressives Agieren Russlands und auch Chinas gesehen. Diese offene Aggressivität war sichtbar, auch und gerade auf nachrichtendienstlicher Ebene. Bei der parlamentarischen Kontrolle geht es darum, ob Recht und Gesetz eingehalten werden. Angesichts der veränderten Weltlage geht es aber immer stärker auch um die Frage, ob die Dienste ihrem Auftrag gerecht werden: Schützen sie die Verfassung und die Interessen Deutschlands und Europas? Gewinnt der BND die notwendigen Erkenntnisse, um Bedrohungen von außen besser abzuwehren? Informiert man die Politik rechtzeitig über aktuelle Entwicklungen?

Stimmen Sie den Autoren Katja Gloger und Georg Mascolo („Das Versagen“) zu, dass unsere Dienste im Fall Russland eigentlich gut geliefert haben – und das „Versagen“ eher auf politischer Seite lag?

Dem würde ich zustimmen. Die Dienste haben die Problematik früh gesehen und immer wieder deutlich adres-

INTERVIEW_ Konstantin von Notz

Dr. Konstantin von Notz ist Mitglied des Bundestages (Bündnis 90/ Die Grünen) und stellvertretender Vorsitzender des parlamentarischen Kontrollgremiums, das die drei Nachrichtendienste des Bundes, den Bundesnachrichtendienst (BND), den Militärischen Abschirmdienst (MAD) und das Bundesamt für Verfassungsschutz (BfV) überwacht. Er war unter anderem Vorsitzender des Untersuchungsausschusses „NSA“ sowie Mitglied im Untersuchungsausschuss „Berliner Breitscheidplatz“, seit 2017 ist er Mitglied im parlamentarischen Kontrollgremium, dessen Vorsitz er von 2021 bis 2025 innehatte.

KEY MESSAGES

- **Zeitenwende für die Dienste:** In einer konfliktreichen Welt brauchen wir leistungsfähige Nachrichtendienste für politische Entscheidungen
- **Russland:** Dienste warnten früh, doch Politik, Wirtschaft und Öffentlichkeit unterschätzten lange die Bedrohung.
- **Cyberabschreckung:** Offensive Cyberfähigkeiten sind denkbar – aber nur mit klaren Zuständigkeiten, gesetzlichen Regeln und strenger Kontrolle.
- **Digitale Abhängigkeiten:** Die starke Abhängigkeit von US-Technologien schwächt die europäische Souveränität.
- **Europäische Kooperation:** Gemeinsame Analysen, ein Lagebild zu Spionage und Sabotage sowie engere Partnerschaften werden wichtiger.

siert. Das Versagen lag aber zweifellos nicht nur bei politischen Verantwortlichen, sondern auch in Teilen der Wirtschaft und der Medien. Man hat sich lange etwas vorgemacht und vieles schöngeredet. Wenn man auf China schaut, sieht man ähnliche Debatten. Teilweise wird noch immer naiv argumentiert, etwa beim Einbau von Technik oder bei Fragen digitaler Souveränität. Und auch auf Palantir setzen wir weiter.

Wie bewerten Sie den aktuellen Prozess zur Reform der Dienste?

Die Debatte, ob die Dienste angesichts aggressiven Verhaltens Russlands und veränderter Partnerlogiken mit den USA Anpassungen brauchen, ist berechtigt. Es besteht Veränderungsdruck, auch im klaren rechtsstaatlichen Rahmen. Beim BND kann ich bestimmte Erweiterungen mit klaren Leitplanken nachvollziehen. Die Ausweitung auf den Inlandsnachrichtendienst halte ich jedoch verfassungsrechtlich für sehr schwierig. Wenn wir schnell handeln wollen, sollten wir tun, was verfassungsrechtlich machbar ist und wofür sich demokratische Mehrheiten organisieren lassen. Für diese Debatten stehen wir zur Verfügung.

Wie beurteilen Sie die Aussagen des neuen BND-Präsidenten Martin Jäger auf der Münchner Sicherheitskonferenz, der Dienst müsse im Hinblick auf hybride Angriffe auch selbst „operativer“ werden, Stichwort „aktive Gegenmaßnahmen“?

Ich glaube, das muss man ernsthaft diskutieren. Deutschland ist die drittgrößte Wirtschaftsnation der Welt, das wirtschaftlich stärkste und bevölkerungsreichste Land Europas. Da kann man sich nicht dauerhaft den Luxus leisten zu sagen, wenn es schwierig wird, sollen es die Niederländer oder die Briten machen. Diese Position trägt

nicht. Gleichzeitig haben wir mit Blick auf die aktuelle Vorlage der Bundesregierung Bedenken, dass sie die rechtliche wie politische Klarheit schafft, die es dringend braucht!

„Deutschland ist eines der am meisten angegriffenen Länder der Welt.“

Konstantin von Notz

Konkret gefragt: Sind Sie für offensive Cyberoperationen?

Mit bestimmten Sicherungsmechanismen kann ich mir das vorstellen. Bisher haben wir immer gesagt, dass die Abwehr von Cybermaßnahmen vor allem wegen der schwierigen Attribution problematisch ist. Inzwischen gibt es Fälle, in denen die Zuordnung relativ klar ist. Gleichzeitig sehen wir, dass sich die Bundesregierung teils nicht einmal einigen kann, ob die Bundespolizei oder das BKA oder das BSI (Bundesamt für Sicherheit in der Informationstechnik) zuständig sein sollen. Wenn dann noch der BND hinzukommt, wird es noch schwieriger. Aber wir werden nicht pauschal Nein sagen. Auch in der Opposition prüfen wir solche Vorschläge sorgfältig und entlang der verfassungsrechtlichen Vorgaben. Wenn es im Rahmen der freiheitlich demokratischen Grundordnung möglich ist, kann man darüber sprechen.

Gerade bei offensiven Cybermaßnahmen stellt sich die Frage, wie nah das verfassungsrechtlich (Artikel 26) an einen Angriff rückt...

Absolut. Das haben wir immer betont, insbesondere wenn Attribution schwie-

rig ist, etwa wenn Server in Drittstaaten genutzt werden. Aber wenn man solche Befugnisse diskutiert und gesetzlich regelt, kann man rechtsstaatliche Bedingungen klar hineinschreiben. Es

geht nicht ums Verunmöglichen, sondern um robuste und rechtssichere Regelungen.

Inwiefern geht es bei offensiven Cyber-Fähigkeiten um Abschreckung?

Auf der einen Seite muss man es faktisch können. Auf der anderen Seite muss man auch signalisieren, dass man es kann. Sonst werden wir weiter täglich angegriffen. Deutschland ist eines der meistangegriffenen Länder der Welt. Das hat mit unserem Wohlstand zu tun, mit Defiziten beim Schutz, aber auch mit mangelnder Rückschlagfähigkeit. Das muss sich ändern.

Welche Rolle spielt dabei unsere technologische Abhängigkeit, insbesondere von den USA?

Das ist ein enormes Problem. Seit Jahren diskutieren wir über Abhängigkeiten bei Social Media, Huawei-Technik im Mobilfunk, kritischer Infrastruktur oder amerikanischer Software für unsere Sicherheitsbehörden. Die Bundesregierung hat lange gezögert, klare Kriterien zu setzen. Bei Energiefragen wurde zwar reagiert, aber vor allem im Digitalen sind wir spät dran. Deutschland ist stark abhängig, das kann schnell existenziell werden. Wir müssen diese >

Abhängigkeiten reduzieren – mit klaren politischen Vorgaben, rechtlichen Regeln und klaren Beteiligungsquoten. Das Wirtschaftsministerium schaut inzwischen genauer hin, aus unserer Sicht aber noch nicht scharf genug.

Was heißt das konkret im Hinblick auf die Abhängigkeit von US-Technologien, gerade auch bei KI? Was können wir hier überhaupt noch tun?

Wir müssen uns auf unsere eigenen Stärken besinnen. So wie wir es bei der Regulierung mit dem Digital Services Act und der EU-Datenschutzgrundverordnung getan haben. Als Wirtschaftsraum mit 450 bis 500 Millionen wirtschaftskräftigen Konsumenten sind wir ein relevanter Marktteilnehmer mit echtem Impact. Daraus folgt, dass wir uns in zentralen digitalen Bereichen nicht vollständig abhängig machen dürfen.

Das heißt, wir müssen darüber reden, welche eigenen Plattformen wir schaffen können. Ich stehe hinter dem öffentlich-rechtlichen Rundfunk. Aber bei rund acht Milliarden Euro im Jahr muss man schon fragen, wie wir das in die digitale Welt übertragen und dort Meinungsvielfalt absichern. Diese Diskussion kann man verlangen....

Meinen Sie damit, wir sollten die Mittel für den ÖRR besser in eine digitale Plattform investieren?

So pauschal würde ich das nicht sagen. Aber digitale Souveränität bedeutet auch, eigene Strukturen zu fördern und zu modernisieren. Es ist legitim zu fragen, wie viel in den letzten zehn Jahren in echte digitale Infrastruktur geflossen ist. Die Frage muss erlaubt sein: Brauchen wir nicht eine europäische Plattform? Es kann doch nicht sein, dass der reichste Mann der Welt morgen entscheidet, ein Netzwerk

abzuschalten oder bestimmte politische Kräfte massiv zu stärken. Der öffentlich-rechtliche Rundfunk ist historisch auch als Antwort auf Gleichschaltung entstanden. Haben wir die nötigen Reformschritte gemacht, um in der digitalen Welt anzukommen? Ich würde sagen, nein.

Wäre das so etwas wie eine öffentlich-rechtliche Konzeption für den digitalen Raum?

Ja, warum eigentlich nicht? Eine Plattform ist kein Hexenwerk. China rollt seine Angebote auch strategisch aus. Wir sind die drittgrößte Wirtschaftsna-tion der Welt mit 84 Millionen Menschen. Europäisch gedacht ist das noch einmal eine ganz andere Dimension. Aber man muss aus dem alten Trott herauskommen. In den letzten Jahren hat es daran gemangelt. Jetzt zwingt uns die globale Entwicklung zum Handeln.

Was bedeutet für Sie europäische nachrichtendienstliche Souveränität? Gemeinsame Analysen, ein europäisches Lagebild, vielleicht sogar ein europäischer Dienst?

Wir haben das Schlagwort „Euro Eyes“ geprägt, weil bislang immer nur von den „Five Eyes“ die Rede ist. Doch selbst dort ist die Lage schwieriger geworden. Kanada, Australien und auch Großbritannien sind durch das Agieren der aktuellen US-Administration verstimmt. Zugleich hängt die Stärke von Diensten vom Zugang zu Netzknoten und Infrastruktur ab. Europa hat hier Gewicht, nutzt es aber zu wenig. Wenn wir uns behaupten wollen, brauchen wir eine engere und bessere Kooperation unter befreundeten Diensten. Sicherheit und Nachrichtendienste sind Kernbereiche staatlicher Souveränität, Integration ist hier besonders anspruchsvoll. Doch wenn Europa nicht nur reagieren

will, muss es entschlossener handeln.

Sollte das ein EU-Projekt sein oder eher eine Koalition williger Partner?

Man muss in Stufen denken. Zuerst braucht es passende Partner. Enge Kooperationen gibt es bereits, die kann man durchaus ausbauen. Wenn daraus später ein Integrationsmodul wird, umso besser. Aber wir sollten nicht erst 37 Jahre an der perfekten Lösung feilen. Wir müssen ins Tun kommen. Das gebieten die stark gestiegenen Bedrohungslagen. Die Welt wartet nicht auf uns.

Zurück zur nationalen Ebene. Wie lässt sich die Kommunikation zwischen Politik und Diensten verbessern?

Wir haben in Deutschland weiterhin kein einheitliches Lagebild zu Spionage und Sabotage, auch nicht zum Ausspähen kritischer Infrastruktur, und schon gar kein öffentlich kommuniziertes. Eigentlich bräuchten wir ein europäisches Lagebild, am besten wöchentlich. Die Menschen müssten nachvollziehen können, was konkret passiert: Spionage allerorten, Sabotage an Gleisen, zerstörte Strommasten, Einbrüche in Kasernen. Stattdessen bleibt alles diffus.

Jeder Drohnenüberflug wirkt nebulös, jeder Vorfall wird relativiert. Es fehlen klare Kategorien und eine systematische Einordnung, die Entwicklungen sichtbar macht. In Bundestagsanhörungen wird die Lage zwar als kritisch beschrieben, doch das dringt kaum durch. Zugleich verharmlosen manche Parteien die Bedrohung. Auch Regierungen haben es versäumt, das Problem öffentlich klar zu benennen.

Wie können Politiker eine bessere, dialogischere Beziehung zu Bürgerinnen und Bürgern aufbauen?

Natürlich muss kommunikativ etwas >

passieren, weil viele das Gefühl haben, es stimmt etwas grundsätzlich nicht. Aber wir sind eine repräsentative Demokratie: Das Grundprinzip ist, dass man jemanden wählt, der für vier Jahre Politik macht. Wenn er es gut macht, wird er wiedergewählt, wenn nicht, dann nicht. Digitalisierung und soziale Medien erzeugen den Eindruck permanenter Echtzeitpolitik, das ist hoch populismusanfällig.

Was meinen Sie damit?

Viele politische Entscheidungen sind extrem komplex und voraussetzungs-voll. Auf der Straße klingt vieles einfach und plausibel, etwa die Idee, dass ein Antrag automatisch genehmigt ist, wenn die Behörde nach drei Monaten nicht reagiert. Aber wenn man das auf Nummernschilder, Waffenscheine oder Bauanträge im Naturschutzgebiet anwendet, merkt man schnell, dass es komplizierter ist....

gung ausbauen und die Transparenz staatlichen Handelns erhöhen. Gleichzeitig braucht es ein realistisches Erwartungsmanagement. Die Menschen wählen Profis, damit sie sich nicht täglich mit allen Details beschäftigen müssen. Am Ende können sie ein hartes Urteil fällen.

Und bei aller Kritik sollten wir die Dinge nicht schlechter reden, als sie sind. Ja, es gibt Probleme. Aber wir leben in Wohlstand und großer Sicherheit. Im globalen Vergleich ist Deutschland alles andere als eine Bananenrepublik. Ich plädiere dafür, selbstbewusster auch eine positive Diskussion über Europa zu führen, gerade im Vergleich zu autoritären Systemen.

Können Nachrichtendienste über ihre klassische Aufgabe hinaus eine aktivere Rolle im demokratischen Diskurs übernehmen, gerade im heutigen Informationsumfeld? Etwa durch ein öffentliches Lagebild?

man könnte es zusammenführen. In Berlin gibt es seit Jahren öffentliche Anhörungen der Präsidentinnen und Präsidenten der Dienste im Bundestag, online abrufbar. Dort wurden zuletzt sehr deutliche Warnungen formuliert – etwa zur russischen Bedrohung....

Welche Warnungen meinen Sie?

Der Präsident des BND hat etwa gesagt, er gehe davon aus, dass Russland die NATO vor 2029 angreift. Das ist eine gravierende Aussage. Er sagt nicht, das könne vielleicht passieren, sondern dass er davon ausgeht. Und er sagt das nicht aus dem Bauch heraus, sondern auf Grundlage der Erkenntnisse seines Dienstes. Mich wundert manchmal, wie wenig solche Informationen in der Öffentlichkeit wirklich diskutiert werden.

Insofern können die Dienste mit ihren Erkenntnissen durchaus einen Beitrag zum demokratischen Diskurs leisten. Nicht als einzige Stimme, aber als wichtiger Teil des Diskurses. Da ist noch Luft nach oben.

Muss sich dafür auch die Kultur der Dienste verändern? Eine Social-Media-Kampagne des BND zur Rekrutierung neuer Mitarbeiter und Testimonials zum 70. Geburtstag des Dienstes werden kaum reichen...

Das finde ich etwas streng. Es gibt heute deutlich mehr Offenheit und Austausch. Dienste diskutieren öffentlich, die Vernetzung mit der Wissenschaft ist gewachsen. Natürlich bleiben sie Geheimdienste, totale Transparenz wäre widersinnig. Aber die Haltung hat sich verändert. Sie verstehen sich stärker als Teil der demokratischen Gesellschaft, werben auf Messen, sprechen mit jungen Leuten und suchen den Dialog mit der Zivilgesellschaft. Auch die Snowden-Enthüllungen und das

„Die Dienste können mit ihren Erkenntnissen einen Beitrag zum demokratischen Diskurs leisten.“

Konstantin von Notz

Was kann die Politik dann überhaupt gegen die Unzufriedenheit vieler Bürger und Bürgerinnen tun?

Interessant ist, dass diese Frustration mit Politik in fast allen westlichen Demokratien existiert, unabhängig davon, wer regiert. Wir haben mit Bürgerräten experimentiert, um Beteiligung zu stärken. Aber selbst dort wurden Ergebnisse infrage gestellt, wenn sie politisch nicht passten. Man sollte Bürgerbeteili-

Ich halte das für sinnvoll. In anderen Ländern wird sehr viel offener mit Intelligence umgegangen – mit Erfolg. Nicht jede Information muss geheim bleiben. Es gibt Erkenntnisse, die für die Öffentlichkeit relevant sind und einen gesellschaftlichen Mehrwert haben, wenn man sie transparent macht. Ein Lagebild zu Spionage und Sabotage wäre zwar sowohl polizeilich als auch nachrichtendienstlich geprägt, aber

NSU-Versagen haben wichtige Lernprozesse angestoßen. Sicher ist nicht alles perfekt, aber die Entwicklung ist durchaus positiv.

Wie blicken Sie heute auf die Snowden Affäre?

Wir haben immer gesagt, die Frage, ob Snowden ein Verräter oder ein Held ist, führt nicht weiter. Er selbst hat gesagt, dass er Gesetze gebrochen hat und sich einem Verfahren stellen würde. Die eigentliche Frage ist, ob er auf Grundlage eines Gesetzes von 1907 dauerhaft ohne angemessene Verteidigungsmöglichkeiten verfolgt wird. Aus heutiger Sicht bleibt für mich auch, dass es ein politisches Versäumnis war, Putin diesen symbolischen Triumph zu überlassen. Das hätte man aus meiner Sicht vermeiden können...

Und zwar wie?

Ich glaube, man hätte einen Weg finden können. Nicht indem man sagt, das sei alles rechtlich in Ordnung gewesen, sondern indem man es politisch einordnet. Kein demokratischer Dienst dieser Welt hat nach den Snowden-Enthüllungen unverändert weitergearbeitet. Er hatte also zweifellos einen Punkt. Das kann man nicht wegdiskutieren. Zugleich ist es problematisch, dass er weiter in Moskau sitzt und instrumentalisiert wird. Bei Julian Assange sehe ich das anders, dort spielten russische Dienste aus meiner Sicht früh eine Rolle. Bei Snowden kam erst die Veröffentlichung, dann die politische Nutzung. Sicher wissen lässt sich das nie. Aber das ist meine Einschätzung.

Sie befassen sich seit vielen Jahren intensiv mit Nachrichtendiensten. Entwickelt man da eine gewisse persönliche Affinität?

Wenn man sich so intensiv mit Diensten beschäftigt, färbt das natürlich ab. Man lernt die Arbeit in den Behörden ken-

nen, spricht mit Mitarbeiterinnen und Mitarbeitern, versteht Abläufe, Risiken, Stärken und Schwächen. Vieles, was vorher abstrakt war, wird konkret. Aber man darf die eigene Rolle nie vergessen. Unsere Aufgabe ist Kontrolle. Wir sollen für das Parlament scharf hinschauen. Und das tun wir.

In den letzten zehn bis zwölf Jahren haben wir die Kontrollmöglichkeiten deutlich ausgebaut, mit inzwischen rund 30 Mitarbeitenden. Wir haben sehr intensive Prüfaufträge durchgeführt, Veränderungen angestoßen und uns auch immer wieder öffentlich sehr kritisch geäußert, etwa bei der Frage deutscher Bundeswehr-Piloten, die in China ausbilden. Kontrolle heißt nicht Nähe, sondern kritische Distanz.

Gibt es ein zentrales Learning aus diesen Jahren der Kontrolle?

Über konkrete Sachverhalte darf ich nicht sprechen. Aber abstrakt gesagt haben wir vor einigen Jahren festgestellt, dass sich die Dienste zu wenig mit russischen Aktivitäten in Europa und Deutschland beschäftigt haben. Auch die Rolle von Proxy-Strukturen und die Aggressivität chinesischer Dienste wurden deutlich unterschätzt. Das hat sich inzwischen stark verändert. Wenn man sieht, wie sich etwa der Militärische Abschirmdienst strukturell und personell neu aufgestellt hat, dann ist das Ausdruck eines Lernprozesses.

Zum Abschluss eine persönliche Frage: Wenn Sie selbst für einen Dienst arbeiten würden – lieber operativ oder analytisch?

Ich glaube, ich wäre im analytischen Bereich besser aufgehoben. Das entspricht eher dem, was ich mitbringe. Wobei ich großen Respekt vor den operativ Tätigen habe. Informationen im Ausland zu beschaffen oder auch im Inland komplexe Sachverhalte aufzuklä-

ren, ist ein anspruchsvoller und sehr relevanter Job. Aber meine Stärke läge wohl in der Analyse und Auswertung. ■

„Man muss sich die Hände schmutzig machen“

Das Trennungsgebot prägt deutsche Nachrichtendienste bis heute. Der Rechtswissenschaftler Luca Manns erklärt, warum es rechtlich kein Tabu ist, wo operative Befugnisse denkbar werden – und weshalb Cyberraum, Fernmeldeaufklärung und politische Risikobereitschaft entscheidend sind.

Luca Manns, was unterscheidet denn die Dienste, die wir in Deutschland haben, von „echten“ Geheimdiensten?

Luca Manns: In Deutschland wird oft zwischen Nachrichten- und Geheimdiensten unterschieden, auch wenn keine trennscharfen Kriterien existieren. Die Differenzierung geht auf historische Erfahrungen mit der Gestapo und der DDR-Staatssicherheit zurück, also Behörden, die Informationen sammelten und zugleich polizeilich handelten. Um solche Allmachtsstrukturen zu verhindern, entstand das Trennungsgebot, das auf den „Polizeibrief“ der Alliierten zurückgeht. Er bestimmte, dass dem Verfassungsschutz keine polizeilichen Befugnisse zustehen und er nicht Teil der Polizei ist.

Was heißt das konkret? Was dürfen BND und Verfassungsschutz und was dürfen sie nicht?

Das Trennungsgebot ist heute in allen Nachrichtendienstgesetzen verankert. Die Mehrheit der Juristen geht aber davon aus, dass es keinen Verfassungsrang hat. Seine Urteile im Sicherheitsrecht hat Karlsruhe folgerichtig nicht hierauf gestützt, sondern das Verhältnismäßigkeitsprinzip des Grundgesetzes herangezogen und hieraus ein informationelles Trennungsprinzip abgeleitet: Nachrichtendienste dürfen Erkenntnisse unter niedrigeren Schwellen erheben, dann aber keine operativen Anschlussbefugnisse darauf gestützt wahrnehmen. In den Worten des Rechtslehrers Christoph Gusy: „Wer >



INTERVIEW_ Luca Manns

Luca Manns ist Geschäftsführer der Forschungsstelle Nachrichtendienste der Universität zu Köln. Der Rechts- und Wirtschaftswissenschaftler publiziert regelmäßig in juristischen Fachzeitschriften, berät Regierungsstellen sowie Parlamente. Daneben wirkt er am Aufbau der Adenauer School of Government der Kölner Universität mit und lehrt zum Recht der Digitalisierung.

KEY MESSAGES

- **Das Trennungsgebot** bestimmt, dass dem Verfassungsschutz keine polizeilichen Befugnisse zustehen.
- **Nachrichtendienste** dürfen Informationen mit niedrigen Schwellen erheben, sind aber bei operativen Anschlussbefugnissen rechtlich stark begrenzt.
- **Die Reformdebatte** zielt auf neue Fähigkeiten im Cyberraum, etwa Hackbacks bei Angriffen.
- **Rechtliche Ermächtigungen** allein reichen nicht aus: Operative Schwächen, Personaldefizite und Risikoaversion mindern die Wirksamkeit.
- **Zeitgemäße Intelligence** erfordert leistungsfähige Fernmeldeaufklärung, temporäre Datenspeicherung und den grundrechtskonformen KI-Einsatz.

(fast) alles weiß, soll nicht alles dürfen; wer (fast) alles darf, soll nicht alles wissen“.

Worum geht es bei der aktuellen Diskussion um die Reform des Nachrichtendienstrechts?

Verfassungsschutzpräsident Sinan Selen hat mehrfach betont, in der heutigen Zeit reiche das Detektieren von Bedrohungen nicht mehr, es brauche auch Disruptionen durch „Abwehrdienste“. Dieser Befund soll in Befugniserweiterungen münden, die beim BND angesichts seines militärischen Auftrags noch weiter reichen werden als beim Verfassungsschutz.

Welche operativen Befugnisse wären rechtlich denkbar?

Über gezielte Tötung oder ähnlich schwerwiegende Eingriffe reden wir sicherlich nicht. Vorrangig geht es um den Cyberraum, weil digitale Bedrohungen massiv zugenommen haben. Die Schädigung der deutschen Wirtschaft durch Hacking ist enorm, gleiches gilt für Angriffe auf Behörden. Das ist, gepaart mit Desinformationskampagnen, eine Form hybrider Kriegsführung. BND und Verfassungsschutz wollen künftig selbst eingreifen, also laufende Attacken stoppen und nötigenfalls gegnerische IT zerstören.

Warum gerade im Internet?

In der Verfassungsrechtsprechung kommt dem schon angesprochene Kriterium der operativen Anschlussbefugnisse eine wichtige Bedeutung zu. Folgt eine staatliche Intervention, die als operativ einzustufen ist, auf eine nachrichtendienstliche Ausgangsmaßnahme, gelten für diesen ersten Schritt plötzlich ebenfalls hohe Schwellen. Hacking im Internet unterliegt jedoch anders als etwa eine Verhaftung, der man sich rechtlich beugen muss, keiner

Logik von Befehl und Zwang und dürfte daher nur selten als operativ zu bewerten sein. Im Netz existiert kein territoriales Gewaltmonopol.

Und bei realweltlichen Maßnahmen?

Hier sprechen wir eher über den BND, denn im Inland stehen an der Seite des Verfassungsschutzes ja die Polizeibehörden. Der Auslandsdienst möchte nun in Krisenlagen zum Beispiel Infrastrukturen sabotieren können. Denken Sie an militärische Einrichtungen oder Glasfaserkabel gegnerischer Geheimdienste. Klar ist, dass diese Überlegungen stärker in das hineinragen, was Anhängern des tradierten Trennungsgebots missfällt, und dass sie rechtlich streitiger sein werden.

Würden nicht bereits „Hackbacks“ Eskalationen mit anderen Staaten befeuern?

Theoretisch ja. Praktisch halte ich das Risiko für geringer. Wir leben in einer hybriden Konfliktlage. Staaten wie Russland oder China gehen ohnehin davon aus, dass zurückgehackt wird, weil sie uns selbst permanent digital beschießen. „Hackbacks“ unterscheiden sich diesbezüglich gravierend von territorialen Einwirkungen.

Ein Restrisiko bleibt also immer?

Das liegt in der Natur der Sache, diese Unsicherheit kann kein Gesetz auflösen. Am Ende ist der Einsatz von Diensten eine politische Risikoentscheidung, für die das Recht die äußeren Grenzen vorgibt.

Können unsere Dienste überhaupt mehr?

Das ist eine berechtigte Frage. Denken Sie etwa an Computer-Netzwerk-Operationen, wie im BND das Hacken feindlicher Computer heißt. Dem Dienst ist bislang operativ längst nicht alles gelungen, was er schon aktuell darf. Gesetzliche Ermächtigungen genügen nicht, wenn Kompetenz und Personal

fehlen. An anderen Stellen wie der Fernmeldeaufklärung sind es tatsächlich juristische Hürden, an denen der BND scheitert.

Die Welt verändert sich rasend schnell, von neuen Technologien bis hin zu geopolitischen Umbrüchen. Wie können Nachrichtendienste Schritt halten?

Die deutschen Dienste sind in Abkehr von der „kämpfenden Verwaltung“ des Dritten Reichs stark behördlich geprägt. Positiv ist zwar, dass angesichts der neuen politischen Unterstützung viele Mitarbeiter in Aufbruchstimmung geraten. Dennoch bremsen mitunter starre Hierarchien die Schlagkraft.

„Dem BND ist operativ längst nicht alles gelungen, was er schon aktuell darf.“

Luca Manns

Das klingt verhalten.

Nehmen Sie den BND: Er hat eine starke Personalvertretung mit Auseinandersetzungen über Arbeitszeiten oder Zulagen bis vor die Gerichte. Das ist ein völlig anderer Laden als etwa die CIA. Dazu kommt eine gewisse deutsche Grundängstlichkeit. Dort, wo der BND gesetzlich viel Spielraum hat, performt er nicht in jedem Fall auf höchstem Niveau. >

...zum Beispiel?

Bei der Satellitenaufklärung. Als 2014 die Annexion der Krim begann, musste der Dienst stundenlang auf kommerzielle Zulieferungen warten, weil er über keine eigenen Bilder verfügte. Die Beschaffung des ersten BND-Satelliten überhaupt läuft seit über zehn Jahren, er ist noch immer nicht im All.

Gilt das auch für menschliche Quellen?

Der BND darf niemanden erpressen. Aber in ärmeren Ländern sind Geld und krumme Deals ohnehin häufiger entscheidend für die Informantengewinnung. Dafür muss man rausgehen, sich in gefährlichem Umfeld bewegen und die Hände schmutzig machen. Eine solche Bereitschaft ist im BND strukturell schwächer ausgeprägt als bei manch anderem Auslandsdienst. Auch, weil die Bundesregierung sich lange vor robustem Auftreten scheute. Präsident Jäger hat deshalb konsequenterweise eingefordert, sein eigenes Haus müsse „operativer“ werden und mehr wagen.

Was muss sich noch verändern?

Der größte, oft unterschätzte Hebel mit Blick auf den BND ist die Fernmeldeaufklärung. Klassische Quellenarbeit ist extrem aufwendig und hängt oft von Zufällen ab. Informanten im Kreml oder im Politbüro der chinesischen KP zu rekrutieren – seien wir ehrlich, so gut sind wir zumeist nicht. Breit angelegte technische Überwachung ist deshalb das Mittel erster Wahl.

Wo stehen wir da?

Der BND muss Daten derzeit nach dem Gewinnen sofort filtern und, wenn bestimmte Schutzrechte eingreifen oder kein eingespeister Selektor anschlägt, löschen. Es erfolgt keine zeitweise Speicherung, wie es fast alle anderen EU-Staaten geregelt haben. Das ist eine

enorme Beschränkung, da gezielte Anfragen oft erst später erfolgen, vielleicht nach einem vermuteten Sabotageakt oder wenn ein Terrorist auf das behördliche Radar gerät. Ende-zu-Ende-Verschlüsselung verstärkt das Problem, weil sich Inhaltsdaten kaum noch lesen lassen. Der neue Gesetzentwurf mit Speicherfristen von sechs Monaten für Inhalte und 18 Monaten für Metadaten wäre ein Schritt zu zeitgemäßer Aufklärung, der mit Blick auf die Dauer sogar noch unterhalb der friedliebenden Schweiz läge.

hilft, Selektierungen zu verbessern und so weniger nachrichtendienstlich irrelevante Treffer menschlichen Auswertern vorzulesen, die diese mitunter sehr privaten Daten bislang zumindest kurz erfassen. ■

„Die Beschaffung des ersten BND-Satelliten überhaupt läuft seit über zehn Jahren, er ist noch immer nicht im All.“

Luca Manns

Dies auch in Verbindung mit KI-Analyse?

An dieser Stelle nehme ich viele Ängste wahr. Es liegt auf der Hand, dass die Verarbeitung auf kommerziellen Servern oder der Einsatz von US-Tools mit Internetverbindung datenschutzwidrig wäre. Mir scheint allerdings, dass unsere Dienste hierfür sensibilisiert sind. Bezogen auf den Grundrechtsschutz kann KI sogar Gutes bewirken, wenn sie

Demokratische Selbstverteidigung

Wie politisch sind die deutschen Nachrichtendienste – und wie politisch dürfen sie sein? Der Rechtswissenschaftler Jan-Hendrik Dietrich über ein mögliches AfD-Verbot und die Funktion des Verfassungsschutzes in der „wehrhaften Demokratie“.

Jan-Hendrik Dietrich, wie sehen Sie die aktuellen Herausforderungen der deutschen Nachrichtendienste zwischen Geopolitik und AfD-Verbotsdiskussion? Wie muss sich der rechtliche Rahmen ändern, insbesondere mit Blick auf „echte“ geheimdienstliche Befugnisse?

Jan-Hendrik Dietrich: Die deutschen Nachrichtendienste stehen zunehmend unter Druck. Das liegt vor allem an der Gleichzeitigkeit von verschiedenen, vielfach entgrenzten Bedrohungen von ganz erheblicher Intensität. Oft hängen einzelne Phänomene auch zusammen. Die Grenze zwischen Reichsbürgern und Rechtsextremisten ist zum Beispiel genauso fließend wie die zwischen Extremisten und Spionen. Schon gar nicht lassen sich innere und äußere

Bedrohungen immer klar voneinander trennen.

Für die Nachrichtendienste bedeutet das Dauerstress. Die einzige Möglichkeit, die wirklich immensen Herausforderungen zu bewältigen, liegt in der sicherheitsbehördlichen Kooperation – national wie international. Die deutschen Dienste – gerade die Verfassungsschutzbehörden der Länder – sind vergleichsweise klein. Sie können ihren Auftrag nur erfüllen, wenn sie optimal mit anderen zusammenarbeiten. Notwendig ist dafür ein schneller Informationsaustausch, auf nationaler Ebene insbesondere mit den Strafverfolgungsbehörden, ggf. auch mit Jugendämtern oder Waffenbehörden. Genau hier liegt aber ein wesentliches Problem. Das



INTERVIEW_ Jan-Hendrik Dietrich

Prof. Dr. Jan-Hendrik Dietrich lehrt an der Hochschule des Bundes in Berlin und der Universität der Bundeswehr München. Mit Prof. Dr. Carlo Masala leitet er das Masterprogramm Intelligence and Security Studies, ist Co-Direktor des Center for Intelligence and Security Studies an der Universität der Bundeswehr München sowie „chercheur invité“ bei SciencesPo Paris. Er ist Autor zahlreicher Publikationen zum Sicherheitsrecht.

KEY MESSAGES

- **Bedrohungen sind entgrenzt:** Extremismus, Spionage und Sabotage greifen ineinander, klare Trennlinien verschwimmen.
- **Das größte Defizit** liegt nicht bei Befugnissen, sondern beim eingeschränkten Informationsaustausch zwischen Behörden.
- **Das informationelle Trennungsprinzip** erschwert operative Gefahrenabwehr und praxisnahe Kooperation erheblich.
- **Europäische Abhängigkeit** von US-Diensten ist strukturell, kann aber nur durch Investitionen und Kooperation reduziert werden.
- **Wehrhafte Demokratie** braucht beides: rechtsstaatliche Grenzen und anpassungsfähige Dienste in veränderten Bedrohungslagen.

Bundesverfassungsgericht hat dem Datenaustausch enge Grenzen gesetzt. Das Gericht nimmt ein informationelles Trennungsprinzip an, das heißt, dass Daten nur im Ausnahmefall ausgetauscht werden dürfen. In der Praxis führt das mitunter zu gewissen Schwierigkeiten. Ich gebe Ihnen ein Beispiel: die nachrichtendienstliche Erkenntnis, dass jemand über einer Bundeswehrkaserne eine Spionagedrohne aufsteigen lassen will, darf derzeit mit der Polizei nicht geteilt werden. Die Strafverfolgung in § 109g StGB ist zu gering, um eine Ausnahme vom Trennungsprinzip zu rechtfertigen. Bevor wir über neue Befugnisse nachdenken, müssen wir vor allem erst einmal für eine optimale Zusammenarbeit unserer Sicherheitsbehörden sorgen. Die Innenministerkonferenz hat sich kürzlich dafür ausgesprochen, die Aufnahme einer Kooperationspflicht beim behördlichen Informationsaustausch in das Grundgesetz prüfen zu lassen. Zu einer Grundgesetzänderung wird es nicht kommen. Das zeigt aber anschaulich, dass es Probleme gibt.

Welche Voraussetzungen braucht es, um besonders die Abhängigkeit von den US-Diensten zu reduzieren?

Es ist richtig, dass Informationen von ausländischen Partnerdiensten oft zur Aufdeckung von terroristischen Anschlagplänen oder Spionageaktivitäten beitragen. Wichtig ist zunächst, dass man versteht, dass das nicht notwendigerweise auf eine Schwäche der deutschen Behörden hinweist. Bei grenzüberschreitenden Bedrohungen gibt es unter den westlichen Diensten durchaus ein „burden sharing“. Manchmal wissen die französischen Dienste mehr, manchmal die britischen. Im Verhältnis zu den amerikanischen Behörden sind

die europäischen Dienste deutlich weniger schlagkräftig. Das ergibt allein der Blick auf Budget und Personalressourcen. Eine Aufkündigung der Zusammenarbeit würde deshalb niemals Sinn machen. Um allerdings politisch nicht erpressbar zu sein, müssen die Europäer viel mehr in ihre Dienste investieren. Auch hier gibt es eine Zeitenwende. Gleichzeitig muss die nachrichtendienstliche Kooperation auf europäischer Ebene verbessert werden. Das ist gar nicht so leicht, weil die EU-Verträge ausdrücklich Belange der „Nationalen Sicherheit“ aus dem europäischen Integrationsprozess exkludieren. Das bedeutet in der Konsequenz, dass die europäische Zusammenarbeit der Nachrichtendienste im Wesentlichen außerhalb der Europäischen Union organisiert werden muss, wenn sich die Verträge nicht ändern.

Machtmaximierung an einer einzigen Stelle innerhalb der Exekutive verhindern. Intra-exekutive Gewaltenteilung könnte man das vielleicht nennen. Außerdem sind die Nachrichtendienste in Deutschland besonders engmaschigen Kontrollen unterworfen. Es gibt bei uns mehr Kontrollorgane als Nachrichtendienste. Für die drei Behörden auf Bundesebene gibt es allein sechs spezifische Kontrolleinrichtungen. Und dabei ist die Kontrolle durch Gerichte und Aufsichtsbehörden gar nicht eingerechnet.

Welche konkrete Funktion haben die deutschen Nachrichtendienste im Rahmen der wehrhaften Demokratie: Sind sie aus Ihrer Sicht primär analytische Frühwarnsysteme oder entwickeln sie sich faktisch zu politischen Abwehrinstrumenten, die selbst an der Grenzziehung des Demokratischen mitwirken?

Ihre Frage spielt aber noch auf eine

„Deutsche Dienste dürfen keine polizeilichen Befugnisse haben.“

Jan-Hendrik Dietrich

Inwieweit prägt die deutsche Geschichte den heutigen Status der deutschen Nachrichtendienste, vor allem auch in rechtlicher Hinsicht?

Sie sprechen Verbrechen von Gestapo und Stasi an. Tatsächlich haben die Lehren aus der Vergangenheit bis heute Einfluss auf die Arbeit der deutschen Nachrichtendienste. Rechtlich drückt sich das zum Beispiel dadurch aus, dass die deutschen Dienste keine polizeilichen Befugnisse haben und keiner polizeilichen Dienststelle angegliedert werden dürfen. Man will dadurch eine

spezielle Facette der Arbeit der Dienste an. Im Grunde fragen Sie: „Wie politisch sind die Verfassungsschutzbehörden?“. Von Links- und Rechtsextremisten wird oft vorgetragen, dass sich der Verfassungsschutz in Deutschland eine Art Deutungshoheit darüber anmaße, was extremistisch sei und was nicht. Das stimmt so nicht. Die Verfassungsschutzbehörden beobachten und dokumentieren Bestrebungen, die sich – mit und ohne Gewalt – gegen die freiheitliche demokratische Grundordnung richten. Das Bundesverfassungsgericht hat in >

ständiger Rechtsprechung klar gemacht, was darunter zu verstehen ist. Die Konkretisierung der fdGO findet sich in allen Verfassungsschutzgesetzen des Bundes und der Länder. Die Verfassungsschutzbehörden beobachten diejenigen, die elementare Grundrechte in Frage stellen, Gerichte und Parlamente nicht anerkennen oder zu gewaltsamen Umstürzen aufrufen. Das machen sie nicht zum Selbstzweck, sondern zur Dokumentation für die Öffentlichkeit. Sie entreißen dabei einigen die Maske der Biederkeit. Es ist naheliegend, dass das nicht jedem passt.

Verändert sich die Rolle der Nachrichtendienste qualitativ, wenn der Staat sich nicht mehr nur präventiv, sondern existenziell bedroht sieht?

Das ist sehr wahrscheinlich. Über unserer Sicherheitsarchitektur liegt immer noch die Patina des Ost-West-Konflikts und transatlantischer Sicherheitsgarantien. Der Ukraine-Krieg und die jüngsten US-amerikanischen Sicherheitsstrategien haben eine doppelte Zeitenwende markiert. Daraus folgt, dass Krieg in Europa nicht länger ein abstraktes Gedankenspiel ist. Für die Nachrichtendienste ändern sich dadurch einige Szenarien ihres Einsatzes. In einem Verteidigungsfall wird zum Beispiel der BND sicherlich weniger die organisierte Kriminalität und internationale Proliferation beobachten. Er wird stattdessen vor allem seine Funktion als militärischer Nachrichtendienst wahrnehmen. Hier wird sich vermutlich schon ein Perspektivenwechsel vollziehen. Der Fokus wird sich zunehmend von strategischer intelligence auf tactical intelligence verlagern. Das allein wird aber nicht reichen. Man wird dem Dienst eigene operative Befugnisse geben müssen.

Alles andere wäre naiv. Wir sprechen zum Beispiel über Sabotageaktionen hinter feindlichen Linien oder aktive Cyberoperationen. Aus dem reinen Nachrichtendienst wird unter diesen Bedingungen ein operativer Geheimdienst.

Der Staatsrechtler Hans Kelsen warnte einst davor, die Demokratie durch inhaltliche Abwehrmaßnahmen zu schützen, sein Kollege Karl Loewenstein befand eben das für notwendig im Sinne einer „militant democracy“. Welche der beiden Positionen ist aus Ihrer Sicht im Grundgesetz stärker angelegt? Wo besteht bis heute eine ungelöste Spannung?

Kelsen hat vielleicht auf den ersten Blick ein logisches Argument auf seiner Seite. Eine Demokratie, die sich – vielleicht sogar nur mit Gewalt – gegen den Willen der Mehrheit behauptet, kann keine Demokratie mehr sein. Das ist sicher richtig. Aber bei Licht betrachtet ist so eine Entwicklung doch eher das, was Juristen als „pathologischen Lehrbuchfall“ ansehen würden. Das ist ein theoretisch denkbarer Fall, der in der Realität wenig wahrscheinlich ist. Wenn in einem Bundesland 35% der Wähler eine gesichert extremistische Partei wählen, haben noch immer 65% diese Partei nicht gewählt. Das Grundgesetz hat aus diesem Grunde Sicherungen von Demokratie und Rechtsstaat angelegt. Beides unterliegt nach Art. 79 Absatz 3 einer sogenannten Ewigkeitsgarantie. Gelangen Extremisten auf legalem Wege an die Macht, können sie die Verfassung in dieser Hinsicht niemals ändern. Außerdem – und das ist ein sehr starkes Statement der Wehrhaftigkeit – enthält Art. 20 Abs. 3 des Grundgesetzes ein individuelles Recht zum Schutz der Verfassung. Dort heißt es: „Gegen jeden, der es unternimmt,

diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist“.

Carlo Schmid sprach in der 2. Sitzung des Parlamentarischen Rates am 8.9.1948 vom „Mut zur Intoleranz“ gegenüber Feinden der Demokratie. Ist diese Intoleranz heute rechtlich als Ausnahmeinstrument zu verstehen – oder als konstitutives Element demokratischer Selbstverteidigung, das auch präventive nachrichtendienstliche Maßnahmen legitimiert?

Ich will Ihnen mit einem Goebbels-Zitat antworten. Josef Goebbels hat 1928 einmal gesagt: „Wir gehen in den Reichstag hinein, um uns im Waffensaal der Demokratie mit deren eigenen Waffen zu versorgen. Wir werden Reichstagsabgeordnete, um die Weimarer Gesinnung mit ihrer eigenen Unterstützung lahmzulegen“. Das Grundgesetz hat daraus seine Lehren gezogen. Die Verfassung und ihre Werte müssen gegenüber ihren Feinden aktiv verteidigt werden. Deshalb ist ein administrativer Verfassungsschutz heute verfassungsrechtlich institutionell gesichert. Art. 73 und Art. 87 des Grundgesetzes gehen davon aus, dass Bund und Länder Behörden zum Zwecke des Verfassungsschutzes einrichten, die eng zusammenarbeiten. Die wehrhafte Demokratie findet darin einen Ausdruck. So sieht es auch das Bundesverfassungsgericht. Wer immer im ganz linken und im ganz rechten Lager die Verfassungsschutzbehörden abschaffen will, sollte vorher in die Verfassung schauen.

Ein mögliches AfD-Verbot wird kontrovers diskutiert. Wäre ein solches Verbot aus Sicht der wehrhaften Demokratie Ausdruck staatlicher Selbstbehauptung oder birgt es die Gefahr, die politische Legitimität von Verfassungsschutz und demokratischer Ordnung zu beschädigen?

>

Ein Parteiverbot ist auf jeden Fall ultima ratio des wehrhaften Verfassungsstaates. In der Geschichte der Bundesrepublik hat es aus gutem Grunde bisher nur wenige Parteiverbote gegeben. Zur Demokratie gehört, andere Meinungen anzuhören und auch auszuhalten. Das Bundesverfassungsgericht hat den Flaschenhals für Parteiverbote in den letzten Jahren sehr eng gemacht. Ob die vorliegenden Informationen über die AfD ausreichen, um ein Parteiverbot zu rechtfertigen, darf wenigstens als unsicher gelten. Ein gescheiterter Verbotsantrag würde meines Erachtens die Verfassungsschutzbehörden nicht notwendigerweise beschädigen.

Die Antragsstellung ist eine politische Entscheidung, die von Bundestag, Bundesrat oder Bundesregierung zu treffen ist. Die Antragsteller müssen den Antrag begründen. Erst in diesem Zusammenhang würden Erkenntnisse der Verfassungsschutzbehörden eine Rolle spielen. Die Ämter erstellen keine Gutachten für Parteiverbote. Sie dokumentieren nur entlang ihres gesetzlichen Auftrags, ob sich eine Bestrebung im Rahmen der freiheitlichen demokratischen Grundordnung unterwegs ist. Bisher haben sich entsprechende Einordnungen des Verfassungsschutzes als gerichtsfest erwiesen. In Bezug auf die Einordnung als „rechtsextremistischer Verdachtsfall“ hat die AfD bislang vor den Verwaltungsgerichten verloren.

Wäre es nach § 3 Abs. 1 BVerfSchG bzw. § 1 Abs. 2 BNDG rechtlich zulässig, wenn deutsche Nachrichtendienste Bestrebungen der USA beobachten, die auf eine aktive Unterstützung der AfD zielen?

Der Verfassungsschutz beobachtet die AfD als gesichert extremistische Bestrebung. Vom Umfang der Beobach-

tung ist auch umfasst, wer die Partei auf welche Weise unterstützt. Von Interesse ist zum Beispiel, woher finanzielle Mittel kommen. Aber auch öffentliche Äußerungen von Unterstützern werden in den Blick genommen. Das sind alles Mosaiksteine, die ein Gesamtbild der Beobachtungsbedürftigkeit ergeben. Es spielt dabei grundsätzlich erst einmal keine Rolle, woher die Unterstützung kommt. Dokumentiert und analysiert wird sie unabhängig davon, ob sie aus Russland, den USA oder von sonst woher stammt.

Beim BND sind die Vorzeichen etwas anders. Der BND sammelt Informationen von außen- oder sicherheitspolitischer Bedeutung mit Bezug zur Bundesrepublik Deutschland. Das kann auch beinhalten, welche ausländischen Staaten oder Organisationen sich offen oder verdeckt in Deutschland politisch engagieren.

einordnen, sachlich begründen und dokumentieren, wenn eine Bestrebung elementare Werte unserer Verfassung in Frage stellt. Das tun sie auch noch immer. Nur wer liest sie? Aus aktuellen Untersuchungen zum Medienkonsumverhalten wissen wir, dass junge Menschen ihre Informationen oft aus sozialen Medien beziehen. Hier fehlt teilweise die Gatekeeper-Funktion von Journalisten.

Viele bleiben in Internetblasen hängen und werden verführbar. Insofern gebe ich Ihnen Recht, dass der Schutz unserer Demokratie bereits damit beginnt, Jugendlichen Medienkompetenz beizubringen. Resilienz geht dann vor Wehrhaftigkeit. Gleichzeitig muss aber auch der wehrhafte Verfassungsstaat neue Formate finden, um z.B. die Gen Z zu erreichen. Hochglanzbroschüren oder markige Sprüche helfen nicht weiter, genauso wenig übrigens wie ideologi-

„Hochglanzbroschüren oder markige Sprüche helfen nicht weiter.“

Jan-Hendrik Dietrich

Ist der klassische Rahmen der wehrhaften Demokratie für heutige Bedrohungslagen noch ausreichend? Müsste man angesichts hybrider Bedrohungen und Radikalisierung im Netz nicht eher von einer „resilienten Demokratie“ sprechen – und liegt darin möglicherweise auch eine europäische Perspektive?

Richtig ist, dass einige traditionelle Mittel der wehrhaften Demokratie in der Informationsgesellschaft zu kurz greifen. Nehmen Sie z.B. die Verfassungsschutzberichte. Sie sollen fachlich

sche Verböhrtheit, wenn etwa Mitarbeitern von Verfassungsschutzbehörden, Polizei und Bundeswehr der Besuch von Schulen verweigert wird. Innerhalb der Europäischen Union ist zumindest die Verletzlichkeit der westlichen Demokratie erkannt worden. Die EU-Kommission hat Ende des letzten Jahres einen „Europäischen Schutzschild für die Demokratie“ vorgestellt. Bis die Maßnahmen greifen, wird es noch etwas dauern. Aber das geht in die richtige Richtung. ■

Vom Protest zur Bedrohung?

Zwischen legitimer Kritik und Extremismus verläuft keine klare Linie. Wie Nachrichtendienste in Europa neue Protestphänomene vermessen und dabei Sicherheit und Freiheit auszutarieren suchen.

„Ausgangspunkt für das neue Beobachtungsobjekt“, so erläuterte Thomas Haldenwang, damaliger Präsident des Bundesamtes für Verfassungsschutz (BfV) anlässlich der Vorstellung des Verfassungsschutzberichts 2021, „war die sehr heterogene Protest-Szene gegen die staatlichen Maßnahmen zur Bekämpfung der Corona-Pandemie, wo Verschwörungstheorien, das Schüren von antisemitischen Ressentiments und eine massive Gewaltbereitschaft gegen Polizei- und Ordnungsbehörden einen fruchtbaren Boden vorfanden.“¹

Die Einführung dieses „neuen Beobachtungsobjekts“ verweist auf zwei Problemkomplexe: Erstens die Schwierigkeiten für die Nachrichtendienste, die heterogenen Strömungen der Corona-Proteste auf einen Begriff zu bringen. Zweitens die Gratwanderung, normale Bürgerinnen und Bürger sowohl als Bedrohung und als Schutzobjekt zu sehen. Denn es handelte sich bei der „heterogenen Protest-Szene“ um Bewegungen, die sich vor allem aus der gesellschaftlichen Mitte speisten, an denen also „ganz normale“ Bürger:innen teilnahmen, die in dieser Zahl und Schnelligkeit kaum je ins Visier der deutschen Nachrichtendienste geraten waren.

Wie sollen Nachrichtendienste in liberalen Demokratien zukünftig mit Protestbewegungen umgehen, die breite Teile einer Gesellschaft erfolgreich mobilisieren – und die teilweise in Extremismus oder Gewalt umschlagen? Das ist keine Frage für Deutschland allein, auch in anderen europäischen Ländern gab es Proteste gegen die Maßnahmen zur Bekämpfung des Corona-Virus. Wie können die nationalen Erfahrungen für eine europäische Zusammenarbeit genutzt werden? >

¹ <https://www.verfassungsschutz.de/SharedDocs/statements/DE/2022/2022-06-07-haldenwang-vorstellung-des-verfassungsschutzberichts-2021.html> (9.1.26).

TEXT_ Eva Herschinger

Prof. Eva Herschinger ist Professorin für Sicherheitsforschung und Leiterin des Forschungsbereichs Sicherheit und Intelligence am Center for Intelligence and Security Studies der Universität der Bundeswehr München.

KEY MESSAGES

- **Die Corona-Proteste** zwangen Nachrichtendienste, neue Kategorien jenseits klassischer Extremismusbegriffe zu entwickeln.
- **Bewegungen** aus der gesellschaftlichen Mitte stellen eine besondere Herausforderung dar, weil Protest und Bedrohung ineinander greifen können.
- **Die Kategorie der „Delegitimierung des Staates“** zeigt die Schwierigkeit, Kritik an Regierung, Staat und Demokratie trennscharf zu unterscheiden.
- **Protestmilieus** bleiben meist gewaltfrei, können aber durch Desinformation und Extremisten partiell radikalisiert werden.
- **Für die Zukunft** braucht es europäische Abstimmung, flexible Analyseansätze und besondere Sensibilität für demokratische Grundrechte.

PROTESTE: BEOBACHTUNGSOBJEKT DER NACHRICHTENDIENSTE

Die Proteste gegen die Corona-Maßnahmen markierten in vielen Ländern eine Zäsur. In Deutschland blieben sie vielfach friedlich, gipfelten aber auch in aggressiven Aktionen – man denke etwa an den versuchten Sturm auf den Reichstag im August 2020. Das BfV sah sich mit einer Protestbewegung konfrontiert, die aus der gesellschaftlichen Mitte kam: Menschen, die zuvor politisch kaum aktiv waren – „Herr und Frau Schmidt“ – protestierten Seite an Seite mit Impfgegner:innen und Verschwörungsgläubigen, Esoteriker:innen und Rechtsextremist:innen. Aus Sicht der Nachrichtendienste entstand eine neue, gegen den Staat gerichtete Szene, die sich nicht in bestehende Extremismus-Kategorien (Rechts-, Links-, oder religiöser Extremismus) einordnen ließ. Das BfV reagierte im April 2021 mit der Einrichtung des Phänomenbereiches „Verfassungsschutzrelevante Delegitimierung des Staates“.

Nachrichtendienste in anderen westlichen Ländern verwendeten ähnliche Bezeichnungen, um die Protestbewegungen zu beschreiben. So nutzt der niederländische Nachrichtendienst „Anti-institutioneller Extremismus“, in den USA ist „regierungsfeindlicher Extremismus“ der gebräuchliche Begriff, Schweden entschied sich für „Anti-Regierungsrhetorik“ und „Anti-Establishment-Narrative“, während auf europäischer Ebene bspw. Europol von Gruppen spricht, die sich durch ihre „Anti-Regierung-, Anti-System- und Anti-Institutionen“-Haltung auszeichnen.² Der Bezug zu Corona-Krise ist dabei zwar Ausgangspunkt, aber kein inhaltlich fester Bezugspunkt.

DIE HERAUSFORDERUNG DER DEFINITION DER „DELEGITIMIERER:INNEN“

Mit der neuen Kategorie erfasst das BfV Personen und Gruppen, die durch ihr Verhalten die Funktionsfähigkeit und Legitimität des Staates erschüttern wollen, etwa indem sie demokratische Entscheidungsprozesse und Institutionen verächtlich machen oder dazu aufrufen, behördliche Anordnungen zu ignorieren. Dies, so das BfV, widerspricht den „elementaren Verfassungsgrundsätzen wie Demokratie oder Rechtsstaatlichkeit“.³ Angesichts der Heterogenität der Protestszene identifizierte das BfV die kategorische Ablehnung der bestehenden Staatsordnung als

das ideologisch verbindende Element. Polizei sowie Politiker:innen und Wissenschaftler:innen, die für die staatlichen Maßnahmen zur Eindämmung des Virus eintraten, wurden nun zum Feindbild.

Gewalttätige Aktionen gegen diese wurden als legitime Akte des Widerstands stilisiert und befürwortet – man denke hier u.a. an die geplante Entführung des damaligen Gesundheitsministers Karl Lauterbach. Kritiker:innen bemängelten, dass das BfV hier Kritik an der Regierung mit Kritik am Rechtsstaat und der Demokratie vermenge, während man Rechtsextremist:innen in der Masse der Protestierenden verschwimmen lasse.⁴ Auch in anderen Ländern war die Abgrenzung schwierig. Ein Beispiel: In den Niederlanden sprach der Nachrichtendienst AIVD von „anti-governmental extremism“, eine Bezeichnung, die bereits vor der Corona-Pandemie existierte. Nach 2022 änderte man die Beschreibung in „anti-institutional extremism“, nachdem neben der Regierung auch Institutionen wie Polizeien und Medien in den Fokus der Bewegungen gerieten.

Die Heterogenität der Szene war und ist jedoch nicht die einzige Herausforderung für die Nachrichtendienste in Europa, wenn es um die Definition geht. Auch inhaltlich blieben die Proteste dynamisch – wenn auch mit abnehmendem Erfolg. So verlor das Thema Corona mit der weitgehenden Rücknahme der staatlichen Maßnahmen zur Bekämpfung der Pandemie im Jahr 2022 viel von seinem Mobilisierungspotenzial. Mit deutlich geringerer Agitationskraft dominieren nun Themen wie Inflation und Energiepreise oder die Ablehnung der Maßnahmen zur Bekämpfung des Klimawandels sowie die Auswirkungen des russischen Angriffskrieges gegen die Ukraine.

Im Verlauf des Jahres 2025 wurde klar, dass die neue Kategorie an Bedeutung verliert. So hat Sachsen entschieden, die Kategorie ab 2026 nicht weiter zu nutzen. Die Akteure verschwinden dadurch nicht aus dem Visier der Nachrichtendienste: Personen, die demokratiefeindlich agieren, werden weiterhin beobachtet, nur eben in die klassischen Phänomenbereiche eingeordnet.

GRATWANDERUNG ZWISCHEN NORMALEN BÜRGER:INNEN UND EXTREMIST:INNEN

Hinter der Debatte um Definitionen steht ein weiteres Problem: die Gratwanderung zwischen der Behandlung normaler Bür- >

² https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf (22.1.26).

³ Alle BfV-Zitate stammen von der folgenden Website: https://www.verfassungsschutz.de/DE/themen/verfassungsschutzrelevante-delegitimierung-des-staates/begriff-und-erscheinungsformen/begriff-und-erscheinungsformen_artikel.html#doc1260196bodyText1 (9.1.26).

⁴ Siehe u.a. <https://www.lto.de/recht/hintergruende/h/verfassungsschutz-kritik-extremismus-delegitimierung-verfassung-bericht> (9.1.26).

ger als Sicherheitsrisiko und ihrem Schutz als Träger:innen demokratischer Rechte. In Demokratien ist Protest legitimer Ausdruck von Meinungsfreiheit und politischer Teilhabe. Doch was, wenn eine Vielzahl an „normalen“ Bürger:innen innerhalb eines legitimen Protests plötzlich gewalttätige Positionen unterstützen, und/oder Ansinnen an der Schwelle zum Extremismus? Es geht um die Frage, was normal und schützenswert, was anormal und bedrohlich ist – und wie der Staat agieren soll, wenn beides in eines fällt, wenn Bürger:innen, die man schützen soll, plötzlich eine Bedrohung darstellen.

„Die Beobachtung ‚normaler Bürger:innen‘ kann leicht zum Vorwurf der Überwachung legitimer Opposition führen.“

Eva Herschinger

Die Berichte des Verfassungsschutzes seit 2021 spiegeln diese Herausforderung wider. Einerseits wird betont, es handle sich um legitimen Protest besorgter Bürger:innen, also um etwas Normales in einer Demokratie. Andererseits konstatiert das BfV, dass ein Teil dieser Bewegung die „Grenze zu verfassungsfeindlichen Bestrebungen“ überschritten habe. Damit rücken manch ein Herr und manch eine Frau Schmidt in den Bereich des „Anormalen“, der wiederum sicherheitsbehördlicher Beobachtung unterliegt.

In Anlehnung an den französischen Philosophen Michel Foucault kann man hier von einem Akt der Klassifizierung sprechen: Durch die Ziehung einer Grenze zwischen „normalem“ und „anormalem“ Protest erschaffen die Berichte eine neue Kategorie, die diese neuen Beobachtungsobjekte aus dem Bereich des Normalen herauslöst und ins Feld des Anormalen rückt. Was vor dieser Grenze liegt – normaler Protest – ist schützenswert. Was dahinter liegt – delegitimierende, demokratiefeindliche Agitation – ist bedrohlich. Ein zweigeteilter Diskursraum entsteht: Hier

die Hegemonie dessen, was als normal gilt – konstruktive Kritik, friedlicher Protest –, dort das Stigma des Anormalen – verfassungsfeindliche Umtriebe, verschwörungsideologische Radikalisierung. Dass in der Praxis die Abgrenzung aufgrund der Dynamik und Heterogenität der Proteste von einer großen Unschärfe gekennzeichnet ist, darauf verweisen die Kritiker:innen.

Für die Nachrichtendienste bedeutet diese Gratwanderung, höchste Sorgfalt walten zu lassen. Die Beobachtung „normaler Bürger:innen“ ist ein sensibles Unterfangen, das leicht zum Vorwurf der Überwachung legitimer Opposition führen kann. Gleichzeitig haben Beispiele gezeigt, dass echte Gefahren von solchen heterogenen Bewegungen ausgehen können; vor allem, wenn extremistische Gruppen versuchen, die Proteste für sich zu instrumentalisieren. So bestätigt Europol in seinem Terrorismuslagebericht, dass die Mehrheit der anti-Regierungs-/anti-System-Gruppierungen gewaltfrei bleibt, aber eine Minderheit Gewalt rechtfertigt oder ausübt. Dieser gewaltbereite Kern kann sich aus zunächst friedlichen Protestnetzwerken herausbilden, befeuert durch online Desinformation und Verschwörungserzählungen. Einige Individuen haben sich bis hin zur Planung von Terrorakten radikalisiert, wie vereitelte Anschlägepläne in verschiedenen Ländern zeigen.⁵

POST-CORONA: ZUKÜNFTIGE HERAUSFORDERUNGEN FÜR DIE NACHRICHTENDIENSTE

Die Erfahrungen der letzten Jahre geben einen Ausblick auf die zukünftigen Herausforderungen für Nachrichtendienste in liberalen Demokratien. Einerseits stellt sich angesichts der zeitlichen Gebundenheit der Corona-Proteste natürlich die Frage, wie dauerhaft dieses Phänomen ist. Andererseits könnten ähnliche Dynamiken – ein plötzlicher Schulterchluss heterogener Unzufriedener, getrieben durch digitale Vernetzung und Desinformation – jederzeit wieder auftreten.

Die nächste große Krise (sei es eine Pandemie, wirtschaftliche Not oder ein breiter gesellschaftlicher Konflikt) könnte erneut zu Protesten breiter Bevölkerungsschichten führen, der auch wieder von Extremist:innen oder feindlichen ausländischen Akteuren unterwandert werden könnte. Und Bürger:innen, die sich einmal als Beobachtungsobjekt gefühlt haben, bleiben eher misstrauisch gegenüber staatlichen Institutionen und sind auch leichter wieder mobilisierbar. Zum anderen sollte die europäische Ebene verstärkt in den Blick kommen. Europol und ande- >

⁵ https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf (22.1.26).

re EU-Organen haben das Thema erkannt und Austauschplattformen geschaffen, etwa Fachkonferenzen zu „Anti-Government Extremism“ und Trainingsprogramme zum Umgang mit Anti-System-Bewegungen.

Es bedarf also in einer zukünftigen europäischen Intelligence-Architektur, Austausch und Abstimmung von Definitionsansätzen, um länderübergreifenden extremistischen Narrativen effektiver zu begegnen. Schließlich agieren auch die extremistischen Ideolog:innen vernetzt über Grenzen hinweg: Verschwörungsmethoden sind online überall und jederzeit verfügbar, und Akteure wie die QAnon-Bewegung oder russische Desinformationskampagnen beeinflussen Protestmilieus europaweit. Eine abgestimmte europäische Reaktion könnte helfen, Trends frühzeitig zu erkennen und Gegenstrategien zu entwickeln.

Allerdings operieren die Nachrichtendienste in Europa bisher im nationalen Rahmen, eng gebunden an die jeweiligen Rechtsordnungen und demokratischen Kontrollmechanismen der Staaten. Dennoch wäre zumindest ein vereinheitlichtes Begriffsverständnis in Europa hilfreich und ein erster Schritt in eine gemeinsame Richtung: Wenn alle von der gleichen Art Bedrohung reden, kann man auch gezielter vereint dagegen vorgehen.

Die Erfahrungen in und nach der Pandemie liefern für diese Zusammenarbeit wichtige *lessons learned*: Angesichts von dynamischen, gesellschaftlich breiten Protestphänomenen brauchen Nachrichtendienste flexible Wege, um die Sicherheit und die offenen Grundrechte der Gesellschaft zu bewahren. Ein Weg ist die europäische Zusammenarbeit. Dieses Navigieren zwischen Sicherheit und Freiheit wird die Zukunft der Nachrichtendienstarbeit in Europa entscheidend prägen. ■

„Einfach machen!“

Zwischen Behörden, politischer Führung und europäischer Zusammenarbeit: Die Politikwissenschaftlerin Anna Daun analysiert, was Nachrichtendienste leisten können – und was sie in Deutschland und Europa daran hindert, strategisch wirksam zu sein.



„Nachrichtendienste schützen nicht die Demokratie an sich, sondern die staatliche Souveränität.“

Anna Daun

Anna Daun, inwiefern schützen Nachrichtendienste unsere Demokratie?

Anna Daun: Nachrichtendienste schützen nicht die Demokratie an sich, sondern die staatliche Souveränität. Sie sichern den Raum, in dem Demokratie stattfinden kann. Innerhalb dieses geschützten Raums entfalten sich politische Kultur, Debatten und demokratische Prozesse. In diesem Sinne leisten die Dienste einen wichtigen Beitrag, ohne selbst demokratische Akteure zu sein.

Welche Art von Nachrichten- oder Geheimdienst würden Sie sich für Deutschland und Europa insgesamt wünschen?

Da muss man erst unterscheiden zwischen Deutschland und Europa. Wenn wir bei Deutschland anfangen, würde ich die grundsätzliche Trennung zwischen Inlands- und Auslandsdienst beibehalten. Das ist sinnvoll. Beim Inlandsdienst würde ich mir wünschen, dass er sich wirklich auf das Notwendigste beschränkt. Weniger Quantität, dafür mehr Qualität. Also nicht alles machen, sondern das, was wirklich relevant ist, dann aber auch konsequent und gut. Und dabei auch etwas risikobereiter, als wir das in der Vergangenheit gesehen haben.

Was ist das „Notwendigste“ für Sie?

In der Vergangenheit hatte ich oft den Eindruck, dass sehr viel gesammelt wurde, viele Quellen, viele Berichte, aber bei zentralen Fällen wie dem NSU oder dem Attentäter Anis Amri ist man

nicht an die entscheidenden Informationen gekommen. Das war qualitativ einfach nicht überzeugend. Der Verfassungsschutz sollte sich darauf konzentrieren, echte Bedrohungen der Demokratie zu identifizieren.

Bedeutet das, die Materialsammlung etwa zur AfD gehört aus Ihrer Sicht nicht dazu?

Das habe ich so nicht gesagt. Es gibt ein reales Problem mit demokratischen Grundwerten in unserer Gesellschaft. Aber nicht jeder, der sich undemokratisch äußert, ist automatisch ein Fall für den Verfassungsschutz. Das ist ein gesamtgesellschaftliches Problem, ein politisches, auch ein bildungspolitisches. Aufgabe des Verfassungsschutzes ist es, organisierte Bestrebungen zu erkennen, die darauf abzielen, das System aktiv zu überwinden.

Also: Fokus auf organisierte Strukturen?

Genau. Auf gewaltbereite Rechtsextremisten, Putschfantasien, staatsfeindliche Netzwerke, aber vor allem auch auf Spionageabwehr. Gerade der Einfluss externer Akteure nimmt zu. Wenn es Verbindungen zu ausländischen Mächten gibt, die unsere Grundordnung gezielt destabilisieren wollen, dann ist das klar ein Fall für den Verfassungsschutz. Aber eben beschränkt auf diese Zirkel.

Und was ist mit extremistischen Aussagen im Netz?

So problematisch das alles ist, das ist nicht primär Aufgabe des Verfassungsschutzes. Vieles fällt eher in den

INTERVIEW_ Anna Daun

Prof. Dr. Anna Daun ist Professorin für Politikwissenschaft an der Hochschule für Wirtschaft und Recht (HWR) in Berlin. Sie unterrichtet Sicherheitsthemen in den Studiengängen gehobener Polizeivollzugsdienst (gehPVD) und Sicherheitsmanagement, außerdem ist sie stellvertretende Direktorin des Forschungsinstituts für öffentliche und private Sicherheit (FÖPS).

KEY MESSAGES

→ **Nachrichtendienste schützen** staatliche Souveränität und damit den Raum demokratischer Politik, nicht Demokratie selbst.

→ **Der Verfassungsschutz** sollte sich auf organisierte, reale Bedrohungen konzentrieren – weniger Quantität, mehr analytische Qualität.

→ **Deutschlands Intelligence-Kultur** ist historisch belastet und strategisch unterentwickelt, geprägt von Risikoaversion und schwacher Fehlerkultur.

→ **Wirksame Intelligence** braucht politische Führung, klare Prioritäten und interdisziplinäre Analyse jenseits klassischer Behördenbiografien.

→ **Europas sicherheitspolitische Zukunft** erfordert engere Intelligence-Zusammenarbeit – bis hin zu gemeinsamen, arbeitsteiligen Strukturen.

Bereich der Polizei oder der politischen Auseinandersetzung. Der Verfassungsschutz sollte mit seinen besonderen Mitteln tief in die relevanten Netzwerke vordringen, dort Quellen haben, wo die Knotenpunkte sind.

Welche Rolle sollte der Auslandsdienst spielen, also der BND?

Beim Auslandsdienst wünsche ich mir vor allem, dass er politisch gut geführt wird. Also dass klare Prioritäten gesetzt werden. Der Dienst muss nicht überall sein und alles können. Es braucht strategische Schwerpunktsetzungen, an denen sich die Arbeit ausrichtet. Und in diesen Feldern sollte der Auslandsdienst dann auch wirklich gut sein. Man muss nicht global alles selbst abdecken, dafür gibt es Partnerdienste, OSINT und auch wissenschaftliche Einrichtungen wie etwa Thinktanks.

In Deutschland hat man oft den Eindruck, dass die Diskussion über die Dienste auf die Frage der Befugnisse und der Kontrolle reduziert wird. Sollte man die Debatte nicht viel politischer führen? Im Sinne der Frage: Was wollen wir eigentlich mit diesen Diensten?

Ja, das denke ich auf jeden Fall. In Deutschland war dieses Feld lange aus der strategischen Kultur ausgeblendet. Über Sicherheit und Verteidigung wurde gesprochen, aber Nachrichtendienste waren eher ein Thema, über das man nicht gern geredet hat. Es haben sich auch vergleichsweise wenige Menschen damit beschäftigt. Dieser Bereich hat in unserer strategischen Kultur lange gefehlt.

Warum war das so?

Das kann man historisch erklären. Deutschland ist ein relativ junger Nationalstaat. Der Blick war lange stärker nach innen gerichtet als nach außen, anders als bei älteren europäischen

Nationen mit kolonialer Geschichte. Dann kamen die schlechten Erfahrungen des Nationalsozialismus und später der Stasi hinzu. Diese Geschichte hat einen langen Schatten auf alles geworfen, was mit Geheimdiensten zu tun hat. Wahrscheinlich erklärt das, warum man sich damit so schwergetan hat.

exklusives Problem der Nachrichtendienste, sondern Teil der deutschen Behördenkultur insgesamt. Es fehlt ein konstruktiver Umgang mit Fehlern. Sehr viel Energie wird darauf verwendet, bloß keine Fehler zu machen, statt das eigentliche Problem in den Blick zu nehmen.

„Im internationalen Vergleich hatte Intelligence in Deutschland lange wenig Prestige.“

Anna Daun

Auch die Politik?

Im internationalen Vergleich hatte Intelligence in Deutschland lange wenig Prestige. Anders als in den USA oder Großbritannien fehlte eine ausgeprägte Intelligence Community. Viele Mitarbeitende fühlten sich geringgeschätzt, Kanzler äußerten sich abfällig, auch in der Wissenschaft war das Thema kaum präsent. Es gab wenig populärkulturelle Auseinandersetzung, keine starke Tradition von Spionageromanen, kaum öffentliche Figuren aus diesem Bereich. Man bemüht sich inzwischen, das zu ändern. Die Dienste sind sichtbarer geworden, schauen Sie sich das schicke und riesige Gebäude des BND in Berlin Mitte an. Aber lange wurde Intelligence kulturell stiefmütterlich behandelt.

Wie würden Sie die deutsche „Intelligence-Kultur“ näher beschreiben?

Da gibt es mehrere Ebenen. Zunächst einmal die interne Ebene, also die bürokratische Kultur innerhalb der Dienste. Da sehe ich beispielsweise ein Problem mit der Fehlerkultur. Das ist aber kein

Nachrichtendienste sind ja letztlich auch Behörden.

Genau. Und diese Logik wirkt dort genauso. Es gibt eine starke Angst, rechtlich oder hierarchisch anzuecken. Das prägt Entscheidungen. Verstärkt wird das durch das große Gewicht von Juristen in den Behörden, was angesichts der rechtlichen Fallstricke verständlich ist, aber dazu führt, dass Risikovermeidung oft wichtiger wird als Wirksamkeit.

Welche Art von Interdisziplinarität wäre aus Ihrer Sicht wünschenswert?

Dienste sind natürlich arbeitsteilig organisiert, mit Ingenieuren, IT-Fachleuten, Analysten. Aber gerade im analytischen Bereich wäre es sehr wünschenswert, Menschen mit sehr unterschiedlichen Erfahrungshintergründen einzubeziehen. Also nicht nur Juristen oder Verwaltungswissenschaftler, die in klassischen Behördenkarrieren sozialisiert sind. Unterschiedliche Biografien, unterschiedliche Disziplinen, auch Quereinsteiger. Das halte ich für wichtig. >

An welche Disziplinen denken Sie konkret?

Zum Beispiel Philosophen. Menschen, die Gegenthesen formulieren können, die nicht nur angepasst denken. Selbstbewusste, intellektuell unabhängige Personen, die nicht nur reproduzieren, was erwartet wird. Vielfalt an Perspektiven ist zentral für gute Analyse.

Wie beobachten Sie das Zusammenspiel zwischen Diensten und Politik?

Öffentlich dominierte lange Desinteresse oder Verachtung, von Adenauer über Kohl bis Schmidt. Ob das stets echtes Desinteresse war, ist von außen schwer zu beurteilen. Oft heißt es, die Dienste hätten versagt oder nicht gewarnt, etwa beim Mauerfall oder anderen Krisen. Zugleich beklagen die Dienste, dass ihre Hinweise ignoriert worden seien. Da gibt es eine gegenseitige Zuschreibung von Verantwortung. Ob intern mehr Austausch stattfand, bleibt offen.

Nehmen wir beispielsweise die Fehleinschätzungen des BND zur russischen Invasion in der Ukraine. Was folgt daraus institutionell?

International zeigt sich ein ähnliches Muster: Versagt ein Dienst, folgen Analyse und mehr Ressourcen und Befugnisse. Das ist ein bürokratischer Automatismus, das kann man seit 9/11 sehen. Es gibt mehr Budget, mehr Befugnisse, aber auch stärkere Kontrolle, die dann selbst wieder Teil des Geheimen wird. Das Parlamentarische Kontrollgremium ist umso weniger öffentlich, je mehr es weiß. Es rückt damit näher an die Logik des Geheimen heran.

Muss eine Demokratie akzeptieren, dass ein Geheimdienst nie vollständig kontrollierbar ist?

Geheimdienste müssen kontrolliert werden, da sie Instrumente der Exekutive sind. Zugleich ist auch die Exekutive

parlamentarisch zu kontrollieren. Öffentliche Transparenz ist dabei kaum möglich, Kontrolle bleibt begrenzt. Innerhalb der Exekutive wirkt sie relativ effektiv, stößt aber am Kernbereich exekutiver Eigenverantwortung an reale Grenzen.

Ist Intelligence aus Ihrer Sicht eine exklusiv staatliche Aufgabe oder können Sie sich neue Formen von Partnerschaften mit privaten Akteuren vorstellen?

Intelligence im engeren Sinne produziert exklusives Wissen für Entscheidungsträger, das auch geheim ist. Das ist erst einmal eine staatliche Aufgabe. Natürlich gibt es Thinktanks und private Akteure, die Analysen liefern, aber das ist etwas anderes als nachrichtendienstliche Intelligence im engeren Sinn.

schen, dass wir uns in diese Richtung entwickeln.

Wäre das für Sie ein Projekt innerhalb der EU oder außerhalb?

Das muss politisch gewollt sein und schrittweise wachsen. Ob es formal ein EU-Projekt ist oder außerhalb der bestehenden Strukturen entsteht, ist zweitrangig. Solche Strukturen entstehen letztlich durch politische Fakten, nicht nur durch institutionelle Prozeduren.

Man könnte sich vorstellen, dass sich etwa Briten, Franzosen und Deutsche zusammenschließen, wie beim Abkommen zum Informationsaustausch „Three Eyes“ (TEYE).

Ja, genau: einfach machen. Angesichts der Lage ist das der einzige realistische Weg. Die Staaten, die das wollen, müs-

„Angesichts der geopolitischen Lage sollte Europa enger zusammenwachsen, auch in der Verteidigung.“

Anna Daun

Wie stehen Sie zur Idee eines europäischen Geheimdienstes?

Das ist eine spannende Frage. Intelligence ist grundsätzlich eine Funktion von Staatlichkeit, die aber nicht zwingend national organisiert sein muss. Angesichts der geopolitischen Lage sollte Europa enger zusammenwachsen, auch in der Verteidigung. Nationale Alleingänge greifen zu kurz. Da Intelligence eng mit Verteidigung verbunden ist, ist eine europäische Verteidigungsstruktur ohne gemeinsame Intelligence kaum vorstellbar. Ich würde mir wün-

sen vorangehen. Es gibt bereits enge europäische Kooperationen im Intelligence-Bereich, aber echte Arbeitsteilung und gegenseitige Abhängigkeiten wären ein neuer Schritt. Die Allianz „Five Eyes“ zeigt, wie gemeinsame Schwerpunkte Vertrauen und einen engen Verbund schaffen.

Und es wäre auch ein starkes gemeinsames Zukunftsprojekt.

Staatlichkeit und Allianzen entstehen oft unter Druck. Das ist jetzt unsere Chance, Dinge auf eine neue Grundlage zu stellen. ■

„Strategie braucht eine Vision“

Strategie ist keine Wunschliste. Der Politikwissenschaftler Holger Janusch über strategisches Lernen, die Fehlannahmen Europas – und die Demokratie als Korrekturmechanismus.

Holger Janusch, wozu brauchen Staaten eine Strategie?

Holger Janusch: Strategie ist fundamental wichtig. Es geht darum, Mittel wirksam einzusetzen, um Ziele zu erreichen, idealerweise mit einem mittel- bis langfristigen Horizont. Problematisch wird es im Sicherheitsbereich dort, wo Erfolg kaum messbar ist. Anders als in Unternehmen gibt es keine klaren Kennzahlen wie Gewinn oder Marktanteile. Es ist schwierig zu sagen, ob eine Strategie „erfolgreich“ war oder andere Faktoren ausschlaggebend waren.

Was muss eine solche „Theory of Success“ beinhalten?

Jede Strategie beruht auf Annahmen über die Zukunft und über kausale Zusammenhänge: Wenn bestimmte

Mittel eingesetzt werden, soll eine bestimmte Wirkung eintreten. Abschreckung etwa beruht auf der Annahme, dass Drohung den Gegner vom Handeln abhält. Sie kann aber auch das Gegenteil bewirken. Eine *Theory of Success* zwingt dazu, diese Annahmen offenzulegen, zu hinterfragen und zu prüfen, ob sie empirisch oder logisch tragfähig sind. Gleichzeitig muss klar definiert sein, was überhaupt als Erfolg gilt. Eine *Theory of Success* regt dazu an, mehr aus den verfügbaren Mitteln herauszuholen, als anfänglich zu erwarten war.

Jede Strategie beruht auf impliziten Annahmen über Gegner, Verbündete und Systemdynamiken. Welche Rolle spielt dabei Strategic Intelligence?



INTERVIEW_ Holger Janusch

Holger Janusch ist Professor für Internationale Politik mit dem Schwerpunkt auf Außen- und Sicherheitspolitik der USA am Fachbereich Nachrichtendienste der Hochschule des Bundes für öffentliche Verwaltung in Berlin mit den Forschungsschwerpunkten nationale Sicherheitsstrategien, die Handelspolitik der USA und Macht in Theorien der Internationalen Beziehungen. Er kuratierte den Sonderband „Integrierte Sicherheit für Deutschland?“ (2025).

KEY MESSAGES

- **Strategie ist eine Theory of Success:** Sie basiert auf überprüfbaren Annahmen darüber, wie Mittel Wirkung entfalten.
- **Strategic Intelligence** prüft, irritiert und falsifiziert diese Annahmen – sie ist mehr als Trendfortschreibung.
- **Europas zentrale Fehleinschätzung** war die Selbstverständlichkeit US-amerikanischer Stabilität.
- **Normen und Legitimität** sind strategische Ressourcen; Macht ohne Anerkennung untergräbt langfristigen Erfolg.
- **Demokratische Vielfalt und offene Debatte** sind kein Nachteil, sondern ein strategischer Korrekturmechanismus.

Wenn wir Strategie als *Theory of Success* verstehen, reden wir über Annahmen und Hypothesen zur Zukunft. Strategic Intelligence hat genau hier ihre Kernfunktion: Sie soll diese Annahmen prüfen, irritieren und – wenn nötig – falsifizieren. Es geht nicht um operative Zielaufklärung, sondern um langfristige, strukturelle Fragen: Wie verändern sich Macht, Technologie, Allianzen, politische Kulturen? Welche Trends sind stabil, welche volatil?

„Wenn Akteure nicht mehr glauben, dass Regeln Nutzen stiften oder von anderen eingehalten werden, beginnt eine Ordnung zu erodieren.“

Holger Janusch

Das heißt, Strategic Intelligence ist mehr als Trendfortschreibung?

Genau. Reine Extrapolation bringt wenig. Sinnvoller sind Szenarioanalysen, Net Assessments oder andere Formen strategischer Zukunftsanalyse. Ziel ist es, konkurrierende Hypothesen zu vergleichen und zu bewerten: Welche Theorie über die Zukunft ist mit den verfügbaren Informationen am plausibelsten? Das schafft die Grundlage, am Mittel langfristig sinnvoll einzusetzen.

Wo lagen aus europäischer Sicht strategische Fehleinschätzungen im Umgang mit den USA?

Eine zentrale Annahme war jahrzehntelang, dass die USA ein verlässlich stabiler Sicherheitspartner bleiben. Diese Annahme hätte man früher hinterfragen

können. Warnsignale gab es: die Burden-Sharing-Debatte, wachsende innenpolitische Polarisierung seit den 1990er-Jahren, zunehmende Volatilität in der Außenpolitik. Strategic Intelligence hätte diese Entwicklungen stärker gewichtet und ihre strategischen Implikationen klarer benennen können.

Ist Donald Trump für Sie primär unberechenbar – oder strategisch konsistent?

Beides. Es gibt erkennbare Muster: transaktionales Denken, Nullsummen-

Hinzu kommen andere Regime – etwa im Seerecht oder im Welthandel. Regeln wurden immer verletzt. Entscheidend ist die Frage, ab wann Normverletzungen so häufig werden, dass Normen ihre bindende Wirkung verlieren. Wenn Akteure nicht mehr glauben, dass Regeln Nutzen stiften oder von anderen eingehalten werden, beginnt eine Ordnung zu erodieren....

Welche Rolle spielt dabei die Trump-Administration?

Eine zentrale. Wenn ausgerechnet der Hegemon, der diese Ordnung mit aufgebaut und durchgesetzt hat, grundlegende Normen offen infrage stellt – etwa territoriale Integrität mit Blick auf Grönland, Panama oder Kanada –, dann ist das qualitativ etwas anderes. Ob man schon vom Zusammenbruch der Ordnung sprechen sollte, ist umstritten. Aber die Erosion wird deutlich beschleunigt.

Geht es dabei nur um formale Regeln oder auch um informelle Normen?

Definitiv auch um informelle Normen. In der Regimeforschung unterscheidet man zwischen Prinzipien, Normen, Regeln und Verfahren. Je abstrakter die Ebene, desto fundamentaler ist ihre Bedeutung für Ordnung. Wenn nicht nur Regeln, sondern grundlegende Normen und Prinzipien der Anerkennung von Souveränität und der gewaltlosen Konfliktaustragung verletzt werden, dann wird die gesamte Ordnung instabiler, auch jenseits formeller Vertragsbrüche.

Welche grundsätzliche Möglichkeiten hat der Schwächere gegenüber einem normbrechenden Stärkeren?

Rein definitorisch kann sich der Stärkere durchsetzen – sonst wäre er nicht der Stärkere. Aber militärische Stärke ist oft trügerisch. Konflikte wie Russland-Ukraine oder die USA in Viet- ➤

logik, maximale Drohung als Verhandlungsmittel. Neu in der zweiten Amtszeit ist ein stärker neoimperiales Denken in Einflusszonen. Unberechenbar wird es dort, wo materielle Interessen, kulturell-normative Bedrohungswahrnehmungen und geopolitische Logik je nach Lage unterschiedlich stark wirken. Strategic Intelligence kann diese Muster sichtbar machen – aber nicht exakt vorhersagen, welches wann dominiert.

Oft ist vom „Ende der regelbasierten Ordnung“ die Rede. Was ist damit eigentlich konkret gemeint?

Im sicherheitspolitischen Kern meint das zunächst die UN-Charta: keine militärische Aggression, Achtung von Souveränität und territorialer Integrität.

nam zeigen, dass kurzfristige Durchsetzung nicht automatisch langfristigen strategischen Erfolg bedeutet. Die eigentliche strategische Frage lautet: Führt das Recht des Stärkeren langfristig zu Stabilität oder untergräbt es die eigene Position?

Spielt dabei mehr als nur militärische Macht eine Rolle?

Absolut. Normative Faktoren, Legitimation und internationale Anerkennung sind zentral. Selbst sehr mächtige Akteure brauchen Rechtfertigungen – innen- wie außenpolitisch. Auch die Trump-Administration stößt an Grenzen, etwa bei Grönland oder Migration. Stärke allein ersetzt keine Legitimität. Nach Antonio Gramsci ist der Einsatz von Gewalt ein Zeichen für fehlende Hegemonie, also mangelnde Akzeptanz einer Herrschaftsordnung.

Was unterscheidet Demokratien in strategischer Hinsicht von Autokratien?

Autokratien können Mittel oft schneller bündeln und einsetzen. Demokratien wirken dagegen langsamer und fragmentierter. Der strategische Vorteil von Demokratien liegt aber im offenen Diskurs und in Korrekturmechanismen. Strategien beruhen auf Annahmen über die Zukunft – und Demokratien haben bessere Voraussetzungen, falsche Annahmen zu erkennen und Strategien anzupassen.

Viele sehen die europäische Reaktion auf die Grönland-Debatte als Wendepunkt.

Wie schätzen Sie das ein?

Kurzfristig war das ein Erfolg. Ob ein härteres Auftreten gegenüber der Trump-Administration stets zu besseren Ergebnissen führt, lässt sich jedoch nicht eindeutig sagen – das Risiko einer Eskalation bleibt bestehen. Strategisch wichtig ist jedoch, Entschlossenheit zu zeigen. Die Trump-Administration sig-

nalisiert klar: Starke, handlungsfähige Partner werden ernster genommen. Europa wird derzeit als schwach wahrgenommen, aber mit Potenzial.

Welche Rolle spielen die viel beschworenen Werte für Strategien?

Werte gehören zwingend dazu. Sie sind zentral für Motivation, Legitimation und gesellschaftliche Akzeptanz – gerade in Demokratien. Menschen handeln nicht für abstrakte Interessen, sondern für den Schutz einer bestimmten Ordnung. Gleichzeitig braucht es Pragmatismus. Werte dürfen nicht zur bloßen Moralrhetorik werden. Eine tragfähige Strategie muss Werte verinnerlichen, ohne sich der Realität zu verweigern.

In Ihrem Verständnis wären Werte also nicht selbst die Ziele, sondern müssten durch eine klare *Theory of Success* operationalisiert werden – etwa: Was heißt es konkret, Werte zu bewahren?

Genau. Hier würde ich zwischen *Theory of Success* und einem anderen strategischen Element unterscheiden: der Vision. Eine Vision verbindet ambitionierte Ziele mit einer klaren Wertebasis. Sie gibt das große Bild vor, definiert, was Erfolg überhaupt bedeutet, und wirkt motivierend – nach innen wie nach außen.

Welche Rolle spielen Lernen und Anpassung für Strategie?

Eine sehr wichtige. Die Umwelt wird immer komplexer und dynamischer, vor allem durch Technologie, die gleichzeitig neue Möglichkeiten eröffnet: mehr Daten, schnellere Auswertung, frühere Rückkopplung. Ein moderner strategischer Prozess braucht daher selbst eine Strategie für den Umgang mit Strategie, also für Lernen, Anpassung und kontinuierliche Überprüfung.

Das klingt fast nach einer visionären Intelligence-Aufgabe.

Ist es auch. Intelligence ist bislang oft stark operativ-taktisch ausgerichtet. Das strategische Sammeln und Einordnen von Informationen, also das Denken in längerfristigen Mustern, Wechselwirkungen und Zukunftsszenarien, kommt zu kurz. Das ist kein deutsches Spezifikum, sondern auch in den USA ein häufig geäußelter Kritikpunkt.

Bräuchte Europa dafür so etwas wie eine echte All-Source-Intelligence?

Zumindest müsste man diese Frage strategisch diskutieren. Welche Quellen sind für welche Konfliktarten wirklich relevant? Wo liefern technologische Mittel mehr Erkenntnis als klassische HUMINT – und umgekehrt? Das allein ist schon eine strategische Entscheidung über Mittel und Effizienz.

Und auf europäischer Ebene?

Dort stellt sich zusätzlich die Kooperationsfrage: Welche Synergien sind realistisch? Wo lohnt Arbeitsteilung? Und wie robust ist Vertrauen zwischen den Staaten? Eine Vision könnte ein europäisches All-Source-Modell sein – etwa ein „Twenty-Seven-Eyes“-Ansatz. Das ist nicht automatisch richtig, aber angesichts begrenzter Ressourcen naheliegend. Nationale Dienste haben komparative Vorteile, die man besser bündeln könnte.

Würden Sie sagen, dass wir eine neue strategische Kultur brauchen?

Ja, strategische Kultur wird oft gefordert, auch für Deutschland. Häufig wird sie mit strategischem Denken gleichgesetzt. Strategische Kultur meint die Narrative, Symbole, Analogien und Denkanahmen darüber, wie Mittel – insbesondere Gewalt – in der internationalen Politik wirken. Daraus leiten sich wiederum strategische Präferenzen ab. Strategische Kultur ist wichtig, aber immer auch mit Bias verbunden. >

Gerade in den USA hat eine bestimmte strategische Kultur in der Vergangenheit zu gravierenden Fehlentscheidungen beigetragen. Deshalb kann ein enger, kritischer Austausch zwischen unterschiedlichen strategischen Kulturen ein echter Vorteil sein.

Also Vielfalt als strategische Ressource?

Genau. Unterschiedliche historische Erfahrungen führen zu unterschiedlichen Perspektiven. Deutschlands strategische Kultur ist stark vom „Nie wieder“ geprägt, Großbritannien blickt auf imperiale und maritime Traditionen zurück, andere europäische Staaten haben wieder andere Erfahrungen. Diese Vielfalt kann helfen, Annahmen zu hinterfragen und blinde Flecken zu reduzieren – gerade in einer gemeinsamen europäischen Intelligence- oder Strategiearchitektur.

Was brauchen wir, um in Deutschland strategisches Denken zu etablieren?

Am Ende braucht es politische Führung, die bereit ist, das eigene Weltbild infrage zu stellen. Strategien sind immer auch parteipolitisch und ideologisch geprägt. Ohne Offenheit für Kritik bleibt kulturelle Vielfalt folgenlos. Oft braucht es erst Krisen oder offensichtliches Scheitern, damit Anpassung möglich wird.

Was ist für Sie im Hinblick auf Europa aktuell die größte Hoffnung, was die größte Sorge in Bezug auf Strategie und strategisches Denken?

Meine größte Hoffnung ist, dass strategisches Denken wieder ernster genommen wird. Man erkennt zunehmend, dass es notwendig ist, langfristiger und systematischer zu denken. Das sieht man daran, dass Strategiepapiere überall entstehen. Das allein ist noch keine Strategie, aber es ist ein Signal, dass sich etwas bewegt. Jetzt kommt es

darauf an, diese Strategien auch umzusetzen, zu überprüfen und anzupassen.

Und die größte Sorge?

Die größte Sorge liegt weniger bei den Menschen als bei den Strukturen. In Ministerien und Behörden gibt es viele sehr kluge Köpfe. Was mir Sorgen macht, sind Pfadabhängigkeiten, Routinen, Silodenken und bürokratische Hürden. Diese können strategisches Lernen und Anpassung massiv ausbremsen.

Manche haben den Eindruck, es sei bereits zu spät – ein gewisser Fatalismus.

Den teile ich nicht. Wir stehen vor ernsthaften Bedrohungen, aber nicht vor einem unausweichlichen Untergang. Strategische Anpassung braucht Zeit. Was über Jahrzehnte gewachsen ist, lässt sich nicht in Monaten verändern. Die Trump-Administration zeigt – bei aller Kritik –, dass sie bereit ist, bestehende Strukturen radikal aufzubrechen. Oft auf unkluge Weise, aber sie macht deutlich: Wandel ist möglich. Europa sollte daraus nicht den Stil, sondern die Bereitschaft zum strategischen Umdenken lernen. ■

„Am Ende braucht es eine politische Führung, die bereit ist, das eigene Weltbild infrage zu stellen.“

Holger Janusch

Modell Schweiz

Zwischen nationalen Interessen, bröckelndem Konsens und neuen Bedrohungen stößt Europas Sicherheitsarchitektur rechtlich an Grenzen. Die Schweizer Juristin Esther Omlin über Neutralität, Informationsaustausch und Kooperation jenseits klassischer Bündnislogiken.

Esther Omlin, Wo liegen aus Ihrer rechtlichen Perspektive die besonderen Schwierigkeiten einer europäischen Sicherheitsarchitektur?

Esther Omlin: Rechtlich ist internationale Zusammenarbeit immer anspruchsvoll. Man braucht Gesetze und Verträge, die von allen getragen werden. Die EU hat dafür eigentlich viele Grundlagen geschaffen. Das Problem ist nur, dass sie lange nicht sicherheitspolitisch genutzt wurden. Gleichzeitig besinnen sich viele Staaten wieder stärker auf nationale Interessen. Der frühere Konsens, auf dem viele Verträge beruhten, existiert so nicht mehr. Er müsste angesichts neuer Herausforderungen und veränderter Regierungen eigentlich neu verhandelt werden.

Wie sehen Sie vor diesem Hintergrund die aktuelle geopolitische Lage und das oft beschworene Ende der regelbasierten Ordnung?

Als Juristin habe ich mit diesem Begriff

Mühe. Diese Ordnung war stark von amerikanischen Interessen geprägt. Sie war nicht unsere Ordnung. Deshalb sehe ich es nicht nur negativ, dass dieser Begriff an Bedeutung verliert. Sanktionen etwa sind außen- und innenpolitische Instrumente. Wenn man fremde Regeln übernimmt, ohne die eigenen Interessen zu reflektieren, entsteht kein Gleichgewicht. Ich sehe darin eher eine Chance, sich europäisch und auch schweizerisch neu zu positionieren.

Trotz aller EU-Skepsis?

Ja. Bei aller Skepsis ist klar: Wertmäßig gehören wir zu Europa. Unsere engsten Partner sind hier. Neutralität heißt nicht Gleichgültigkeit. Wir fühlen uns europäischen Werten näher als anderen Machtblöcken. Dass diese Spannungen jetzt offener sichtbar werden, hat nicht erst mit Trump begonnen. Es wird nur deutlicher ausgesprochen als früher.

Welche Rolle spielt die Schweiz?



INTERVIEW_ Esther Omlin

Dr. Esther Omlin ist Dozentin für Sicherheitsrecht- und Wirtschaftsrecht an der Ostschweizer Fachhochschule (OST) und war zuvor als Oberstaatsanwältin tätig. Sie forscht zu den Gebieten äußere und innere Sicherheit, internationale Sicherheitspolitik, Weltraum und Außenwirtschaft und bietet dementsprechende Weiterbildungen an.

KEY MESSAGES

- **Europäische Sicherheitsarchitektur** scheitert weniger am Recht als am fehlenden politischen Konsens und neu erstarkten nationalen Interessen.
- **Die regelbasierte Ordnung** war nie neutral, sondern interessengeleitet – ihr Wandel eröffnet Europa die Chance zur strategischen Neupositionierung.
- **Nachrichtendienste** sind für Kleinstaaten wie die Schweiz zentral, weil Information Austausch, Prävention und Sicherheit ermöglicht.
- **Flexible Intelligence-Kooperationen**, auch mit nichtdemokratischen Partnern, sind realpolitisch notwendig und potenziell identitätsstiftend für Europa.
- **Neue Bedrohungen** in Cyberraum und Weltraum erfordern multilaterale Regeln, Offenheit über Interessen und den Mut, Sicherheit neu zu definieren.

Der aktuelle Konsens in der Schweiz ist, eher einen eigenständigen Weg zu gehen. In den letzten Jahren hat sich das sogar verstärkt, auch in der Westschweiz. Gleichzeitig erlaubt uns die EU eine gewisse Mitwirkung. Das ist ein bewusstes Rosinenpicken, das rechtlich und politisch nicht unproblematisch ist.

Viele gehen davon aus, dass sich Europa unabhängiger von den USA machen muss. Was heißt das aus schweizerischer Sicht für die Nachrichtendienste?

In der Schweiz wissen wir, wie zentral Nachrichtendienste für unsere Sicherheit sind. Es geht weniger ums Ausspionieren als um Austausch und Prävention. Da unsere militärischen Mittel begrenzt sind, sind verlässliche Beziehungen und funktionierende Informationsflüsse entscheidend. Genf ist als Sitz vieler internationaler Organisationen ein gewollter Treffpunkt für Dienste – mit offiziellen Formaten für frühen Informationsgewinn.

Wäre der Ansatz auch etwas für Europa?

Absolut. Präventive Nachrichtendienst-Arbeit und strukturierter Informations-transfer wären für Europa extrem wichtig. Natürlich weiß ich nicht, wie offen alle Nationalstaaten dafür wären, aber ich sehe eine Chance. Europa hat Länder, die stärker nach Osten schauen, andere eher nach Westen. Das könnte man bündeln.

Europa als eine Art „große Schweiz“?

Ja, ein bisschen überspitzt gesagt. Aber die Idee ist, dass man mit verschiedenen Seiten reden kann. Genau das macht die Schweiz seit Jahrzehnten. In Europa wären diese Perspektiven ja bereits vorhanden.

Könnte so eine Intelligence-Kooperation auch identitätsstiftend wirken?

Ja, das glaube ich. Entscheidend ist Offenheit und je nach Bedrohungslage

„Dienste haben oft keine Freunde oder Feinde, sondern Partner. Und die sind nicht immer moralisch einwandfrei.“

Esther Omlin

auch die Einbindung externer Staaten. Das zeigt sich etwa bei den BRICS: Ihre Anti-Terror-Arbeitsgruppen sind wirksam, weil dort Länder vertreten sind, die direkt betroffen sind. Die Formate sind bewusst flexibel – und genau darin liegt ihr Potenzial

Also Zusammenarbeit auch mit nichtdemokratischen Staaten wie Saudi-Arabien?

Genau. Das ist klassisches Nachrichtendienst-Handwerk. Nachrichtendienste haben oft keine Freunde oder Feinde, sondern Partner. Und diese sind nicht immer moralisch einwandfrei.

Solche Kooperationen stehen natürlich im Spannungsverhältnis zur Idee der wehrhaften Demokratie.

Ja, das ist ein Problem. Aus Schweizer Sicht ist Demokratie ohnehin anders definiert, weil wir direkte Demokratie haben. Rein rechtlich betrachtet gibt es zwischen verschiedenen Staatsformen oft weniger Unterschiede, als man politisch gerne annimmt. Die Umsetzung ist natürlich eine andere Frage. Aber auch Demokratien sind historisch nicht immer demokratisch entstanden.

Heißt das, moralische Abgrenzung stößt schnell an Grenzen?

Genau. Für die Schweiz ist Kooperation grundsätzlich möglich. Wir sind darauf angewiesen. Als Kleinstaat können wir es uns nicht leisten zu sagen, mit diesen reden wir und mit jenen nicht. Vermittlung und Gesprächsoffenheit sind Teil unseres Modells.

Sehen Sie heute eine neue oder größere Rolle für neutrale Staaten?

Ja, durchaus. Gerade weil sich Europa ein Stück weit von den USA löst und stärker auf sich selbst zurückgeworfen ist. Neutralität muss dabei nicht strikt im völkerrechtlichen Sinn verstanden werden. Blockfreiheit wäre ein anderes Modell. Viele Staaten, auch im BRICS-Kontext, waren ursprünglich blockfrei. Dass sie heute anders wahrgenommen werden, ist eher Ergebnis geopolitischer Verschiebungen.

Je mehr Beziehungen in unterschiedliche Richtungen bestehen, desto besser das Lagebild...

Genau. Für Kleinstaaten ist Information der zentrale Sicherheitsfaktor. Information hält uns im Frieden.

Zwingen neue Bedrohungen wie Cyberangriffe dazu, Sicherheit grundsätzlich neu zu denken?

Ja, definitiv. Cyberbedrohungen machen an Grenzen nicht halt. Das hat auch die Schweiz erkannt. Nationale Lösungen reichen hier nicht mehr aus. Deshalb ist internationale Kooperation zwingend notwendig. In den letzten Jahren hat sich hier viel getan. Gerade in der Schweiz, aber auch in Abstimmung mit dem EU-Recht, gab es zahlreiche Gesetzesnovellen. Rein rechtlich sind wir inzwischen relativ gut aufgestellt. Das eigentliche Problem liegt weniger im Recht als in der Sensibilisierung.

Woher kommt das?

>

Das hat viel mit der Schweizer Mentalität zu tun. Wir gehen oft davon aus, dass uns niemand etwas Böses will. Das ist einerseits Lebensqualität, andererseits ein Risiko. In Unternehmen und Behörden werden Warnsignale häufig relativiert. Erst wenn sich Vorfälle häufen, wird reagiert. Dieser Weg von „wahrscheinlich harmlos“ zu „das war ein Angriff“ dauert zu lange.

Und das lässt sich schwer ändern?

Ja. Selbst mit Schulungen bei Polizei, Armee und Unternehmen bleibt diese Grundhaltung bestehen. Sensibilisierung ist unser größtes Defizit. Und ich vermute, dass ähnliche Probleme auch in Teilen der EU existieren.

Sie forschen auch zum Weltraumrecht. Im Weltraum tummeln sich inzwischen staatliche und kommerzielle Akteure. Ist das eigentlich ein rechtsfreier Raum?

Nein. Seit dem Weltraumvertrag von 1967 ist der Weltraum völkerrechtlich geregelt. Über 100 Staaten, darunter auch die Schweiz, waren von Anfang an dabei. Damals ging es ausschließlich um Staaten und ihre Verantwortung. Das Problem heute ist der Eintritt privater Akteure. Gleichzeitig sehen wir, dass Staaten wie China bereits sehr konkrete Ressourcenstrategien entwickeln. Das erinnert an Antarktis- oder Arktisfragen, nur dass es hier um Mond und Weltraumressourcen geht.

Wer haftet, wenn private Satelliten Schaden verursachen?

Die Schweiz hat entschieden, dass private Unternehmen selbst haften. Der Staat zieht sich zurück. Andere Länder, auch viele in der EU, sehen weiterhin den Staat in der Verantwortung. Das hat massive Folgen für Versicherungen und Finanzierung, weil Unternehmen für potenziell milliardenschwere Schäden vorsorgen müssen.

Wenn ein privates Unternehmen aus der Schweiz einen Aufklärungssatelliten betreibt, trägt es selbst die Verantwortung?

Ja. In anderen Ländern wäre der Staat verantwortlich. Das zeigte sich auch bei Elon Musk. In den USA haftet der Staat für seine Satelliten. Als diese im Ukraine-Krieg eingesetzt wurden, war das völkerrechtlich relevant, weil damit die USA indirekt Partei wurden. Für die Schweiz wäre so etwas ein politischer Super-GAU, weil die Neutralität hier unmittelbar betroffen wäre.

Was passiert, wenn Großmächte den Weltraumvertrag von 1967 einfach aufkündigen? Gilt dann auch im Weltraum das „Recht des Stärkeren“?

Das ist bei allen völkerrechtlichen Verträgen das zentrale Risiko. Der Weltraumvertrag ist im Kern eine Absichtserklärung, ergänzt durch Haftungsabkommen. Ein Austritt großer Akteure würde das Fundament erschüttern. Gleichzeitig sind heute viele neue Player entscheidend, etwa in Indien, Afrika oder in der arabischen Welt. Ohne sie ist Weltraumpolitik nicht mehr denkbar.

Das heißt, neue Regeln wären kaum ohne sie machbar?

Genau. Ein neues Regelwerk müsste multilateral ausgehandelt werden. Bilaterale Lösungen würden nicht ausreichen. Für die traditionellen Großmächte wäre das unbequem, aber realistisch gibt es keine Alternative mehr.

Sollten wir heute über Regeln und ihre Absicherung ganz neu nachdenken?

Ich glaube schon. Wenn man gezwungen ist, neu zu verhandeln und Interessen offen auf den Tisch zu legen, entstehen möglicherweise auch Allianzen, mit denen man vorher nicht gerechnet hätte. Das eröffnet die Chance, nachhaltiger und langfristiger zu denken.

Was fehlt uns heute besonders?

Sicherheit im Sinne von Berechenbarkeit. Menschen, die im Kalten Krieg gearbeitet haben, sagen oft: Das war gefährlich, aber stabil. Man kannte die roten Linien, selbst gegenüber dem Gegner. Heute fällt vieles zusammen. In dieser globalisierten Welt weiß man oft nicht mehr, was gilt und was nicht.

Könnten neue Regeln diese Sicherheit wieder herstellen?

Ja, wenn jedes Land ehrlich formuliert, was ihm wichtig ist. Das könnte eine tragfähige Sicherheitsarchitektur für Jahrzehnte schaffen. Dafür braucht es Mut zur Offenheit.

Die Frage bleibt aber: Wie sichert man solche Regeln ab, wenn Vertrauen fehlt?

Genau das ist der Knackpunkt. Ich glaube aber, dass der Weltraum hier ein interessantes Paradigma sein könnte. Diese Idee einer friedlichen, gleichberechtigten Zusammenarbeit ist noch immer stark verankert.

Als Gegenmodell zur klassischen Machtpolitik?

Ja. Ein Weltraumspezialist der Schweizer Armee sagte mir einmal: Wir garantieren den Frieden im Weltraum, nicht die Sicherheit. Das klingt zunächst paradox, meint aber, der Weltraum müsse bewusst außerhalb von Machtlogik gehalten werden. Dort gibt es keine Sanktionen, auch keinen Wirtschaftskrieg.

Auch aus praktischen Gründen.

Natürlich. Niemand kann die internationale Raumstation allein betreiben. Aber dass man nicht einmal darüber nachdenkt, den Weltraum mit Sanktionen zu überziehen, zeigt, wie stark diese Idee noch ist. Und ich glaube, genau dieser Traum einer friedlichen Zusammenarbeit hat politische Kraft. Der Weltraum kann ein Symbol dafür sein. ■

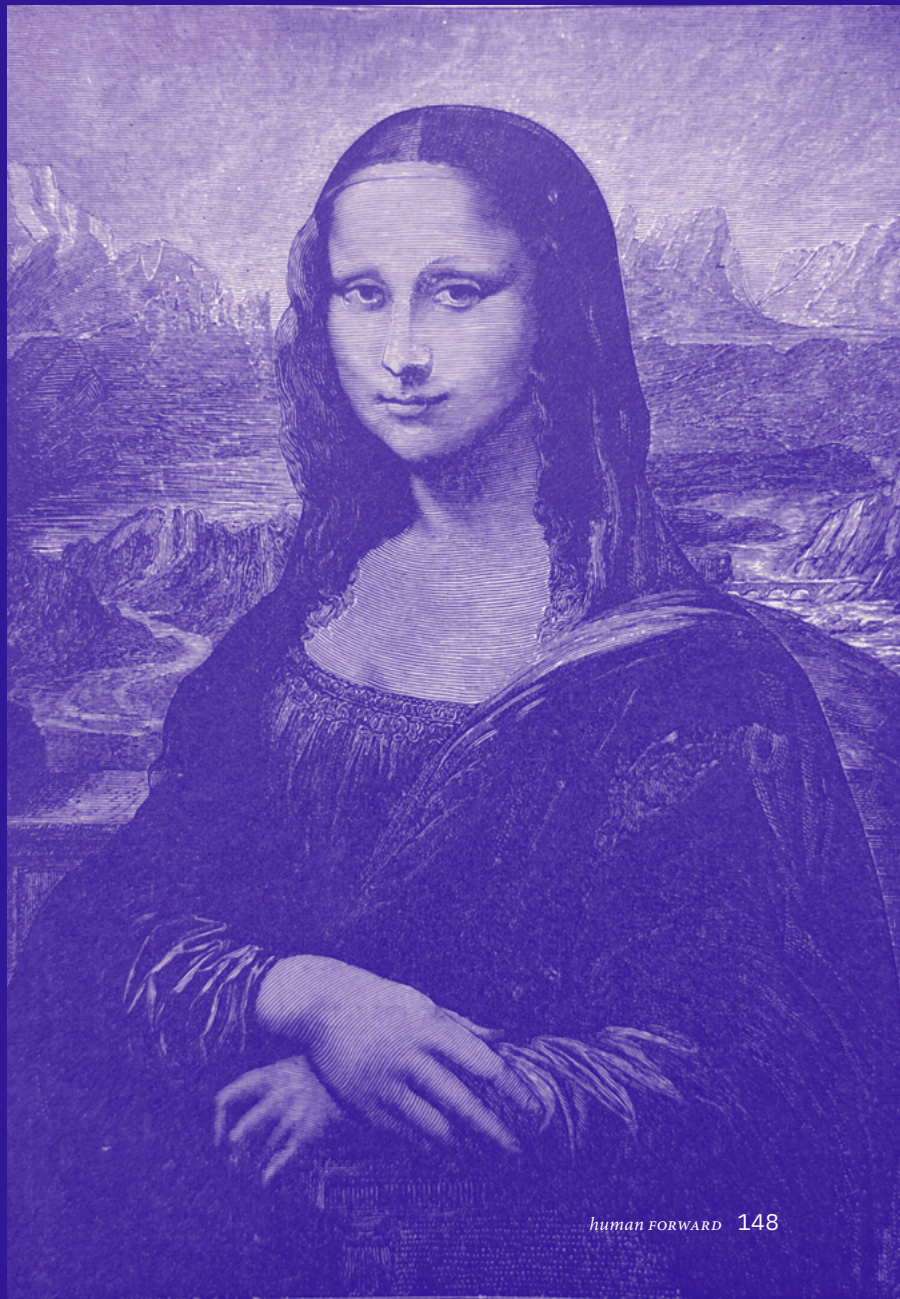
05_ Ecosystem

Europas Kräfte bündeln

*„Krieg beginnt und endet nicht
beim Militär. Er trifft immer die
Schwachstellen einer
Gesellschaft – Informationsräume,
Infrastruktur, Psyche, Alltag“.*

Dr. Larysa Visengeriyeva,
Ukraine/Deutschland

Illustration Campwillowlake/Stock



Das Zeitalter autonomer Verteidigung

Hybride Angriffe, KI-beschleunigte Bedrohungen und Desinformation erzwingen einen Paradigmenwechsel. 2026 muss Europa Cybersicherheit und strategische Intelligence zusammenführen – weg von reaktiver Abwehr, hin zu einer demokratisch verankerten, proaktiven Sicherheitsarchitektur.

Im Jahr 2026 muss die künstliche Trennung zwischen „Cybersicherheit“ und „strategischer Intelligence“ faktisch aufgehoben werden. Für Europa ist Intelligence keine periphere Staatsfunktion mehr, sondern die Kerninfrastruktur einer resilienten Gesellschaft. Im folgenden argumentieren wir für einen grundlegenden Übergang von reaktiver, technisch geprägter Abwehr hin zu einer proaktiven, menschenzentrierten Interpretationsfähigkeit. Intelligence wird dabei nicht länger als abgeschlossener Aufgabenbereich der Geheimdienste verstanden, sondern als ganzheitliche gesellschaftliche, politische und technologische Aufgabe.

Die vorgeschlagene Architektur balanciert die „Last des Verteidigers“ ethischer Betriebsmodelle – verankert in den Transparenzanforderungen des EU AI Act – mit einem strategischen Pivot hin zu proaktiver Verteidigung in Maschinengeschwindigkeit. Indem autonome Verteidigung und erweiterte OSINT fest in demokratischen Werten verankert werden, transformiert Europa Intelligence zu einer Grundlage von Verantwortung und kollektiver Selbstvergewisserung. Dieses Rahmenwerk überwindet eine überholte „Firewall“-Mentalität zugunsten eines Continuous Threat Exposure Management (CTEM)-Ansatzes und stellt sicher, dass strategische Klarheit unser zentrales Kapital beim Schutz demokratischer Souveränität gegenüber hybriden Bedrohungen bleibt. >

TEXT_ **Brendan Kotze**

Brendan Kotze ist Chief Delivery Officer bei dem international tätigen Cybersecurity-Unternehmen Performanta (Hauptsitz London, UK). Mit über 20 Jahren Erfahrung in der IT-Sicherheit war er entlang des gesamten Security-Lebenszyklus tätig, bis hin zur Rolle als CISO. Heute verantwortet er Entwicklung, Automatisierung und Beratung mit Fokus auf praxisnahe Sicherheitslösungen, die Geschäftsrisiken reduzieren und Menschen im digitalen Raum schützen.

KEY MESSAGES

- **Die Trennung zwischen Cybersicherheit und strategischer Intelligence** ist überholt: Europas Resilienz erfordert eine integrierte Intelligence-Architektur.
- **Europa muss auf** hybride Bedrohungen mit autonomer Verteidigung sowie kollektiver Attribution reagieren.
- **Intelligence** ist eine demokratische Versorgungsleistung: Transparenz, OSINT und „Duty to Share“ stärken Staat, Wirtschaft und Gesellschaft.
- **Öffentliche Finanzierung** ist strategische Sichtbarkeit: Informationsblackouts und De-Priorisierung schwächen Abschreckung und Souveränität.
- **Europas Vorteil** liegt nicht in unregulierter KI, sondern in vertrauensbasierter, ethisch verankerter Verteidigung als strategischem Differenzierungsmerkmal.

1 Jenseits des Datendiebstahls: Kognitive Kriegsführung und strukturelle Sabotage

Cyberoperationen haben sich von klassischer Spionage hin zu struktureller Sabotage und kognitiver Kriegsführung verlagert.

- **Das Ziel:** Erosion institutionellen Vertrauens und Manipulation der öffentlichen Wahrnehmung durch synthetisierte Desinformation.
- **Die Methode:** „Ransom-as-Espionage“, bei der Ransomware-Angriffe als taktischer Rauchvorhang für tiefgreifende Exfiltration geistigen Eigentums oder zur politischen Erpressung dienen.

2 Der geopolitische Schmelztiegel: Cyber als „erste Front“

Cyberoperationen stehen inzwischen im Zentrum geopolitischer Dynamiken:

- Fragmentierte digitale Rechtsräume haben zu „digitalen Blockaden“ geführt. Gegner greifen gezielt Engpässe in Lieferketten (Halbleiter, maritime Logistik, Energie- und Versorgungsinfrastruktur) an, um Volkswirtschaften zu lähmen, noch bevor ein physischer Schuss fällt. Dies kann zu erweiterten Störungen führen, etwa durch Hafenstillstände, Standort-Spoofing in der Logistik, Manipulation von Frachtmanifesten sowie logische und physische Abfang- oder Angriffshandlungen, die Treibstoffknappheit und Störungen auf der letzten Meile verursachen.
- Obwohl sie der Sicherheit dienen sollen, können bekannte Schwachstellen in verpflichtenden „Transparenzlisten“ von Gegnern ausgenutzt werden. Software-Stücklisten (Software Bill of Materials, SBOM) von Komponenten kritischer Infrastrukturen werden gezielt instrumentalisiert, indem die kleinste, unauffälligste Softwarebibliothek angegriffen wird, von der das gesamte System abhängt.
- Die Trennlinie zwischen digitalen „Mafia“-Strukturen und staatlichen Nachrichtendiensten ist verschwunden. Staaten bedienen sich krimineller Stellvertreter zur Durchführung von Cyber-Erpressung und gewähren im Gegenzug rechtliche Immunität, um kritische europäische Sektoren und deren Lieferketten zu de-stabilisieren.

3 Nachrichtendienste als demokratische Versorgungsleistung (gesellschaftliche Dimension)

Nachrichtendienstliche Erkenntnisse sind kein exklusives Sicherheitsinstrument mehr, sondern die operative Grundlage ge-

sellschaftlicher Verantwortung und Teilhabe. Angesichts systemischer Cyberbedrohungen und Desinformation ist ein Übergang von einer „Need-to-know“-Kultur zu einem „Duty-to-share“-Modell erforderlich.

- In einer Ära kognitiver Kriegsführung und digitaler Polarisierung müssen hochauflösende Cyber-Intelligence-Produkte als öffentliche Versorgungsleistung fungieren. Durch belastbare Attribution von Cyberangriffen und Desinformationskampagnen ermöglichen sie die Zurückweisung gegnerischer Narrative und Einflussnahme.
- Soziale Medien sind zu den primären Verbreitungssystemen für „Wahrnehmungs-Hacks“ geworden. Vor diesem Hintergrund muss der Austausch nachrichtendienstlicher Erkenntnisse auch die Identifikation koordinierten, inauthentischen Verhaltens und algorithmischer Manipulation umfassen. Indem offengelegt wird, wo ausländische staatliche Akteure polarisierende Inhalte einspeisen, verhindert hochauflösende Intelligence die scheinbar organische Radikalisierung der Bevölkerung und schützt die Integrität des nationalen Informationsraums.
- Gegner richten ihre Angriffe zunehmend gegen Einzelpersonen – von Beamten bis zu Privatpersonen – und nutzen dabei „Lifestyle-Pattern“-Analysen und OSINT-Erkenntnisse für hochpräzises Social Engineering, Einflussnahme, Erpressung oder sogar kinetische Zielauswahl. Durch die Demokratisierung von Threat Intelligence können Individuen mit „digitalen Frühwarnsystemen“ ausgestattet werden. So wird verdeckte Telemetrie in persönliche Verteidigungsinstrumente überführt, etwa durch automatisierte Hinweise auf Deepfake-Medien oder die Identifikation bössartiger Infrastruktur, noch bevor ein Klick erfolgt. Auf diese Weise wird der private Bürger als kritisches Glied in der nationalen Sicherheitskette geschützt – insbesondere vor dem Hintergrund, dass die persönliche digitale Identität leicht zum Vektor für laterale Bewegungen werden kann, über den Angreifer die Lücke zwischen verwundbaren häuslichen Umgebungen, dem Individuum und hochrangigen Unternehmens- oder Staatsnetzen überbrücken.

4 Der KI-gestützte Gegner und die Governance-Lücke

Im Jahr 2026 ist das „KI-Wettrüsten“ durch ausgeprägte Asymmetrien geprägt.

- **Unregulierte vs. ethische KI:** Gegner setzen „jailbroken“ Modelle ohne Sicherheits- oder ethische Leitplanken ein, um die Erstellung von Malware zu automatisieren, Social-Engineering-An- ➤

griffe zu lokalisieren und Schwachstellen auszunutzen – und in noch problematischerer Weise auch unerfahrenen Akteuren zu ermöglichen, komplexe, mehrstufige Angriffe mit der Präzision und Geschwindigkeit von Experten in großem Maßstab durchzuführen.

- **Die Last der Verteidiger:** Europäische Akteure operieren unter dem EU-KI-Rechtsrahmen (EU AI Act), der Erklärbarkeit, Transparenz und menschliche Aufsicht („human in the loop“) verlangt. Diese „eingebaute Latenz“ ist ethisch zwingend notwendig, wird jedoch zunehmend zu einem taktischen Nachteil.
- **Die Überwindung der Trennung** zwischen akademischen und operativen Silos ist kein rein intellektuelles Ziel, sondern eine Voraussetzung für Souveränität. Europa muss eine interdisziplinäre Talentpipeline aufbauen, die die Kluft zwischen technischen Ingenieurwissenschaften und geopolitischen Instituten überbrückt. Es gilt, eine neue Generation von „Strategic Analysts“ und „Intelligence Ethicists“ auszubilden, die autonome Verteidigungssysteme steuern und maschinenschnelle Warnsignale in ihren jeweiligen ethischen und geopolitischen Kontext einordnen können.

5 Der akademische Knotenpunkt

Um eine gemeinsame strategische Sprache für das Zeitalter hybrider Bedrohungen zu entwickeln, muss Europa die Silos zwischen Disziplinen auflösen, die traditionell getrennt voneinander betrachtet werden. Eine ganzheitliche Intelligence-Kultur erfordert die Konvergenz von akademischer Tiefe, ethischer Strenge und operativer Ingenieurskunst.

- Nachrichtendienste müssen als interdisziplinäres Forschungsfeld verstanden werden (Sozialwissenschaften, Ethik und Ingenieurwissenschaften). Europa muss ein eigenes Forschungsökosystem fördern, um die intellektuelle Souveränität über seine analytischen Werkzeuge zu sichern.
- Europa muss eine interdisziplinäre Talentpipeline etablieren, die technische Ingenieurhochschulen mit geopolitischen Instituten verbindet.
- Es ist eine neue Generation von „Strategic Analysts“ und „Intelligence Ethicists“ auszubilden, die als strategische Dirigenten agieren: Sie definieren missionskritische Zielsetzungen und ethische Parameter autonomer Systeme, anstatt sich auf manuelle Einzelfalltrage zu beschränken.
- Durch die Verbindung dieser Disziplinen lösen wir uns von rein technokratischen Reaktionen hin zu einem „Total-Defence“-An-

satz. Dieser interdisziplinäre Zugang ermöglicht es Entscheidungsträgern und Praktikern, technische Telemetriedaten durch eine einheitliche Linse zu interpretieren und sicherzustellen, dass jedes Signal in seinem angemessenen geopolitischen und ethischen Kontext verankert ist.

6 Der Public-Private-Nexus

Die europäische Nachrichtendienstarchitektur kann nicht länger ein staatliches Monopol sein. Vielmehr sollte ein formalisierter Rahmen geschaffen werden, um Experten aus dem privaten Sektor in systemischen Krisen gezielt zu „aktivieren“ und so den Betrieb kritischer Infrastrukturen sicherzustellen. Dieser Rahmen schließt die Umsetzungslücke zwischen staatlicher Attribution und privater Innovationsfähigkeit und gewährleistet, dass kritische Infrastrukturen auch unter hybriden Zwangslagen funktionsfähig bleiben. Gleichzeitig stellt er sicher, dass essenzielle Dienstleistungen, auf die europäische Bürgerinnen und Bürger angewiesen sind, selbst unter Angriffen resilient und transparent verteidigt werden.

Dimension	Staatliche Nachrichtendienste	Privatsektor
Mandat	Nationale Souveränität und Sicherheit	Risikominderung und Geschäftskontinuität
Datenzugang/ Fokus	Zielgerichtete, hochwertige Signale sowie klassifizierte HUMINT- und SIGINT-Erkenntnisse	Breite, globale Telemetrie und OSINT
Rechtsrahmen	Klassifizierte Sicherheitsgesetze	NIS2 / DSGVO / DORA / CIS / NIST / ISO
Fähigkeiten	Legitime Attribution und staatliche Reaktion	Schnelle technologische Innovation und globale Skalierbarkeit

Gleichzeitig muss die Dual-Use-Natur des nichtstaatlichen Intelligence-Marktes anerkannt werden. Während private „Threat-Intelligence“-Unternehmen unverzichtbare Partner sind, stellt der Aufstieg unregulierter kommerzieller Überwachungs-„Marktstrukturen“ ein erhebliches Spionageabwehrrisiko dar. Europa muss daher einen regulatorischen „Safe Harbor“ schaffen, der privaten Verteidigern Rechtssicherheit bietet, wenn sie in systemischen Krisen hochauflösende Telemetriedaten teilen. ➤

7 Resilienz finanzieren: Lehren aus dem US-amerikanischen „Defunding“-Modell

Eine zentrale Verwundbarkeit im Jahr 2026 ist die Erosion institutioneller Finanzierung. Die jüngsten Erfahrungen in den USA dienen als eindringliche Warnung: Die Mittelkürzungen für die CISA (Cybersecurity and Infrastructure Security Agency) und das Auslaufen des Cybersecurity Information Sharing Act Ende 2025 führten zu:

- **Informationsblackout:** Einem geschätzten Rückgang des freiwilligen Bedrohungsaustauschs um 80 %, ausgelöst durch den Wegfall von Haftungsschutz für private Unternehmen.
- **Massiven Budgetkürzungen:** Einsparungen von bis zu 62 % in Engagement-Abteilungen und 73 % in Risikomanagementzentren haben die Fähigkeit, Frühwarnungen für Kommunen und kleine Unternehmen bereitzustellen, erheblich geschwächt.
- **Fragmentierung der Verteidigung:** Die Unterfinanzierung öffentlicher „Clearingstellen“ zwingt Organisationen zur Arbeit in Silos. Diese zersplitterte Verteidigung ist für staatlich unterstützte Akteure leicht zu durchdringen und wird so selbst zur strategischen Chance für Angreifer.

Europa muss dieses Modell der **De-Priorisierung** entschieden zurückweisen. Dauerhafte öffentliche Finanzierung ist kein Kostenfaktor, sondern eine strategische Investition in die kollektive Sichtbarkeit, die notwendig ist, um „Grey-Zone“-Manöver frühzeitig zu erkennen.

8 CTEM: Die operative Brücke zur strategischen Klarheit

Europa muss **Continuous Threat Exposure Management (CTEM)** einführen, um Sicherheitsmaßnahmen mit strategischer Souveränität zu verknüpfen – und dort anzusetzen, wo der größte strategische Mehrwert erzielt werden kann.

1. **Abgrenzung (Scoping):** Definition der Schutzgüter – von Stromnetzen bis zu demokratischen Datenbanken –, die für eine „freie Gesellschaft“ essenziell sind.
2. **Erkennung (Discovery):** Identifikation nicht nur technischer Schwachstellen, sondern auch von Identitätsrisiken und Fehlkonfigurationen, die in der Grey Zone ausgenutzt werden.
3. **Priorisierung:** Bewertung von Bedrohungen nach ihrem Potenzial, die europäische Stabilität zu unterminieren – nicht allein nach technischer Schwere.
4. **Validierung:** Einsatz von Red-Teams sowie KI-gegen-KI-Simulationen, um zu überprüfen, ob eine Bedrohung bestehende

Verteidigungen tatsächlich überwinden kann.

- 5. **Mobilisierung:** Abkehr von reiner „Alert-Jagd“ hin zur automatisierten Behebung jener 1 % der Exponierungen, die strategisch wirklich relevant sind.

9 Cyberhygiene: Das Fundament strategischer Resilienz

Mit dem Übergang Europas zu autonomen Verteidigungsfähigkeiten muss sich Cyberhygiene von einer Abfolge routinemäßiger Maßnahmen zu jener strukturellen Systemgesundheit entwickeln, die Hochgeschwindigkeits-Intelligence- und Verteidigungssysteme überhaupt erst funktionsfähig macht. Ohne diese Basis ist der „strategische Pivot“ nicht möglich: Vernachlässigte Hygiene erzeugt Erkennungslücken und Telemetrie-Rauschen, das von Angreifern als Rauchvorhang genutzt werden kann.

Der erfahrene Angreifer des Jahres 2026 „bricht“ nicht mehr ein – er „loggt“ sich ein.

- **Living off the Land (LotL):** Hochentwickelte Akteure umgehen klassische Antivirenlösungen, indem sie integrierte Administrationswerkzeuge, Edge-Geräte (Router, Firewalls) sowie Lieferketten missbrauchen. Sie verschmelzen mit legitimen Netzwerkaktivitäten und erreichen so dauerhafte Präsenz.
- **Identitätsbasierte Infiltration:** Gegner priorisieren den Diebstahl nicht-menschlicher Identitäten, etwa von KI-Agenten oder Service-Tokens. Das Management dieser „Geisteridentitäten“ stellt eine der größten derzeitigen Verteidigungslücken dar.

Im Rahmen der regulatorischen Vorgaben für wesentliche Einrichtungen unter der NIS2-Richtlinie und dem Cyber Resilience Act sind die folgenden Punkte verpflichtende Säulen der europäischen Intelligence-Architektur:

- **Sichtbarkeitsgebot:** Man kann nicht verteidigen, was man nicht sieht. Kontinuierliche Asset-Erkennung stellt sicher, dass die Scoping-Phase des Continuous Threat Exposure Management (CTEM) belastbar ist; ein nicht erfasstes IoT-Gerät oder ein vergessener Legacy-Server fungiert als unsichtbare Umgehung selbst für hochentwickelte KI-Agenten.
- **Identitätshygiene:** Europa muss von klassischer MFA (Multi-Faktor-Authentifizierung) zu hardwarebasierter, phishing-resistenter Authentifizierung übergehen. Im Zeitalter KI-generierter Angriffe sind traditionelle Multi-Faktor-Verfahren (z. B. E-Mail oder SMS) nicht länger „angemessen und verhältnismäßig“.
- **Lieferkettenverantwortung:** Organisationen tragen nun stra- ➤

tegische Verantwortung für die Sicherheitslage ihres gesamten Zulieferer-Ökosystems. Der Cyber Resilience Act (CRA) unterstützt diesen Wandel, indem er den Übergang von „implizitem Vertrauen“ zu kontinuierlicher Lieferantenbewertung erzwingt.

10 Erkennung und Reaktion: Das Zeitalter autonomer Verteidigung

Die Umsetzungslücke muss geschlossen werden. Wenn CTEM das Radar ist, das Bedrohungen am Horizont erkennt, dann sind Erkennung und Reaktion die Reflexe, die sie in Echtzeit neutralisieren.

Geschwindigkeit und Volumen moderner Cyberangriffe haben menschenzentrierte Reaktionsmodelle zu einer sekundären Unterstützungsfunktion gemacht. Das klassische Security-Operations-Centre-Modell (SOC) muss sich entsprechend wandeln. Anstelle manueller Bedrohungssuche oder statischer Erkennungsregeln ist ein Übergang zu Multi-Agenten-Systemen erforderlich, die Echtzeit-Triage und automatisierte Eindämmung leisten.

- **Das Ende der Verweildauer:** Früher hielten sich Angreifer durchschnittlich über 200 Tage unentdeckt in Netzwerken auf. KI-gestützte Erkennung muss auf „Zero Dwell Time“ zielen – die Identifikation und Neutralisierung von Angreifern in Maschinengeschwindigkeit.
- **Autonome Eindämmung:** Wird eine hochauflösende Bedrohung erkannt, müssen Systeme selbstheilende Reaktionen ausführen: kompromittierte Knoten isolieren, geleakte Session-Tokens deaktivieren und Netzwerkverkehr stoppen – ohne auf menschliche Freigabe zu warten.
- **Auditierbare Autonomie:** Jede autonome Aktion wird mit einer KI-generierten Begründung protokolliert. Dies erfüllt die Transparenzanforderungen des EU-AI-Acts, ohne die Verteidigungsgeschwindigkeit zu reduzieren.
- **Geschäftskontext-Risiko:** Eine zentrale strategische Herausforderung besteht darin, „selbstverursachte Ausfälle“ zu vermeiden, etwa wenn KI zur Eindämmung einer geringfügigen Infektion eine kritische Produktionslinie stilllegt. Entscheidungsträger müssen daher kontextbewusste KI priorisieren, die geschäftliche und mission-kritische Abhängigkeiten versteht.

11 OSINT und KI: Das neue „strategische Radar“

In einem demokratischen Rahmen ist Open-Source-Intelligence (OSINT) eine tragende Säule von Transparenz. Im Gegensatz zu verdeckten Methoden stützt sich OSINT auf rechtmäßig erhobene, öffentlich oder kommerziell verfügbare Daten und eignet sich damit besonders für Gesellschaften, die Rechtsstaatlichkeit und öffentliche Rechenschaftspflicht betonen.

- Bis 2026 übersteigt das Volumen digitaler Daten – von Satellitenbildern bis zu Social-Media-Telemetrie – die menschliche Verarbeitungskapazität. KI-gestützte OSINT fungiert als Radar, das dieses Umfeld kontinuierlich scannt, um Grey-Zone-Aktivitäten zu erkennen, bevor sie eskalieren. Fallstudien zeigen, dass die Verknüpfung von OSINT mit technischer Telemetrie gegnerische Vorbereitungsinfrastruktur bis zu 48–72 Stunden vor einem aktiven Einsatz identifizieren kann.
- Die Integration großer Sprachmodelle (LLMs) und autonomer KI-Agenten transformiert rohe „Open-Source-Informationen“ (OSINF) in „handlungsrelevante Intelligence“ (OSINT). KI komprimiert die Intelligence-Wertschöpfungskette und ermöglicht das Echtzeit-Scannen von Millionen von Assets zur Erkennung früher Kompromittierungsindikatoren und Verhaltensanomalien.
- Im Zeitalter der „Informationsverschmutzung“ fungiert OSINT als Instrument des „Pre-Bunking“. Durch die Bereitstellung einer verifizierten, transparenten Faktenbasis können demokratische Institutionen gegnerische Narrative benennen, bevor sie im öffentlichen Bewusstsein Fuß fassen.
- Um eine demokratische Versorgungsleistung zu bleiben, muss dieses „strategische Radar“ unter auditierbarer Autonomie operieren. Während KI die notwendige Geschwindigkeit liefert, müssen die Kriterien für Analyse und Scanning gegenüber Aufsichtsinstanzen transparent bleiben, um die Einhaltung des EU-AI-Acts und der Grundrechte sicherzustellen.
- Da OSINT auf öffentlichen Daten beruht, können seine Ergebnisse breiter mit Zivilgesellschaft, Wirtschaft und internationalen Partnern geteilt werden, ohne geheime Quellen zu gefährden.
- **Interdisziplinäre Zusammenarbeit:** Dieses Radar entfaltet seine größte Wirkung, wenn es staatliche Nachrichtendienste, private Telemetrie und akademische Forschung verbindet und so eine gemeinsame strategische Sprache für das 21. Jahrhundert schafft.

>

12 Strategische Optionen für eine europäische Intelligence-Architektur

Wir plädieren für ein proaktives europäisches Intelligence-Paradigma, das auf strategische Handlungsfähigkeit ausgerichtet ist:

- **Stärkung der Single Intelligence Analysis Capacity (SIAC)** zu einem rund um die Uhr arbeitenden Echtzeit-Lage- und Bewertungszentrum, das technische Telemetrie mit geopolitischer Vorausschau integriert.
- **Formalisierung von Marktstrukturen**, in denen der private Sektor schnelle Innovation liefert, während der Staat legitime Attribution und souveränen Schutz gewährleistet.
- **Lehren aus dem „Informationsblackout“ von 2025** in anderen Rechtsräumen ziehen: Europa muss sicherstellen, dass öffentliche Finanzierung von Behörden ein nicht verhandelbarer Pfeiler nationaler Resilienz bleibt.
- Eine europäische Intelligence-Architektur muss einen **einheitlichen Cyber-Lagezentrum (Unified Cyber Situation Room)** umfassen. Dieses überbrückt die Lücke zwischen technischer Telemetrie (aus dem Privatsektor) und geopolitischer Intention (staatliche Dienste) und schafft ein gemeinsames Lagebild („Common Operating Picture“) für alle 27 Mitgliedstaaten, um kollektive Attribution zu ermöglichen.
- Auch wenn die „Aktivierung“ des Privatsektors für die Aufrechterhaltung der Geschäftskontinuität essenziell ist, muss die Dual-Use-Natur des nichtstaatlichen Intelligence-Marktes anerkannt werden. Um Risiken durch unregulierte kommerzielle Überwachungsstrukturen zu begrenzen, muss Europa einen **demokratischen Standard für private Intelligence-Anbieter** etablieren. Dieser stellt sicher, dass aktivierte private Experten innerhalb eines regulatorischen „Safe Harbor“ agieren und denselben ethischen Leitplanken sowie Transparenzanforderungen unterliegen wie souveräne staatliche Dienste.

13 Schlussfolgerung: Ein Aufruf zu strategischer Klarheit

Nachrichtendienstliche Erkenntnisse sind die Grundlage fundierter Urteilsbildung. Durch die Integration eines CTEM-basierten operativen Standards und die Anerkennung der KI-Governance-Lücke vollzieht Europa den Übergang von reaktiver „Cyberabwehr“ zu proaktiver strategischer Klarheit.

- Das Versäumnis, das digitale Umfeld richtig zu interpretieren, ist ein Versagen demokratischer Verantwortung. Intelligence muss als Versorgungsleistung verstanden werden – konstant, verlässlich und grundlegend. Dies befähigt nicht nur Staat und

Wirtschaft, sondern auch die Bürgerinnen und Bürger, sich in einer Ära der Desinformation zu orientieren.

- Eine europäische Intelligence-Architektur muss über reinen Informationsaustausch hinausgehen und **kollektive Attribution** ermöglichen. Der Unified Cyber Situation Room fungiert als „Hohes Gericht der Attribution“, das private technische Telemetrie mit staatlicher geopolitischer Bewertung verbindet. Wenn 27 Mitgliedstaaten mit einer gemeinsamen, evidenzbasierten Stimme sprechen, wird technische Intelligence zu einem wirksamen strategischen Abschreckungsinstrument und verleiht diplomatischen Reaktionen das notwendige politische Gewicht.
- Das Modell der **De-Priorisierung**, das zu Informationsblackouts führt, muss abgelehnt werden. 2026 ist Sichtbarkeit Abschreckung. Stete öffentliche und wissenschaftliche Finanzierung ist eine strategische Investition, die Gegnern signalisiert, dass man Grey-Zone-Manöver sofort erkennt und kollektiv attribuiert. Wenn hochauflösende Intelligence als verlässliche Versorgungsleistung behandelt wird, stärkt dies Staat, Wirtschaft und Gesellschaft gegen kognitive und strukturelle Sabotage.
- Die **„Patch-alles“-Illusion** muss aufgegeben werden. Erfolg misst sich daran, 99 % des technischen Rauschens ignorieren zu können, um jene 1 % der Schwachstellen auf dem kritischen Pfad zur Souveränität fehlerfrei zu verteidigen – identifiziert durch das CTEM-Radar.
- **Finanzierung ist Sichtbarkeit:** Wie die systemische Fragilität nach der De-Priorisierung von Behörden wie der CISA in den USA zeigt, sind Kürzungen bei Cyber-Intelligence-Budgets selbstzugefügte Verwundungen. Nur nachhaltige Finanzierung erhält den „Clearinghouse“-Effekt, der für kollektive europäische Verteidigung erforderlich ist.
- Der Übergang muss von **menschengeschwindigen Gremien zu agentischer Verteidigung** erfolgen. Systeme müssen selbstheilende Reaktionen ausführen können. Dies erfordert jedoch autonome Compliance: eine interne Schicht „digitalen Rechts“, die sicherstellt, dass maschinenschnelle Maßnahmen ethisch vertretbar, auditierbar und mit dem EU-AI-Act vereinbar bleiben.
- **Souveränität 2026 ist eine gemeinsame Aufgabe.** Ein formeller Rahmen, der private Innovation und akademische Forschung in Krisen aktiviert, ist für die Funktionsfähigkeit kritische Infrastrukturen auch unter hybriden Zwangslagen entscheidend.
- Während Gegner durch unregulierte KI an Geschwindigkeit gewinnen, **gewinnt Europa Resilienz durch Vertrauen.** Indem ethische Leitplanken fest in automatisierte Verteidigung integriert werden, stellen wir sicher, dass Sicherheit niemals auf Kosten unserer Werte erreicht wird. ■

Krieg im Kopf

Cognitive Warfare operiert mit Desinformation, Fake News und Manipulation. Organisationsexpertin Rafaela Kraus über psychologische Angriffsflächen moderner Gesellschaften, den Umgang mit Unsicherheit – und warum demokratische Resilienz lange vor der Technik beginnt.



Wie ordnen Sie den Begriff Cognitive Warfare ein – auch im Verhältnis zu klassischer Propaganda oder Informationskriegsführung?

Rafaela Kraus: Die Begriffe überlappen sich. Hybride Kriegsführung beginnt häufig mit der Spaltung von Gesellschaften. Medien spielen dabei eine zentrale Rolle: Denken wir an Deep-fakes, Fake News und gezielte Desinformationskampagnen. Hinzu kommt die Einflussnahme auf einzelne Personen, wie z.B. Politiker, die bewusst als Instrumente genutzt werden. Es geht aber insgesamt weniger darum, Menschen von bestimmten Inhalten zu überzeugen, sondern vielmehr darum, zu verunsichern und zu polarisieren – Gesellschaften auseinanderzubringen und dadurch angreifbarer, weniger resilient zu machen.

Cognitive Warfare ist also ein Teil hybrider Kriegsführung?

Ich denke schon. Auch klassische Sabo-

tageakte – etwa Stromausfälle – haben eine psychologische Komponente. Sie erzeugen den Eindruck, dass Politik und Institutionen unfähig sind, dass der Staat seine Bürger nicht schützt. Subversion ist dabei eine Eskalationsform: Bestehende innere Spannungen werden verstärkt, Minderheiten mit antidemokratischen Narrativen instrumentalisiert. Das sieht man etwa in den baltischen Staaten, wo russische Minderheiten gezielt über soziale Medien und spezifische Kanäle angesprochen werden.

Lernt hybride Kriegsführung dabei auch vom Terrorismus?

Die Methoden ähneln sich teilweise, aber es gibt einen wichtigen Unterschied. Im Falle eines Terroranschlags möchten sich die Täter meist als Verursacher zu erkennen geben. Beim hybriden Krieg und bei Cognitive Warfare ist dagegen Unklarheit die zentrale Strategie. War es Sabotage, ein Unfall, ein

INTERVIEW_ Rafaela Kraus

Prof. Dr. Rafaela Kraus ist Professorin für Unternehmens – und Personalführung an der Universität der Bundeswehr München. Sie forscht unter anderem über Intrapreneurship und Entrepreneurship, Defense/ Dual Use Innovation, Transformation (z.B. Autoindustrie und Verteidigung), Leadership und Organisationskultur.

KEY MESSAGES

→ **Cognitive Warfare** ist Teil hybrider Kriegsführung und zielt primär auf Verunsicherung, Polarisierung und Vertrauensverlust – nicht auf klassische Überzeugung.

→ **Ambiguität ist Strategie:** Unklare Urheberschaft wirkt destabilisierender als offene Gewalt.

→ **KI und skalierbare Desinformation** verstärken psychologische Effekte bei minimalem Ressourceneinsatz.

→ **Bildung, Medienkompetenz und produktiver Dissens** sind zentrale Verteidigungsinstrumente.

→ **Resilienz bedeutet:** Unsicherheit aushalten, ohne in Naivität oder Totalmisstrauen zu verfallen.

„Menschen müssen lernen, aktiv Fragen zu stellen: Woher kommt diese Information? Wem nützt sie?“

Rafaela Kraus

Einzel Täter, ein fremder Staat? Je diffuser die Zuschreibung, desto wirksamer die Strategie...

...weil wir mit Uneindeutigkeit schlecht umgehen können?

Genau. Unsere Gesellschaft basiert auf klaren Regeln. Wir sind es gewohnt, dass Konflikte benennbar sind, mit eindeutigen Eskalationsstufen. Grauzonen widersprechen unseren Erwartungen und Wahrnehmungen. Im Alltag fühlt es sich zwar nicht so an, als befänden wir uns im Krieg – und doch sind wir in einer Art Kriegszustand. Hinter den Kulissen ereignen sich viele Dinge parallel, deren Urheber wir nicht klar benennen können. Das macht die Bedrohung so ernst.

Ziel hybrider Kriegsführung ist also kollektive Verunsicherung – das erinnert an das psychologische Phänomen des Gaslighting.

Ja. Es wird ein Zustand erzeugt, in dem man der eigenen Wahrnehmung nicht mehr traut. Mit geringen Mitteln lassen sich Effekte erzielen, für die sonst militärische Gewalt nötig wäre. Man nutzt etwa sogenannte Wegwerfagenten oder „nützliche Idioten“, die glauben, das Richtige zu tun. Das ist extrem kosteneffizient im Vergleich zu einem offenen militärischen Angriff.

Nehmen wir das Beispiel des Berliner Blackouts im Januar. Welche Fragen sollte man sich da als Bürger stellen?

Das Wichtigste ist Aufklärung. Der Bevölkerung muss klar werden, dass wir uns in einer Situation befinden, in

der gegnerische Akteure gezielt versuchen, unsere Gesellschaft von innen heraus zu verunsichern und zu spalten. Es geht darum, Vertrauen in unsere Institutionen zu untergraben – in den Staat, in Behörden, Polizei, Bundeswehr. In anderen Ländern, etwa in Skandinavien, wird schon in der Schule für diese Gefahr sensibilisiert, ganz im Sinne einer Gesamtverteidigung. Dazu zählt auch Verteidigung in unseren Köpfen. Wir müssen akzeptieren, dass die „graue“ Kriegssituation Realität ist und eine gewisse Instabilität zur neuen Normalität gehört. Entsprechend braucht es Awareness in der Breite der Gesellschaft.

Awareness – das meint auch kritisches Denken und Medienkompetenz?

Absolut. Kritisches Denken und der Umgang mit Medien kommen in Schulen noch immer zu kurz. Das ist oft ein punktuelles Thema, dabei müsste es dauerhaft präsent sein. Menschen müssen lernen, aktiv Fragen zu stellen: Woher kommt diese Information? Wem nützt sie? Wenn man es nicht weiß, sollte man misstrauisch sein. In dem Moment, in dem wir uns instrumentalisieren lassen, hat der Gegner bereits gewonnen.

KI-Sprachmodelle können extrem überzeugende Texte generieren, mit denen sich massenhaft und skaliert Meinungen beeinflussen lassen – um etwa die Unterstützung für die Ukraine zu untergraben. Was kann man dagegen tun?

Wir brauchen mehr als nur technische

Abwehr. Nötig sind jetzt deutlich mehr Bildung, Informationskampagnen und strukturelle Resilienz. Covid hat gezeigt, wie schnell sich Verschwörungstheorien verbreiten. Seither ist zu wenig passiert. Andere Länder, insbesondere die baltischen Staaten, sind weiter, weil sie auch stark betroffen sind. Und wir müssen auch Unternehmen mitdenken: Resilienz kritischer Infrastrukturen, klare Standards, entsprechende Gesetze. Das kostet Geld und ist aufwendig – aber wir kommen nicht darum herum.

Gab es Momente, in denen Sie erkannten, selbst verwundbar für solche Mechanismen zu sein?

In der Startup-Bubble, in der ich ja oft bin, schimpft man gern auf Regulierung, die Schwerfälligkeit Europas, die Unfähigkeit, konzertiert zu handeln und wirklich zu kooperieren. Bei diesem Europa-Bashing ertappe ich mich schon manchmal. Ich frage mich, ob Europa-Bashing nicht auch Teil dessen ist, was hybride Kriegsführung bezweckt: dass wir Europa als nicht funktional empfinden und nur noch kritisieren, statt konstruktiv zu sein. Ich glaube, man muss aufpassen, dass man dieses Narrativ nicht einfach nachbetet. Es ist ja nicht völlig falsch – aber es spielt dem Gegner in die Hände.

Gibt es überhaupt noch Institutionen, denen man als Bürger komplett vertrauen sollte?

Das wahre Risiko besteht für mich im Entweder – Oder. Einerseits vertraut >

„Es ist unmöglich, alles abzusichern oder vorherzusehen. Wir werden mit Unsicherheit leben müssen.“

Rafaela Kraus

man Institutionen blind, weil da etwa „Spiegel Online“ drübersteht. Vielleicht klickt man aber auf eine Fake-Seite. Diese Naivität, auf vertraute Muster zu reagieren, weil sie seriös wirken, einen Anstrich von Wissenschaftlichkeit haben, ist fatal. Andererseits ist da die Gefahr des totalen Misstrauens gegenüber jeder Institution, der Wissenschaft, der Politik. Am Ende entwickelt man ein allumfassendes Misstrauen. Wir müssen einen Mittelweg finden: Bildung, um die eigene Naivität abzulegen - und zugleich Vertrauensbildung, um nicht überall Gespenster zu sehen.

Überreaktionen können Teil des Problems werden.

Genau. Wir können nicht alles schützen. Wenn ich an kritische Infrastrukturen denke: Energieversorgung, Krankenhäuser, Wasser, Logistik. Es ist unmöglich, alles abzusichern oder alles vorherzusehen und zu detektieren. Wir werden mit Unsicherheit leben müssen. Die Herausforderung ist: vorsichtig und sensibel sein, aber nicht den Kopf verlieren und unüberlegt reagieren. Als im Oktober letzten Jahres mehrfach Drohnen über dem Münchner Flughafen gesichtet wurden, wurden sofort Stimmen laut, die sagten: Die müssen alle abgeschossen werden. Das ist nicht immer die richtige Reaktion. Man kann nicht wie auf einem Gefechtsfeld einfach „wild rumballern“. Es gibt rechtliche Rahmenbedingungen, ein reguliertes Umfeld. Und Reaktionen müssen angepasst und verhältnismäßig sein

Das Beispiel Drohnen zeigt auch, wie es von einem Extrem ins andere kippen kann: Erst herrschte Alarmzustand, dann war das Thema plötzlich wieder von der Bildfläche verschwunden.

Genau. Und das zeigt die multidimensionale Herausforderung. Es geht darum, was es in den Köpfen bewirkt – aber auch um die reale Gefahr, etwa für einen Flughafen und den Flugbetrieb. Hier hat Wissenschaftskommunikation eine wichtige Aufgabe: Menschen dafür zu sensibilisieren, dass diese einfachen Schwarz-Weiß-Wahrheiten – „einfach abschießen“ – eben auch gefährlich sind. Solche Vereinfachungen können auch Teil von Cognitive Warfare sein.

Wir alle bewegen uns in Bubbles. Ist es nicht extrem schwierig, aus einer Gruppenmeinung auszuscheren?

Sicher, es ist schwierig. Genau deshalb ist das auch eine Bildungsaufgabe. Solche Mechanismen müssten schon in der Schule trainiert werden. Wie gehe ich damit um, wenn ich anderer Meinung bin? Wie argumentiere ich? Wie halte ich Widerspruch aus? Natürlich ist nicht jede abweichende Meinung automatisch gut oder richtig. Es kann auch sein, dass jemand völlig danebenliegt. Aber entscheidend ist, dass wir lernen, in den Dialog zu gehen und uns auf der argumentativen Ebene auseinanderzusetzen. Das halte ich für eine der zentralen Aufgaben.

Heißt das nicht auch, dass wir produktiven Dissens in der Gesellschaft viel stärker fördern müssten?

Ja, genau. Ein Beispiel: Ich war im Herbst auf einer Veranstaltung, die hieß „Sicherheitsdialog“. Da saß unter anderem ein Vertreter der Bundesschülerkonferenz auf dem Podium, außerdem eine Vertreterin der Feuerwehr und General André Bodemann, der am Operationsplan Deutschland mitgearbeitet hat. Ich fand das extrem gut, weil dort ganz unterschiedliche Perspektiven zusammenkamen – auch solche, die nicht automatisch konform sind. Genau das ist die Herausforderung: mehr Interdisziplinarität, mehr Perspektivenvielfalt statt Eindimensionalität.

Liegt das Problem auch an unseren institutionellen Strukturen?

Sehr stark sogar. In Forschungseinrichtungen und Hochschulen sind wir nach wie vor in Silostrukturen gefangen: Fakultäten, Departments, Disziplinen. Der Austausch ist begrenzt. Dabei könnten gerade die Sozialwissenschaften, etwa die Psychologie, enorm viel beitragen – ebenso die Technologie, die zeigt, was technisch möglich ist, zum Beispiel mit KI. Dazu kommt die Sicherheits- und Außenpolitik, die strategisches Verhalten von Akteuren versteht, und die Soziologie, die gesellschaftliche Dynamiken analysiert. Wir brauchen viel mehr interdisziplinären Austausch. Technologie wird in den Geistes- und Sozialwissenschaften manchmal als etwas Fremdes wahrgenommen – und genau das müssen wir überwinden, wenn wir zu besseren Lösungen kommen wollen.

>

„Mit KI haben wir bessere Möglichkeiten, interdisziplinär zu arbeiten und vernetzt zu denken.“

Rafaela Kraus

Wenn Sie sagen: Cognitive Warfare ist im Kern eine Bildungsaufgabe – gehört dazu nicht auch, Kinder früh als Individuen zu stärken und sie gegen übermäßigen Einfluss von Bubbles zu immunisieren?

Ja. Unser Schulsystem ist stark auf Konformität ausgerichtet: Regeln einhalten, sich anpassen. Vieles, was früher als Kern von Bildung galt – Wissen speichern, reproduzieren –, ist im Zeitalter von KI obsolet. Jetzt haben wir bessere Möglichkeiten, interdisziplinär zu arbeiten, vernetzt zu denken und Wissensgebiete zu erschließen, die früher unzugänglich waren. Früher mussten wir uns abgrenzen und fokussieren, weil das Wissen explodiert ist. Jetzt müssen wir wieder lernen, eigenständig, kritisch und auch breiter zu denken – ein Stück „undisziplinierter“ zu werden.

Was heißt das konkret fürs Lernen?

Eigene Fragestellungen zu entwickeln, kreativ und kritisch zu sein, das sind Fähigkeiten, die heute zentral sind – auch, um nicht anfällig zu werden für Manipulation, für gezielte Beeinflussung und für subversive Strategien.

Was lernen Sie von jungen Leuten und Start-Up-Gründern?

Eine Machermentalität. Dieses: nicht nur reden, sondern anfangen. Dinge ausprobieren, iterativ vorgehen, dranbleiben. Diese Beharrlichkeit, reale Probleme lösen zu wollen – nicht nur theoretisch darüber zu sprechen – finde ich faszinierend. Nehmen wir zum Beispiel Fake News: Wir Ältere diskutieren

oft abstrakt darüber, wie gefährlich sie sind. Start-ups gehen eher hin und fragen: Wie können wir sie technisch erkennen? Welche Methoden gibt es? Was lässt sich konkret bauen? Von jungen Leuten lässt sich auch lernen, ein sehr klares Gefühl dafür zu entwickeln, wozu Technologie heute in der Lage ist. Ob die Jungen allerdings grundsätzlich reflektierter sind und mehr Awareness für Manipulation haben als andere Generationen, da bin ich skeptisch. Ich glaube, wir sitzen da alle im selben Boot.

Sie glauben also nicht, dass die Gen Z subtiler Beeinflussung, etwa durch Sprachmodelle, weniger erliegt?

Da bin ich nicht so sicher. Aber insgesamt habe ich schon den Eindruck, dass Digital Natives mit Fake News souveräner umgehen als die Boomer-Generation, die teilweise mit größerer Gutgläubigkeit auf Inhalte schaut. Das ist keine wissenschaftliche Aussage, aber eine Beobachtung, die ich wiederholt gemacht habe. ■

Die Nebelmaschine der KI

Generative KI produziert Plausibilität im industriellen Maßstab. Was wie technischer Fortschritt erscheint, untergräbt leise die Grundlagen demokratischer Urteilsbildung. Europas wichtigste Sicherheitsfrage lautet mehr denn je: Wie bewahren wir eine gemeinsame Wirklichkeit?

Günther Anders, einer der maßgeblichen Denker des 20. Jahrhunderts, schrieb *Die Antiquiertheit des Menschen* im Jahr 1956 – zu einem Zeitpunkt, an dem das Atomzeitalter die Romantisierung technologischer Macht unmöglich gemacht hatte. Sein Ziel war es, einen neuen Zustand zu beschreiben.

Moderne Gesellschaften haben gelernt, Folgen in einem Ausmaß hervorzu- bringen, dem ihre Vorstellungskraft nicht mehr gewachsen ist. Wir waren in der Lage, Wirkungen zu erzeugen, die Kontinente und Jahrzehnte überspannten, doch es fiel uns schwer, sie klar vor Augen zu haben, sie wirklich zu empfinden und in einem angemessenen Verhältnis Verantwortung für sie zu übernehmen.

Anders bezeichnete diesen Zustand als die „prometheische Lücke“: die Diskrepanz zwischen dem, was Menschen hervorbringen können – etwa die Atombombe – und dem, was sie geistig und moralisch zu begreifen vermögen.

Er führte das Argument weiter aus.

Diese Diskrepanz hinterlässt Spuren im Selbst. Sie erzeugt prometheische Scham, ein Gefühl der Unterlegenheit gegenüber den eigenen Artefakten, als seien die Produkte menschlicher Hände und Systeme verlässlicher, präziser, perfekter als ihre Schöpfer. Für Anders lag die zentrale Gefahr in der menschlichen Reaktion.

Menschen passen sich dem an, was sie überfordert. Sie normalisieren es. Sie akzeptieren eine Welt, die sie nicht mehr verstehen, als neuen Normalzustand. Das Problem liegt dann weniger in einer einzelnen Technologie als in einer Zivilisation, die stillschweigend ihr Verantwortungsgefühl schwächt, um funktionsfähig zu bleiben. Deshalb ist Anders heute erneut relevant.

Europa tritt in eine Epoche ein, in der Bedeutung selbst im industriellen Maßstab produziert wird. Generative Künstliche Intelligenz (KI) kann Plausibilität schnell und kostengünstig erzeugen und den öffentlichen Raum mit Inhalten überfluten, die glaubwürdig wirken und klingen, noch bevor Bürgerinnen und Bür- ➤

TEXT_ Raluca Csernatonî

Dr. Raluca Csernatonî ist Fellow bei Carnegie Europe in Brüssel mit Schwerpunkt europäische Sicherheits- und Verteidigungspolitik sowie KI und neue Technologien. Sie leitet dort die Forschung zur Geopolitik von KI, zudem ist sie Gast- und Visiting Professor an der Vrije Universiteit Brussel, der University of Antwerp und forscht in mehreren EU-geförderten Projekten zu Cyber- und Digitalpolitik

KEY MESSAGES

- ➔ **Generative KI** verschiebt Sicherheitspolitik: Nicht Wahrheit selbst, sondern Plausibilität wird zur strategischen Ressource und zur Angriffsfläche.
- ➔ **Epistemische Unsicherheit** entsteht, wenn Gesellschaften Inhalte schneller produzieren als sie prüfen können.
- ➔ **Demokratische Ordnung** benötigt keine Einigkeit, aber eine minimale gemeinsame Wirklichkeit.
- ➔ **Plattformdesign und Algorithmik** sind sicherheitsrelevant und daher als Teil kritischer Infrastruktur zu sehen
- ➔ **Epistemische Resilienz** ist ein öffentliches Gut: Sie entscheidet, ob Europa urteils- und handlungsfähig bleibt.

ger oder Institutionen die Möglichkeit hatten, sie zu überprüfen. Das prometheische Paradox kehrt hier als eine Politik der Wahrnehmung zurück. Wir schaffen ein Umfeld, das unsere Fähigkeit übersteigt, es zu beurteilen – und in dieser Lücke gedeiht Disruption.

„Wenn geteilte Wirklichkeit zerbricht, schwindet demokratische Legitimität.“

Raluca Csernaton

Die prometheische Scham erfasst zusehends das Unbehagen, das entsteht, wenn KI-Systeme uns scheinbar übertreffen und Menschen beginnen, sich selbst als obsolet zu empfinden und maschinellen Urteilen den Vorrang zu geben – eine epistemische und emotionale Drift, die Autorität, Verantwortung und demokratische Zustimmung stillschweigend neu ordnen kann.

Europa sieht sich mit einer Bedrohung konfrontiert, die konventionelles sicherheitspolitisches Denken nicht erfassen kann: der industriellen Produktion von Plausibilität. Dies nenne ich epistemische Unsicherheit, und sie ist inzwischen ein

strategisches Problem erster Ordnung. Dennoch greifen europäische sicherheitspolitische Debatten weiterhin auf vertraute Themen zurück – von Netzwerken, Infrastruktur, Grenzen und Resilienz bis hin zur militärischen Einsatzbereitschaft. All dies ist notwendig. Doch zugleich wirkt ein leiserer Druck auf die strategische Landschaft. Er betrifft die Bedingungen, unter denen Europäer einander weiterhin verstehen, widersprechen und gemeinsam Entscheidungen treffen können. Er stellt infrage, ob eine gemeinsame Welt noch aufrechterhalten werden kann.

Hier liegt die strategische Verschiebung. Wenn geteilte Wirklichkeit zerbricht, schwindet demokratische Legitimität, Krisenmanagement verlangsamt sich, und Koalitionsbildung wird fragil. Solidarität bei Sanktionen, Verteidigung und der Unterstützung von Partnern lässt sich dann deutlich leichter untergraben.

Hier wird epistemische Sicherheit zentral. Sie bezeichnet die Widerstandsfähigkeit des Wissensökosystems, auf das demokratisches Leben angewiesen ist: glaubwürdige Institutionen, rechenpflichtige Expertise, eine Mediensphäre, die vermitteln kann statt bloß zu verstärken, gemeinsame Referenzpunkte, die Erschütterungen standhalten, sowie zivile Praktiken, die Menschen befähigen zu prüfen, zu schließen, zu zweifeln und zu revidieren. Epistemische Sicherheit wirkt auf der gesellschaftlichen Ebene. Ihre Einheit ist die Öffentlichkeit – jenes fragile Gefüge, das Information in geteiltes Urteil überführt.

Demokratie beruht auf einer fragilen Errungenschaft, die leicht zu übersehen und nach ihrem Verlust nur schwer wiederherzustellen ist: einer gemeinsamen Sicht auf die Wirklichkeit. Ein politisches Gemeinwesen braucht keinen vollständigen Konsens. Es braucht erkennbare

Streitpunkte. Wahlen. Haushalte. Kriege. Pandemien. Korruption. Verantwortung. Wenn diese gemeinsame Sicht zerbricht, wird Politik primitiver. Überzeugung weicht Dominanz. Öffentliche Vernunft wird durch tribale Gewissheit ersetzt. Wahrheit wird zur Waffe – geführt und durchgesetzt, beansprucht durch Lautstärke und Wiederholung.

Hybride Bedrohungen zielen seit Langem genau auf diese Ebene. Ihre Taktik ist Zersetzung. Sie gedeihen in Mehrdeutigkeit und Reibung. Sie verwischen die Grenzen zwischen echtem Dissens und orchestrierter Manipulation, zwischen Satire und Sabotage, zwischen Graswurzelmobilisierung und synthetischer Koordination. Ihr bevorzugtes Ergebnis ist Erschöpfung. Eine Bürgerin oder ein Bürger, der müde, zynisch und dauerhaft misstrauisch ist, lässt sich leichter lenken und schwerer mobilisieren. Eine Gesellschaft, die im Nebel lebt, hat Mühe, Solidarität aufrechtzuerhalten – sei es in Fragen der Migration, der öffentlichen Gesundheit, der Ukraine oder der Legitimität der Union selbst.

Es mag abstrakt erscheinen, bis man es sich in einer ganz gewöhnlichen Szene vor Augen führt. Ein Montagmorgen in einer kleinen europäischen Stadt. Eine Sprachnachricht verbreitet sich rasch, angeblich vom Bürgermeister. Sie warnt, dass die Wasserversorgung kontaminiert sei. Sie fordert dazu auf, Krankenhäuser zu meiden und auf „offizielle Anweisungen“ zu warten. Innerhalb weniger Stunden beginnt der Hamsterkauf. Notrufleitungen sind überlastet. Schulen diskutieren Schließungen. Die Richtigstellung erreicht die Öffentlichkeit erst, als diese bereits darauf eingestellt ist, ihr zu misstrauen. Als entscheidend stellt sich heraus, wie schnell Verwirrung zu einer politischen Tatsache wird. >

Generative KI wirkt auf diese Logik der Disruption wie ein Brandbeschleuniger.

Unter generativer KI versteht man Systeme des maschinellen Lernens – meist große neuronale Netze, die auf umfangreichen Sammlungen von Texten, Bildern, Audio- oder Videodaten trainiert wurden –, die neue Inhalte erzeugen können, die dem Gelernten ähneln. Sie können flüssige Texte, überzeugende Bilder, geklonte Stimmen, synthetische Clips sowie interaktive Gesprächsagenten erzeugen, die Dialoge aufrechterhalten und Persönlichkeit imitieren. Sie sind probabilistische Maschinen der Plausibilität. Sie können autoritativ klingen und zugleich unzutreffend sein. Sie können spielerisch und kreativ wirken. Sie können ebenso bürokratisch überzeugend und strategisch manipulativ eingesetzt werden.

Innerhalb des europäischen Informationsökosystems wirkt generative KI gleichzeitig in drei verschiedenen Dimensionen: Skalierung, Personalisierung und Geschwindigkeit.

Erstens die Skalierung. Die Produktionskosten sinken drastisch. Texte, Bilder und Audiodateien lassen sich in Mengen erzeugen, die die Möglichkeiten zur Überprüfung übersteigen. Was früher Teams erforderte, kann heute von wenigen Akteuren mithilfe von Prompts, Vorlagen und Distributionskanälen bewältigt werden. Synthetische Inhalte nehmen ein solches Ausmaß an, dass sie Sättigung erreichen. Die Herausforderung verlagert sich von der Erstellung zur Auswahl. Und diese Auswahl wird von Plattformarchitekturen und Algorithmen gesteuert, die Engagement, emotionale Wirkung und schnelle Reaktionen priorisieren.

Zweitens die Personalisierung. Einflussoperationen stützen sich nicht länger auf ein einziges übergreifendes Narrativ. Stattdessen erzeugen sie Mikro-Narrative,

zugeschnitten auf unterschiedliche Kränkungen, Sprachen und Subkulturen, jeweils abgestimmt auf Stimmung und Wortschatz einer Gemeinschaft. Eine Zielgruppe erhält ein politiknahes Briefing. Eine andere ein sarkastisches Meme. Eine dritte stößt auf einen Thread, der moralische Panik schürt. Propaganda wird so zur Massenindividualisierung.

Drittens die Geschwindigkeit. Generative KI beschleunigt die Volatilität von Narrativen. Gerüchte werden gestartet, verändert, „gewaschen“ und erneut ausgespielt – schneller, als Institutionen reagieren können. In einer mehrsprachigen Union verstärkt sich dieser Effekt. Ein und dieselbe Behauptung kann in einer Sprache platziert, in einer anderen umformuliert, durch synthetische Konten „validiert“ und anschließend als europäischer Streit zurückgespielt werden. Disruption verbreitet sich rasch. Korrektur kommt spät. Erschöpfung setzt bei bei-

„Wer hat das Recht, Wirklichkeit in einer umkämpften Öffentlichkeit zu definieren?“

Raluca Csernatoni

dem früher ein. Das Ergebnis ist eine besondere Art von Bedrohung. Sie ist intim und alltäglich. Das spektakuläre Deepfake ist nur die Schlagzeile. Die tiefere Wirkung besteht in permanenter, niedrigschwelliger Unsicherheit. Der Clip, der echt aussieht. Der Screenshot, der zu gut zur Geschichte passt. Das „geleakte“ Memo in makellosem Verwaltungston. Die Sprachnachricht von jemandem, dem man vertraut. Das freundliche Profil, das geduldig chattet und sich an die eigenen Sorgen erinnert.

Die Frage lautet dann weniger: „Ist das wahr?“ als vielmehr: „Kann ich überhaupt noch sagen, ob es wahr ist?“ Wenn Menschen das Vertrauen in ihre Fähigkeit verlieren, zu unterscheiden, werden sie selten zu aufgeklärten Skeptikern. Sie werden resigniert. Vertrauen wird kostspielig. Zynismus wird zur Bewältigungsstrategie.

Eine weitere Falle öffnet sich. Wenn alles fabrizierbar ist, kann alles bestritten werden. Akteure mit böswilliger Absicht gewinnen einen strukturellen Vorteil. Sie säen Zweifel und überlassen dem Ökosystem den Rest. Sie lassen das Argument selbst sinnlos erscheinen. Eine Öffentlichkeit, die Wahrheit nicht mehr als gemeinsamen Horizont erwartet, wird anfällig für jene, die Gewissheit am aggressivsten behaupten.

Autorität wird leichter zu imitieren und vorzutäuschen – und zugleich schwerer zu erkennen. Journalistische Stile, akademische Tonlagen und institutionelle Sprache lassen sich im großen Maßstab simulieren. Sicherheit im Auftreten kann flüssig nachgeahmt werden, um Expertise vorzuspiegeln. Die zentrale Frage verschiebt sich damit auf Autorität: Wer hat das Recht, Wirklichkeit in einer umkämpften Öffentlichkeit zu definieren? Wird diese Frage destabilisiert, folgt die demokratische Legitimität. >

Auch Einflussnahme (persuasion) verändert sich grundlegend. Das frühere Modell beruhte auf Rundfunklogiken, bei denen Botschaften an ein Publikum ausgespielt wurden. Generative Systeme ermöglichen nun interaktive Manipulation. Bots können Gespräche führen, schmeicheln, provozieren und über Zeit Vertrauen aufbauen. Einfluss wird relational; er verankert sich in Gemeinschaften und Mikrointeraktionen. Kognitive Sicherheit wird damit untrennbar mit sozialer Interaktion verknüpft.

All dies verändert Europas digitalen Konsum – die tägliche Aufnahme von Information, Emotion und Identitätssignalen. Die Metapher der digitalen „Ernährung“ ist hilfreich, weil sie Stoffwechsel und Gewohnheit betont. Eine Gesellschaft kann gelegentliche Toxine verkraften, gerät jedoch in Schwierigkeiten, wenn sich die gesamte Nahrungskette verschiebt.

Synthetische Inhalte, die auf maximale Aufmerksamkeit ausgelegt sind, drohen diese Ernährung in Junkfood zu verwandeln: hochgradig anziehend, emotional manipuliert und inhaltlich nährstoffarm. Die langsamen Folgen sind politischer Natur: verkürzte Aufmerksamkeitsspannen, gesteigerte Reaktivität, geringere Toleranz für Komplexität und eine stärkere Abhängigkeit von algorithmischer Kuratierung. Demokratische Tugenden wie Geduld, Maß und Nuance lassen sich zunehmend schwerer aufrechterhalten.

Europas kulturelles Gefüge ist davon tief betroffen. Ein politisches Gemeinwesen wird durch mehr zusammengehalten als durch Gesetze und Märkte. Es lebt von gemeinsamen Bezugspunkten und einer dünnen Schicht geteilter Wirklichkeit – gerade ausreichend für Debatte, solange man sich noch in derselben Welt bewegt. Beginnt diese dünne Schicht porös zu werden und zu zerfallen, wird Politik zum

„Europa muss epistemische Resilienz als öffentliches Gut behandeln.“

Raluca Csernatosi

Schauplatz unvereinbarer Wirklichkeiten. Hybride Akteure verschärfen bestehende Spaltungen, indem sie Kränkungen in Identitäten und Kontroversen in existentielle Konflikte verwandeln. Europa bringt zudem eigene Verwundbarkeiten mit. Koalitionspolitik lässt sich durch Mikroskandale destabilisieren. Medienvertrauen und digitale Kompetenz variieren stark zwischen den Mitgliedstaaten. Der Informationsmarkt ist grenzenlos, und Narrative zirkulieren mit Leichtigkeit zwischen Sprachen und Kontexten. Der Entscheidungsprozess der EU beruht auf Kompromiss – und Kompromiss setzt minimale gemeinsame Fakten voraus. Werden Fakten dauerhaft bestreitbar, lässt sich die Handlungsfähigkeit des Staatenverbunds deutlich leichter blockieren.

Es gibt zudem eine geopolitische Dimension. Ein großer Teil der kritischen Infrastruktur Europas wird von außereuropäischen Plattformen beeinflusst. Die KI-Fähigkeiten Europas hängen weitgehend von externen Rechenressourcen, Modellen und Cloud-Ökosystemen ab.

Das bedeutet nicht Ohnmacht, erfordert aber Nüchternheit. Epistemische Sicherheit darf nicht ausgeblendet werden, wenn die Architekturen, die das öffentliche Leben in Europa organisieren, anderswo gebaut und von Akteuren genutzt werden, die Disruption als Waffe begreifen.

Zugleich braucht Europa Ambition. Generative KI bietet reale Chancen – etwa einen breiteren Zugang zu Expertise, Unterstützung für Bildung, Übersetzung über Sprachgrenzen hinweg sowie Produktivitätsgewinne in öffentlichen Diensten und der Industrie. Die Herausforderung liegt in einer Governance mit Bewusstsein (awareness). Diese Systeme können oberflächliche Verarbeitung normalisieren und Urteilsvermögen delegieren. So werden Zusammenfassungen Standard; Verifikation wird optional; Entwürfe werden automatisiert; Denken wird performativ.

Europas Antwort muss epistemische Resilienz als öffentliches Gut behandeln. Zudem sollte Europa eine klare Haltung einnehmen – eine Art, sich in einem umkämpften Informationsumfeld zu bewegen: Vertrauensgerüste aufbauen, Prozesse verlangsamen, wo Überprüfung erforderlich ist, und verhindern, dass Gegner Geschwindigkeit, Skalierung und Zielgenauigkeit in Überlegenheit verwandeln.

Diese Haltung lässt sich in konkrete Schritte übersetzen.

Erstens: Aufbau von Verifikationsinfrastruktur im großen Maßstab. Die Authentifizierung offizieller Kommunikation, die Stärkung von Herkunfts- und Provenienzen für Medien sowie die Schaffung vertrauenswürdiger Mechanismen zur Identifikation synthetischer Artefakte werden zentral. Das ist vergleichbar mit zivilem Ingenieurwesen für die Öffentlichkeit: Es schafft Gerüste für Urteilsbildung in

einem Umfeld, das mit plausiblen Inhalten überflutet ist.

Zweitens: Kognitive Resilienz als zivilgesellschaftliche Kompetenz. Medien- und Digitalkompetenz müssen lebenslang und praxisnah angelegt sein. Sie sollten Aufmerksamkeitsgewohnheiten fördern – insbesondere das Verlangsamen, das Erkennen emotionaler Manipulation, das Aufspüren koordinierter Verstärkung sowie das Erlernen von Triangulation ohne Paranoia.

Drittens: Plattformdesign als sicherheitsrelevante Frage behandeln. Empfehlungssysteme, Algorithmen, Viralitätsmechanismen und Monetarisierungsanreize prägen das Informationsterrain ebenso grundlegend wie Grenzen das Territorium. Europa braucht Transparenz, die nutzbar ist, Rechenschaftspflichten, die durchsetzbar sind, und Designentscheidungen, die die Anreize für Empörung, synthetisches Engagement und koordinierte Manipulation reduzieren.

Viertens: Demokratische Institutionen gegen Aufmerksamkeits-Sabotage schützen. Wahlbehörden, öffentlich-rechtliche Medien, Gesundheitsbehörden und kommunale Verwaltungen benötigen Handlungsleitfäden und Ressourcen, um unter Bedingungen gezielt erzeugter Unsicherheit arbeitsfähig zu bleiben – einschließlich schneller Reaktionsfähigkeiten, sicherer Kommunikationskanäle und grenzüberschreitender Koordination zwischen den Mitgliedstaaten.

Fünftens: KI zur Stärkung demokratischer Resilienz einsetzen – nicht allein zur Wettbewerbsfähigkeit. KI kann dem Gemeinwohl dienen. Maschinelle Geschwindigkeit kann Narrative über Sprachgrenzen hinweg analysieren, koordinierte Operationen identifizieren, investigativen Journalismus unterstützen und Institutionen helfen, klar und schnell zu kommunizieren.

Und dann gibt es Anders' schwierigste Lehre. Die Gefahr liegt nicht nur in der Macht der Maschine, sondern in der menschlichen Anpassung, die ihr folgt. Eine Zivilisation kann sich an Nebel gewöhnen. Sie kann epistemische Erosion als Normalzustand akzeptieren. Sie kann Zynismus für Raffinesse halten. Sie kann auch Urteilsvermögen an Maschinen delegieren und dies als Realismus ausgeben.

Europa sollte sich diesem Trend entgegenstellen. Epistemische Sicherheit ist die demokratische Überlebensfunktion des kommenden Jahrzehnts. Sie schützt unsere gemeinsame Welt, das kulturelle Gefüge und die Bedingungen, unter denen vielfältige Gesellschaften weiterhin streiten, einander anerkennen und kollektiv handeln können.

Die zentralen Auseinandersetzungen der kommenden Zeit werden sich in den alltäglichen Infrastrukturen von Aufmerksamkeit und Bedeutung abspielen – in Feeds und Foren, in synthetischen Stimmen und glaubwürdig wirkenden Dokumenten sowie in der leisen Umformung dessen, wie Gesellschaften lernen und sich erinnern.

Günther Anders fürchtete eine Menschheit, die von ihren eigenen technischen Meisterwerken beschämt ist und versucht, sich der Verantwortung zu entziehen. Europa kann sich diesen Rückzug nicht leisten. Doch so klar sich die Aufgabe benennen lässt, so schwer ist sie zu erfüllen: Wie lässt sich geteilte Wirklichkeit schneller wiederherstellen, als Disruption sie auflösen kann? Und wie lässt sich menschliches Urteilsvermögen präsent, sichtbar und rechenschaftspflichtig halten – bevor wir uns im Nebel ganz zuhause fühlen? ■

Im KI-Zeitalter ist Mut die neue Sicherheit

von Jim Sengl und Felix Rieger

In Europa verwechselt man Sicherheit oft mit Stabilität. Wenn technologische Zyklen sich allerdings nicht mehr in Jahrzehnten, sondern in Monaten bemessen, ist diese Gleichsetzung von Sicherheit und Stabilität ein gefährlicher Trugschluss. Im 21. Jahrhundert ist Sicherheit etwas anderes, nämlich Handlungsfähigkeit.

Die geopolitischen Spannungen der letzten Jahre haben uns eine unbequeme Wahrheit vor Augen geführt: Die Zeit, in der wir uns blind auf internationale Partnerschaften verlassen konnten, ist vorbei. Wir müssen anerkennen, dass einstmals verlässliche Verbündete zunehmend dazu übergehen, wirtschaftliche Abhängigkeiten für politische Zwecke zu nutzen. Wenn Handelszölle und Marktzugang als geopolitische Waffen eingesetzt werden, wird unsere digitale Infrastruktur zur Achillesferse.

Dieses Risiko ist kein rein politisches, sondern auch ein wirtschaftliches. Wer seine sensibelsten Daten und Prozesse ausschließlich über externe Plattformen abwickelt, akzeptiert Kontrollverlust. Der Abfluss von Geschäftsgeheimnissen oder die Nutzung eigener Daten zum Training fremder KI-Modelle sind keine theoretischen Risiken, sondern reale Gefahren für die Wettbewerbsfähigkeit europäischer Unternehmen. Und wer in dieser Lage von „Sicherheit“ spricht, meint oft nur den Schutz des Status quo. Wer aber Sicherheit schaffen will, braucht Mut.

Regulierung ist das Fundament, Technologie das Haus

Ein wichtiger Schritt für die Zukunftsfähigkeit der Europäischen Union ist der AI Act. Dieses Regelwerk ist kein Hindernis, sondern schafft die notwendige Rechtssicherheit und einen klaren Ordnungsrahmen, in dem wir uns bewegen können. Aber: Wir dürfen uns nichts vormachen. Gesetze selbst schreiben keine Software. Regulierung definiert das Spielfeld; die Spieler:innen stellt sie nicht auf. >

Jim Sengl leitet das KI-Kompetenzzentrum Medien (KI.M), eine gemeinsame Initiative der Medien. Bayern GmbH und der Bayerischen Landeszentrale für neue Medien (BLM). Seine Arbeit im KI.M konzentriert sich auf die Unterstützung der Medienbranche in der rechtssicheren und zukunftssichernden Nutzung von Künstlicher Intelligenz.

Felix Rieger verantwortet die Öffentlichkeitsarbeit des KI-Kompetenzzentrum Medien (KI.M). In seiner täglichen Arbeit befasst er sich mit Künstlicher Intelligenz, Medieninnovation und Community-Building.

Das KI-Kompetenzzentrum Medien (KI.M) ist die zentrale Anlaufstelle für den Einsatz Künstlicher Intelligenz in der Medienbranche. Das Ziel des KI.M. ist es, die bayerische Medienbranche bei der rechtssicheren und zukunftssichernden Nutzung von Künstlicher Intelligenz zu unterstützen.

Technologische Unabhängigkeit definiert sich nicht allein durch den AI Act. Eine Aufgabe wie diese kann nicht allein von Jurist:innen bewältigt werden, sondern sie wird von Ingenieur:innen und Unternehmen mitgestaltet. Das KI-Kompetenzzentrum Medien (KI.M) unterstützt diesen Prozess: Wir verstehen uns als technische Ermöglicher, die den rechtlichen Rahmen mit notwendiger technologischer Substanz füllen.

Medien sind kritische Infrastruktur der Demokratie

Für die Medienbranche ist diese Unabhängigkeit existenziell. Wenn Redaktionen bei der Recherche oder der Content-Erstellung auf „Black Box“-Systeme angewiesen sind, deren Funktionsweise sie nur eingeschränkt verstehen und prüfen können und deren Betreiber politischen Launen unterworfen sind, opfern sie einen Teil ihrer Integrität.

Souveränität bedeutet hier ganz pragmatisch: Die Wahl zu haben. Die Wahl, ob Daten in eine Cloud in Übersee fließen oder lokal verarbeitet werden. Diese Wahlfreiheit erfordert eigene Hardware und physische Orte, an denen experimentiert werden kann.

In Bayern haben wir diese Orte geschaffen. Mit dem KI-Real-labor bieten wir bayerischen Medienunternehmen genau das, was der Markt oft verwehrt: Zugang zu High-End-Infrastruktur unter Wahrung der Datensouveränität. Mit eigener Hardware schaffen wir einen Möglichkeitsraum, der frei von Cloud-Zwang ist. Hier können Unternehmen mit uns den Einsatz von KI testen, indem wir KI-Prototypen entwickeln, ohne dass ihre Daten Europa verlassen. Das ist eine technische Antwort auf politische und ökonomische Unsicherheiten.

Hightech demokratisieren

Mut bedeutet auch, Wissen zu teilen und nicht in Silos zu

denken. Die Vorstellung, dass jedes mittelständische Medienhaus seine eigene KI-Infrastruktur im Alleingang aufbaut, ist illusorisch. Die Antwort auf die Übermacht globaler Tech-Konzerne kann nur Kooperation sein.

Das KI.M ist deshalb dem Open-Source-Gedanken verpflichtet: Die Erkenntnisse aus unseren Machbarkeitsstudien, die Codes und die technischen Dokumentationen verschwinden nicht unsichtbar in einer Schublade, sondern sind frei verfügbar in öffentlich zugänglichen Repositories. Wir demokratisieren den Zugang zu Hightech. Ein kleiner Lokalsender oder ein Fachverlag erhält durch das KI.M Zugriff auf Blaupausen, die sonst nur Großkonzernen vorbehalten wären. Das stärkt die wirtschaftliche Basis des Medienstandorts Bayern und macht uns als Gemeinschaft resilienter gegen äußere Schocks.

Die Lage ist ernst, aber sie ist gestaltbar

Europa hat eine Stärke: Wir können Institutionen bauen, die Bestand haben. Das KI.M ist ein bayerischer Beitrag zu dieser europäischen Aufgabe. Wir warten nicht darauf, dass sich die Großwetterlage ändert. Wir verbinden die notwendige juristische Expertise – etwa durch die praxisnahe Übersetzung des AI Act – mit konkreter technischer Entwicklung.

Letztlich ist Mut eine strukturelle Entscheidung. Es ist die Entscheidung, Geld und Ressourcen nicht nur in kurzfristige Effizienzgewinne zu stecken, sondern in langfristige Souveränität. Es ist die Entscheidung, notwendige Kompetenzen im eigenen Haus aufzubauen, statt Lösungen blind einzukaufen.

Wer die infrastrukturellen Grundlagen seiner digitalen Arbeit versteht und kontrolliert, muss politische Volatilität nicht fürchten. Sicherheit ist kein Schutzschild, den man einmal kauft. Sie ist eine kontinuierliche Bauaufgabe. Das KI.M hat die Werkzeuge dafür bereitgelegt. Jetzt liegt es an uns allen, sie auch zu nutzen. ■

„Die psychische Belastung wird massiv unterschätzt“

Blackout, Informationskrieg, psychische und physische Belastungen: Larysa Visengeriyeva beschreibt, wie Gesellschaften unter Druck funktionieren – und warum Vorbereitung kein Alarmismus, sondern Selbstwirksamkeit ist.

Larysa Visengeriyeva, wie haben Sie den Berliner Blackout persönlich erlebt?

Larysa Visengeriyeva: Der Blackout war für mich eine totale Überraschung. Gleichzeitig war er ein sehr klares Beispiel dafür, wie eine sogenannte „mentale Firewall“ zusammenbricht – also diese tief verankerte Annahme, dass hier schon nichts passieren wird, dass alles funktioniert. Genau das ist gefallen: die Erkenntnis, dass es eben doch passieren kann.

Wie sind Sie emotional und praktisch mit dieser Situation umgegangen?

Ich persönlich bin relativ gelassen geblieben. Ich bin in den 1990er-Jahren in der Ukraine aufgewachsen. Wer diese Zeit dort erlebt hat, weiß, was es heißt, keinen Strom, kein Benzin oder

keine Versorgung zu haben. In so einer Situation greife ich automatisch auf Erfahrungswerte aus meiner Kindheit zurück. Mir war klar: Das kenne ich.

Waren Sie dadurch konkret handlungsfähig oder eher psychologisch vorbereitet?

Wahrscheinlich beides. Ich wusste, was zu tun ist. Ganz konkret heißt das: Zuerst beobachtet man die Temperatur in der Wohnung und entscheidet, in welchem Raum man bleibt. Man zieht sich schichtweise an, um sich warm zu halten. Dann prüft man, welche unabhängigen Energiequellen es gibt, zumindest für Licht. Wir mussten tatsächlich noch Lampen und Stirnlampen besorgen. Gleichzeitig haben wir bei Nachbarn geklopft und gefragt, wer was hat. Diese Vernetzung hätte eigent-



INTERVIEW_ Larysa Visengeriyeva

Dr. Larysa Visengeriyeva ist eine Expertin für KI und MLOps. Ihr Fachbuch „The AI Engineer's Guide to Surviving the EU AI Act“ (2025) ist ein Leitfaden, um AI-Systeme rechtskonform und verantwortungsvoll in den Markt zu bringen. Als Mitgründerin von „Women in Defense Tech“ treibt sie die Transformation der europäischen Verteidigungsindustrie voran – mit klarem Fokus auf „Combat-Driven Innovation“ und weibliche Führung.

KEY MESSAGES

- **Ein Blackout ist kein isoliertes Ereignis.** Versorgung, Kommunikation und Arbeit brechen gleichzeitig weg.
- **Resilienz entsteht dort, wo Menschen schnell handlungsfähig werden** – durch Vorbereitung und lokale Netzwerke.
- **Die größte Schwachstelle moderner Gesellschaften** ist nicht Infrastruktur, sondern der Normalitätsbias und mangelnde Informationsresilienz.
- **Die Ukraine zeigt, wie Dezentralisierung und Selbstorganisation kollektive Handlungsfähigkeit sichern.**
- **Vorbereitung heißt Szenariodenken:** Plan A, B und C – nicht aus Angst, sondern um Ruhe, Kontrolle und Selbstwirksamkeit zu bewahren.

„Ein Blackout ist keine einzelne Störung, sondern eine Welle, die viele Lebensbereiche betrifft.“

Larysa Visengeriyeva

lich schon vorher existieren sollen.

Welche weiteren Schritte waren wichtig?

Wasser erhitzen zu können war zentral. Der Blackout passierte ja bei Minusgraden, da sind arme Getränke elementar. Danach organisiert man sich weiter über Freundeskreise. Es sind sehr einfache, aber entscheidende Dinge.

Wie lief die Kommunikation während des Blackouts?

In den ersten Stunden und Tagen war das Mobilfunknetz sehr instabil. Ich hatte zufällig noch eine ukrainische SIM-Karte im Roaming, die aus irgendeinem Grund funktionierte. Sobald man den betroffenen Bezirk verlassen hat, war Mobilfunk teilweise wieder verfügbar. Festnetz gab es gar nicht – ohne Strom kein Telefon.

Was bedeutet Resilienz für Sie, wie würden Sie das auf den Punkt bringen?

Resilienz ist die Fähigkeit, innerhalb kürzester Zeit handlungsfähig zu werden, unabhängig davon, was passiert.

Woran erkennt man Resilienz in den ersten 24 Stunden einer Krise?

Resilienz zeigt sich auf verschiedenen Ebenen, von der staatlichen bis zur persönlichen. Entscheidend ist, zu wissen, auf welcher Ebene man selbst Kontrolle hat. Diese Handlungsfähigkeit kann man trainieren oder man wird durch Krisen dazu gezwungen. Für mich ist Resilienz ein holistisches Systemdesign: robuste Infrastruktur, funktionierende Governance, eine vorbereitete Bevölkerung und vor allem Informationsresilienz. Gerade soziale

Medien eröffnen neue Angriffsflächen, mental und emotional.

Wie haben Sie Resilienz in Ihrem unmittelbaren Umfeld erlebt?

Es gab sehr positive Momente. Ältere Nachbarn, die nach dem Zweiten Weltkrieg aufgewachsen sind, kamen aktiv auf uns zu. Sie boten Campingausrüstung an und Hilfe, falls wir etwas bräuchten. Auch Behörden wie das Technische Hilfswerk habe ich als außerordentlich engagiert erlebt. Informationspunkte wurden eingerichtet, Menschen wurden orientiert, es gab Notunterkünfte. Das hat funktioniert.

Und was hat nicht funktioniert?

Der Blackout dauerte fünf Tage. Für Berlin und für Deutschland als drittgrößte Wirtschaftskraft ist das aus meiner Sicht zu lang. Besonders problematisch war, dass die Bundeswehr mit Feldküchen einspringen musste, um die Bevölkerung zu versorgen. Auch Supermärkte wie Lidl waren noch Tage später geschlossen. Für ältere oder vulnerable Menschen ist das ein massives Problem. Das hat klar gezeigt: An dieser Stelle hat das System nicht funktioniert.

Was unterschätzen Menschen in einer Blackout-Situation am meisten?

Entscheidend sind die Kaskadeneffekte. Viele denken bei einem Blackout nur an fehlenden Strom. Tatsächlich folgt eine Kette von Ausfällen: Der Herd funktioniert nicht, das Internet fällt aus, Arbeit und Kommunikation brechen weg, selbst Alltägliches wird kompliziert.

Glücklicherweise hat in Berlin die Wasserversorgung funktioniert. Wir hatten kaltes Wasser, aber immerhin Wasser – das ist für Hygiene und Würde enorm wichtig. Normalerweise gilt: kein Strom, kein Wasser. Dann wird es existenziell, bis hin zur Frage, wie man überhaupt noch zur Toilette geht. Hinzu kommt: Keine funktionierenden Geldautomaten, kaum Einkaufsmöglichkeiten. Diese Abhängigkeiten werden massiv unterschätzt. Ein Blackout ist keine einzelne Störung, sondern eine Welle, die viele Lebensbereiche gleichzeitig trifft.

Wenn wir Ihre Ukraine-Erfahrung miteinander verbinden: Was funktioniert wirklich, wenn Gesellschaften unter dauerhaftem Druck stehen?

In der Ukraine haben viele Menschen bereits in den 1990er-Jahren blackout-ähnliche Situationen erlebt. Und seit 2013 lebt das Land faktisch im Krieg. Diese Resilienz wurde nicht über Nacht aufgebaut, sondern über Jahre hinweg – weil es gar nicht anders ging. Während wir in Berlin fünf Tage ohne Strom waren, wurde die Stadt Dnipro in der Ukraine komplett lahmgelegt. Innerhalb von 24 Stunden war sie wieder einsatzfähig. Das ist keine Wertung, sondern ein Fakt, der zeigt, wie schnell Handlungsfähigkeit zurückkehren kann, wenn Strukturen und Routinen vorhanden sind.

Sie sprachen von einer „Mental Firewall“.

Wie kann man diese überwinden?

Die Mental Firewall ist ein kognitiver Schutzmechanismus: „Das kann hier >

„Die Freiwilligenhilfe in der Ukraine ist enorm stark. Ohne sie hätte das Land nicht überlebt.“

Larysa Visengeriyeva

nicht passieren.“ Sie hilft, Angst und Stress zu vermeiden – und das ist zutiefst menschlich. Aber in Krisen wird sie gefährlich. Die Ukraine hat diese Firewall durch reale Erfahrung verloren – durch Krieg. Ich wünsche mir sehr, dass es auch anders geht.

Also ohne dauerhafte Krise?

Ja. Wir sehen das in nordischen Ländern wie Schweden oder Norwegen. Dort gibt es eine systemische Vorbereitung. In Schweden bekommt jeder Haushalt eine Broschüre: „Im Falle eines Krieges oder einer Krise“. Darin stehen klare Botschaften wie: „Wenn Schweden angegriffen wird, geben wir nicht auf.“ Dazu kommen praktische Checklisten für den Alltag. Das ist nüchtern, nicht alarmistisch, aber klar.

Wie lässt sich das auf unsere Gesellschaft übertragen?

Indem wir Normalitätsbias und Verdrängung anerkennen, statt sie zu tabuisieren. Man kann Vorbereitung auch positiv framen: nicht als Angst, sondern als Stärke. Als Handlungsfähigkeit. Als Selbstwirksamkeit. Dafür braucht es Expertise aus Systemdesign, Psychologie und Governance. Aber die Beispiele existieren: Die Ukraine zeigt, was erzwungene Resilienz bewirken kann. Und Schweden zeigt, dass es auch durch vorausschauendes Systemdesign geht.

Welche soziale Infrastruktur brauchen wir, um Krisensituationen zu überstehen?

In Blackout-ähnlichen Situationen wird Selbstorganisation entscheidend. Man

ist zunächst auf sich gestellt, aber nicht allein: Nachbarn und lokale Netzwerke gewinnen an Bedeutung. Schnell entstehen informelle Formen der Selbsthilfe auf Nachbarschafts- oder Bezirksebene. Man klopft an die Türen, teilt Ressourcen, Informationen und Fähigkeiten. Länder wie Schweden empfehlen sogar, solche Strukturen und Übersichten über vorhandene Fähigkeiten im Vorfeld vorzubereiten.

Welche Rolle spielt dabei Information?

Eine sehr große. Jeder hat unterschiedliche Informationen, Erfahrungen und Kompetenzen. Manche wissen, wie man sich praktisch organisiert, andere haben medizinisches Wissen, wieder andere Planungserfahrung. Wenn man diese Perspektiven zusammenlegt, entsteht ein gemeinsames Lagebild, das allen hilft. Diese Form von geteilter Information ist essenziell für kollektive Handlungsfähigkeit.

Welche Lehren lassen sich hier aus der Ukraine ziehen?

In der Ukraine haben besonders kleine, lokale Gemeinschaften gut funktioniert – oft auf Dorf- oder Quartiersebene. Ein entscheidender Faktor war die Dezentralisierung, die bereits vor 2022 eingeführt wurde. Dadurch konnten lokale Verwaltungen, lokale Unternehmen und vor allem Ehrenamtliche sehr schnell handeln. Die Freiwilligenhilfe in der Ukraine ist enorm stark. Ohne sie hätte das Land nicht überlebt.

Was bedeutet das für das individuelle Mindset?

Es führt zu einem Bruch der „Mental Firewall“. Das Framing verschiebt sich von „Der Staat wird das regeln“ hin zu „Wir können uns nur auf uns selbst verlassen“. Das verändert das Verhalten fundamental. Menschen handeln schneller, pragmatischer und übernehmen Verantwortung – für sich und für andere.

Heißt das, man sollte sich nicht auf staatliche Anweisungen verlassen?

Man sollte zumindest einkalkulieren, dass es sie nicht geben wird. Nicht aus bösem Willen, sondern weil der Staat andere Ziele hat: Stabilität, Ordnung, das Vermeiden von Panik und ökonomischen Schäden. Ein bekanntes Beispiel ist die Ukraine: Nach späteren Angaben verfügte die politische Führung vorab über Hinweise auf eine großflächige Invasion und entschied sich, diese Information zunächst nicht öffentlich zu kommunizieren, unter anderem, um keine Massenpanik auszulösen.

Was folgt daraus für Krisensituationen bei uns in Deutschland?

Dass zentrale Anweisungen möglicherweise ausbleiben – sei es wegen ausgefallener Kommunikationskanäle oder aus strategischen Gründen. Darauf muss man vorbereitet sein. Soziale Infrastruktur bedeutet deshalb: lokale Netzwerke, Selbstorganisation, Vertrauen untereinander und die Fähigkeit, auch ohne zentrale Steuerung handlungsfäh zu bleiben.

Was ist Informationsresilienz? Meinen Sie damit die Fähigkeit, Informationen zu

„Informationsresilienz bedeutet auch, bewusst weniger konsumieren, selektiver sein und nicht alles teilen.“

Larysa Visengeriyeva

misstrauen – oder sogar ohne staatliche Informationen auszukommen?

Informationsresilienz bedeutet vor allem zu verstehen, dass man heute keine kinetischen Angriffe mehr braucht, um eine Gesellschaft zu brechen. Man kann sie mental destabilisieren und ihre Widerstandsfähigkeit massiv schwächen – so sehr, dass physische Kontrolle fast automatisch folgt. Informationskrieg ist eine parallele Kriegsform, gleichwertig zu klassischen militärischen Angriffen.

Was bedeutet das für Resilienz?

Vorbereitung auf Informationsangriffe ist genauso wichtig wie physische oder infrastrukturelle Vorbereitung. Informationsresilienz heißt, Abwehrmechanismen zu haben: individuell und kollektiv. Zu wissen, wie Manipulation funktioniert – und wie man sich dagegen schützt.

Gibt es dafür konkrete Beispiele aus der Ukraine?

Ja. Ein sehr wichtiges Beispiel ist der Umgang mit Echtzeitinformationen aus Kriegsgebieten. Die ukrainischen Geheimdienste haben sehr intensiv mit der Bevölkerung gearbeitet, um klarzumachen: Wer Raketen- oder Einschlagssorte postet, hilft dem Feind. Viele Menschen haben das anfangs nicht verstanden – jeder hat ein Smartphone, jeder filmt, jeder will posten. Aber solche Bilder liefern eine präzise Zielbestätigung.

Wie reagiert man darauf?

Mit klaren Regeln und Konsequenzen.

Das war keine moralische Debatte, sondern eine sicherheitsrelevante Notwendigkeit. Nur so konnte dieses Verhalten gestoppt werden. Parallel dazu wurden offizielle Informationskanäle etabliert: verlässliche Telegram-Kanäle, Bots, über die Beobachtungen gemeldet werden konnten, ohne sie öffentlich zu verbreiten.

Also eine bewusste Steuerung von Informationsflüssen?

Genau. Heute wissen in der Ukraine fast alle, welche Kanäle offiziell sind und welchen man vertrauen kann. Informationen werden gesammelt, geprüft und erst dann verbreitet. Die Bevölkerung wurde regelrecht „trainiert“, Informationen nicht impulsiv zu konsumieren oder weiterzugeben.

Gibt es dafür auch zivile Vorbilder außerhalb der Ukraine?

Ja, zum Beispiel Schweden. Dort wird empfohlen, Informationen grundsätzlich über mehrere offizielle Kanäle zu verifizieren, bevor man handelt. Erst prüfen, dann reagieren. Das ist Teil staatlich unterstützter Informationsresilienz.

Woran erkennt man Manipulation auf alltäglicher Ebene?

Ein ganz einfaches Signal sind starke Emotionen. Wenn eine Nachricht extreme Angst, Wut oder Hass auslöst, ist das ein Warnzeichen. Emotionen sind fast immer der Träger von Manipulation. Das zu erkennen, ist ein zentraler Bestandteil von Informationsresilienz.

Wie setzt man das um?

In der Ukraine war das ein langer Lern-

prozess. Aber er zeigt: Informationsresilienz ist nicht abstrakt. Sie ist erlernbar – und entscheidend für die Handlungsfähigkeit einer Gesellschaft in Krisen.

Wie sollte man in Krisensituationen mit Informationen umgehen?

In einer Krise neigen Menschen instinktiv zum „Doomscrolling“. Man konsumiert pausenlos Informationen, in der Hoffnung, Kontrolle zurückzugewinnen. Das ist völlig menschlich – aber genau das Falsche. Denn in solchen Momenten werden gezielt Bots und Desinformationskampagnen aktiviert, die Angst, Verwirrung und Unsicherheit verstärken sollen. Informationsresilienz bedeutet deshalb auch „information diet“: bewusst weniger konsumieren, selektiver sein und nicht alles teilen.

Kommen wir noch einmal auf den Blackout zurück. Wie hat sich in diesen Stunden und Tagen Ihre Wahrnehmung der Realität verändert?

Das ist etwas, was aktuell sehr viele Menschen in der Ukraine erleben. Man kennt dieses Phänomen auch aus dem Bergsteigen: Kälte verändert deine kognitiven und psychischen Fähigkeiten massiv. Alles dauert plötzlich viel länger – Entscheidungen, Denken, Handeln. Man kann nicht mehr so funktionieren wie im Normalzustand.

Also nicht nur organisatorisch gesehen, sondern auch körperlich und mental?

Genau. Man denkt zunächst: Ich ziehe mich warm an, dann kann ich wieder normal arbeiten, telefonieren, deken. ➤

„Krieg beginnt und endet nicht beim Militär. Er betrifft immer die Schwachstellen einer Gesellschaft – Informationsräume, Infrastruktur, Psyche, Alltag.“

Larysa Visengeriyeva

Aber so funktioniert es nicht. Der Körper schaltet in einen Sparmodus. Dein Körper gehört dir nicht mehr vollständig – und dein Geist auch nicht. Dieses Erkenntnis kam bei mir relativ spät, aber sie ist zentral.

Was bedeutet das Ihrer Erfahrung nach für längere Krisenlagen?

Es bedeutet, dass man die psychische Belastung massiv unterschätzt. In der Ukraine sehen wir derzeit einen enormen Anstieg psychischer Schäden. Dauerstress, Kälte, Unsicherheit – das alles verändert Menschen nachhaltig. Resilienz ist also nicht nur eine Frage von Infrastruktur oder Organisation, sondern auch von psychischer Belastbarkeit und Regeneration.

Welche Gewohnheit sollten wir uns zur Vorbereitung auf solche Krisen aneignen?

Die wichtigste Gewohnheit ist, zu akzeptieren, dass wir in unsicheren Zeiten leben. Das ist nichts Dramatisches – es ist schlicht Realität. Und darauf kann man sich vorbereiten. Stichwort: Szenariodenken.

Was heißt das praktisch?

Ganz banal: Plan A, Plan B, Plan C. Mit der Familie durchsprechen. Wo kaufen wir ein, wenn der Supermarkt zu ist? Wie kommunizieren wir, wenn Mobilfunk ausfällt? Wo treffen wir uns, wenn nichts mehr funktioniert? In Kyjiw hatten viele Familien feste Regeln: Eine Hauptperson, bei der sich alle melden – „Uns geht es gut“. Solche Absprachen wirken banal, aber sie beruhigen enorm, weil man weiß, was zu tun ist.

Das wäre also ein Gegenmittel zur „Mental Firewall“.

Genau. Nicht den Kopf in den Sand stecken, sondern vorbereitet sein – ohne Panik, ohne Alarmismus. Vorbereitung ist Beruhigung.

Sie sprechen für eine Community von Frauen im Bereich Defense Tech. Welche Botschaft möchten Sie abschließend mitgeben?

Die wichtigste Erkenntnis ist: Krieg beginnt und endet nicht beim Militär. Er trifft immer die Schwachstellen einer Gesellschaft – Informationsräume, Infrastruktur, Psyche, Alltag. Deshalb sollte sich jede und jeder fragen: Bin ich selbst eine Schwachstelle – oder Teil der Resilienz? Awareness ist der erste Schritt. Und Verantwortung beginnt nicht „oben“, sondern bei uns selbst. ■

Intelligence ohne Staat?

Open Source Intelligence, soziale Medien und KI verschieben die Macht über Information. Die Demokratisierung von Intelligence erfordert neue Regeln für Wahrheit, Verantwortung und Sicherheit.

In den 1980 Jahren in der damaligen Sowjetunion lebten Menschen in großer Angst, dass Nachbarn, Freunde, Kollegen sie ausspähen würden, dass das Gesagte oder das Erscheinen an „verbotenen Orten“ wie z.B. einer religiösen Stätte, das Gesehen werden mit jemanden, z.B. der aus dem Ausland kommt, an den gefürchteten Geheimdienst, die KGB, herangetragen werden. Misstrauen, Angst und leise Töne beherrschten den Alltag. Der gesellschaftliche Alltag war durch den Kalten Krieg, wenige Nachrichtenkanäle und Feindbilder geprägt. Auch damals fanden Menschen alternative Quellen der Information, brachten sich allerdings damit in Gefahr.

Ein fast halbes Jahrhundert später erleben wir eine Wende. Der Zugang zu nahezu allen Informationsquellen, teilweise zu personenbezogenen Daten und möglicherweise auch zu sensiblen Informationen ist möglich. Mit etwas technischem Geschick lassen sich mithilfe von Open Source Intelligence (OSINT), Human Intelligence (HUMINT) und KI-Tools Geodaten, persönliche Daten, Verhalten, Haltungen und vieles mehr sammeln, auswerten und veröffentlichen. Ein Vorgehen, das wenige Jahrzehnte zuvor Menschen ihre Freiheit oder zumindest ihre Karriere und ihren Sozialstatus gekostet hätte, heute jedoch gewisse Normalität.

Eine neue Dimension erreicht die Open Source Intelligence (OSINT) im russischen Angriffskrieg gegen die Ukraine. Bereits im Februar 2022 haben OSINT Analysten durch Analysen von Geodaten, Social Media Posts und Auswertung von Webcams Truppenbewegungen an der ukrainischen Grenze beobachtet. Social-Media-Kanäle auf Tik-Tok und Instagram werden zu Quellen fürs Lokalisieren von feindlichen Truppen. Es findet eine Verschränkung von privaten und staatlichen Akteuren in der Kriegsintelligence statt. Monitoring War, OSINT for Ukraine und DeepStateMap sind nur einige der privaten Initiativen und NGOs, die sich an Intelligence im Krieg, übrigens nicht nur in der Ukraine ansässig, beteiligen. Intelligence im neuen Zeitalter ist >

TEXT_ Irina Rosensaft

Irina Rosensaft ist Expertin für Digitale Transformation und Cybersicherheit – an der Schnittstelle von IT, Organisationsprozessen und Zivilgesellschaft. Mit einem politikwissenschaftlichen Hintergrund und fundierter Erfahrung in Prozessoptimierung, Change Management und Cybersicherheit schlägt sie eine Brücke zwischen Technologie, Governance sowie organisatorischen und gesellschaftlichen Anforderungen.

KEY MESSAGES

- **Intelligence** verliert ihr staatliches Monopol und wird durch OSINT, KI und digitale Vernetzung zunehmend kollektiv.
- **Zivilisten und private Akteure** gewinnen Analysefähigkeit und beeinflussen politische Entscheidungen.
- **Der Ukrainekrieg** zeigt Chancen kollektiver Intelligence, aber auch Risiken von Fehlinterpretation und Manipulation.
- **KI steigert Effizienz**, kann Fehler und Biases jedoch massiv verstärken.
- **Demokratische Gesellschaften** brauchen neue Regeln für Deutungshoheit, und Validierung von Informationen.

eine kollektive Aufgabe geworden, die mithilfe von digitalen Technologien ihren Höhepunkt erreicht. Private Akteure ergänzen und ersetzen staatliche Funktionen – wer prüft aber den Wahrheitsgehalt?

Weiterhin verbleiben klassifizierte Daten und Informationen bzw. Verschlusssachen in der Hand der nachrichtendienstlichen Aktivitäten zwischen Staaten; sie gewinnen gerade in der sich zugespitzten geopolitischen Lage an Bedeutung. Die globale Vernetzung und die jederzeit verfügbare Masse digitaler Daten erhöhen dieses Informationsmonopol zunehmend aus.

Früher brauchte Kontrolle über Information und somit über Staat und sein Handeln Spitzel, heute steckt beiläufig sensibelste Information in jedem Smartphone. Spitzel werden durch Klicks, Fotos, Metadaten und offene Quellen ersetzt.

DIE EVOLUTION VON INTELLIGENCE - VOM STAATLICHEN MONOPOL ZUR PRIVATISIERUNG

Was ist eigentlich Intelligence? Mark M. Lowenthal bezeichnet in seinem Werk *Intelligence: From Secrets to Policy* diese treffend als ein Produkt aus Sammeln, Verarbeiten, Bewerten und Analysieren von Interpretationen mit dem Ziel politische und militärische Entscheidungsträger zu unterstützen. Viele Jahrhunderte haben Staaten und ganze Reiche Informationen einen besonderen Wert beigemessen und sie kontrolliert. Bereits im 16. Jahrhundert sprach man über geheimnisvolle Nachrichten und über Spionage. Wenige Jahrhunderte später erlangte Intelligence ihren Höhepunkt als systematischer organisierter Prozess, ebenfalls dem Militär und der Polizei zwecks innerer und äußerer Sicherheit vorbehalten. Zu Beginn des 20. Jahrhunderts entstanden

„Staaten verlieren ihr Informationsmonopol, Zivilisten gewinnen es zunehmend.“

Irina Rosensaft

Zwischen Zentralisierung und Diversifikation liegen vermeintlich Welten. Beruhigend finde ich weder das eine noch das andere. Bei allen Vorteilen für die Verteidigung meines Geburtslandes Ukraine lässt mich die Privatisierung solch sensibler und bisher Staaten vorbehaltender Bereiche, die unter anderem über Krieg und Frieden entscheiden, aufhorchen. Was, wenn diese Daten nicht korrekt sind oder – ggf. absichtlich – falsch gelesen und übermittelt wurden. Sind wir Menschen heute selbst dafür verantwortlich, die Wahrheit zu definieren und rauszufinden?

Staaten verlieren ihr Informationsmonopol, Zivilisten gewinnen es zunehmend. Die Entwicklungen der letzten Jahrzehnte lassen daher die Frage aufkommen: Wem gehört Information im 21. Jahrhundert? Wer entscheidet über die Richtigkeit der daraus gezogenen Schlüsse und auch, wer hat die Hoheit darüber, was davon veröffentlicht wird? Wer trägt Verantwortung und Konsequenzen über die Schlüsse, die wir daraus ziehen? Wie verändert die Privatisierung von Intelligence den Staat und seine Souveränität? Um zu verstehen, was sich gerade entstaatlicht und privatisiert, lohnt sich ein Blick darauf, wie sich der Begriff und seine Praxis verändert haben. Dieser Paradigmenwechsel zeigt, dass wir neue Rahmenbedingungen für Intelligence brauchen.

moderne Geheimdienste bzw. Nachrichtendienste und führten zur Institutionalisierung von Intelligence. Der Besitz von geheimen Informationen und die Kontrolle über Informationsverbreitung werden teils bis heute mit Macht assoziiert. Staaten wie Maos China sahen Informationen als Herrschaftsinstrument. Der britische Premierminister Benjamin Disraeli hingegen wertete den Besitz von Information als Mehrwert für den Erfolg eines Individuums. In unterschiedlichen Kontexten und mit unterschiedlichen Zielen hielten diverse Staaten und Staatsmänner Information für ein Instrument zur Herstellung von Sicherheit und Ordnung.

Der geheimdienstliche Informationsgewinnung und -auswertung sowie deren Nutzung im Auftrag von Machthabern standen früher im Fokus. Die Praktiken dienten dazu, Sicherheit im Inneren sowie Bedrohungen von außen früh zu erkennen und abzuwehren. Das Sammeln von Informationen bezog sich auf Terrorismus oder Staatsfeinde im In- und Ausland, Militär, Spionage und Diplomatie. Lowenthals Definition gilt für staatliche Intelligence. Digitalisierung macht sie kollektiv.

Mit der Demokratisierung von Gesellschaften und Wissen im Zuge der Digitalen Revolution verändert sich auch das Ver- ➤

ständnis von Informationshoheit. Diversifizierung von Informationsquellen, Transparenz von Daten in offenen Quellen durch das Internet, Plattformdaten, Sensoren, Social Media Plattformen eröffnen eine unendlich große Variation und Anzahl von Möglichkeiten, Daten und Informationen zu erhalten, zu analysieren und bereitzustellen.

Wir befinden uns also in einer übervollen Informationsumgebung, und es stellt sich die Frage: Wer ordnet, filtert und interpretiert Informationen und mit welchem Zweck? Bleibt die Herstellung der Sicherheit zentral oder sind auch andere Ziele der Informationsgewinnung und -auswertung zu verzeichnen?

Mit Diversifizierung und Transparenz rücken auch nicht-staatliche Akteure in den Vordergrund. Sie bedienen sich der Möglichkeiten, den Meinungsdiskurs voranzubringen, Wahrheiten ans Licht zu bringen und vielfältig zu informieren. Staaten behalten ihre Geheimnisse, aber Zivilisten gewinnen weiter an Bedeutung: Neue Akteure sind Threat-Intelligence-Unternehmen, NGOs, Journalist:innen, lose OSINT-Communities und Ehrenamtliche, die in Krisen wie der Ukraine fehlende staatliche Ressourcen ausgleichen. Auch Tech-Unternehmen, die Daten sammeln, aufbewahren und so Intelligence-Kompetenzen aufbauen, zählen dazu.

Künstliche Intelligenz verstärkt die Entwicklung gravierend. Sie sammelt nicht nur in Rekordzeit Daten. Sie ist auch in der Lage, größere Datenmengen in Sekundenschnelle auszuwerten, Anomalien zu erkennen und in Zusammenhang mit anderen relevanten Ereignissen zu stellen. All das, was Menschen in Nachrichtendiensten früher in mühsamer Arbeit zusammentrugen und ausgewerteten, erledigt heute die Maschine.

Während der Mensch weiter zentral bleibt, findet im neuen Zeitalter von Intelligence eine Interaktion von Menschen und Maschine statt, wenn es darum geht, die richtigen Daten zu extrahieren und gezielte Information zu erhalten. Dies eröffnet neue Chancen, aber erfordert auch eine neue Verantwortung.

KOLLEKTIVE INTELLIGENCE - CHANCE ODER BÜRDE?

Die Demokratisierung von Informationen klingt erst mal befreiend und passend für die freiheitlichen und liberalen Werte. Um Chancen und Risiken in der modernen Intelligence-Arbeit zu identifizieren, sollten wir die Ziele und Absichten hinter Intelligence nicht außer Acht lassen. Im Kern geht es darum, Sicherheit durch Risikominimierung für politische und militärische Entscheidungsprozess zu gewährleisten; etwa im Falle von Terrorismus, Cyberangriffen und staatlichen Aggressionen. Intelligence soll Entscheidungen erleichtern und Gefahren abwehren.

Im Fall von Ukraine-OSINT helfen Zivilisten, das Land zu verteidigen, Propaganda zu entlarven und Kriegsverbrechen aufzudecken. Der transparente und unmittelbare Zugang zu Informationen ohne Filter liefert schnell und effektiv Informationen. OSINT wirkt an vielen Stellen wie die moderne Partisanenarbeit einerseits und ein Dienst am eigenen Land, ohne dafür offizielle Positionen übernehmen zu müssen. Doch wer bewertet die Echtheit und die Richtigkeit der gesammelten Informationen, besonders im Zeitalter des Digitalen, bei dem diese genauso schnell manipulierbar sind, wie sie entstehen?

Werden Informationen schnell über Social-Media-Kanäle veröffentlicht, können diese positiv oder auch negativ (Entstehen von Panik) die öffentliche Meinung und das öffentliche Handeln beeinflussen. Ein banales Beispiel der Manipulation von Geodaten liefert uns der Berliner Künstler Simon Weckert: In einem Experiment zog er rund 100 Smartphones in einem Bollerwagen durch Berlin und täuschte so Google Maps einen Stau vor. Das System erkannte dies und leitete die Nutzer:innen um. Dieser Fall illustriert die Manipulierbarkeit von öffentlichen Quellen und die Lenkbarkeit von Verhalten.

Die neu gewonnene Freiheit lässt sich nicht unkritisch nutzen. Die Richtigkeit und Deutungshoheit stehen hier auf dem Prüfstand. Die modernen Datensammler könnten an manipulierte Daten geraten sein. Daten, ohne einen weiteren Kontext >

„Was Menschen in Nachrichtendiensten früher in mühsamer Arbeit zusammentrugen, erledigt heute die Maschine.“

Irina Rosensaft

zu analysieren, könnte ebenfalls zu falschen Schlüssen führen.

Kritisches Denken und Digitale Mündigkeit von Nutzer:innen und Nutzern wird essenziell im 21. Jahrhundert. Informationen gelangen ungefiltert an uns, und diese zu validieren, ist wichtig. Das Gesehene und Gehörte zu hinterfragen und daraus Schlüsse zu ziehen, die Informationen in einen Kontext zu stellen, ist heute ebenfalls eine individuelle Aufgabe. Die Diversifikation von Quellen und Akteuren führt einerseits dazu, dass wir weit mehr Informationen und Quellen als je zuvor nutzen können, um die Wahrheit herauszufinden, Risiken zu minimieren – und dann eigenständig und verantwortungsvoll zu handeln. Die Qualität von Quellen zu prüfen und Informationen zu validieren ist eine notwendige Kompetenz für das neue Zeitalter.

Im Cyberraum existieren viele schädliche Phänomene wie Manipulation, Ausspähen, Identitätsdiebstahl. Über diese Phänomene informiert zu sein und auch erste Handlungsoptionen an die Hand bekommen, wie man sich dagegen schützen kann, ist entscheidend. Neben Entstaatlichung und Diversifizierung zeigt sich ein weiteres Risiko. Die Effizienzsteigerung von Intelligence durch KI-gestützte Tools kann Fehlentscheidungen massiv verstärken. Der menschliche Verstand und die menschlichen Schutzmechanismen bleiben also selbst oder gerade im digitalen Zeitalter eine tragende Säule von Intelligence.

Maccabi Fans gekommen war. Nur erwies sich diese Risikoanalyse, wie BBC berichtete, als eine Halluzination der von der Polizei eingesetzten KI. Laut Untersuchungsberichten übernahmen die Polizeibeamten diese Information, ohne sie weiter zu prüfen, und erstellten einen Sicherheitsbericht. Die Kosten dieser falschen Informationsauswertung sind hoch. Es kam zum Ausschluss von zwei Tausend Personen basierend auf ungeprüfter Information und der daraus entstandenen Risikoanalyse.

Während ich diesen Artikel schreibe, sind noch viele Fragen ungeklärt. Wie kam es zu dieser ungewöhnlichen Halluzination eines KI-Tools, wurde das Tool kompromittiert? Liegt der Fehler bei der KI oder bei den Beamten, die diese bedienten? Zumindest wurden Konsequenzen gezogen, nicht nur personelle, sondern auch im Hinblick auf den Einsatz von KI durch die Polizei. Der Fall ist ein diplomatischer Fauxpas.

Doch der Fall erteilt uns eine weitere wichtige Lektion: Intelligence ist weiterhin eine sensible Angelegenheit; die Sicherheit und Validität von Daten aus öffentlichen Quellen, die von privaten Unternehmen bereitgestellt werden, sind hoch problematisch. Der Fall zeigt das Versagen von staatlichen Institutionen, die mit Hilfe von Technologie falsche Entscheidungen trafen. Ihre Intelligence hätte andere verlässliche Quellen wie z.B. Sicherheitsbehörden anderer Länder wie Dänemark oder Holland

„Eine der größten Herausforderungen moderner Gesellschaften ist es, die Deutungshoheit über Daten und Informationen zu behalten.“

Irina Rosensaft

DEUTUNGSHOHEIT – WAS MODERNE GESELLSCHAFTEN LERNEN MÜSSEN

Im November 2025 sorgte das Fußballspiel zwischen Aston Villa und Maccabi Tel Aviv für Furore. Den Maccabi Fans wurde komplett untersagt, das Stadion zu betreten. Es hieß, es gäbe massive Sicherheitsbedenken. Das Spiel wurde zu einem Hochrisikospiegel erklärt. Doch was diente der Polizei von West Midlands als Wissensgrundlage für diese Erklärung? Diese wurde auf ein Spiel zwischen West Ham United und Maccabi Tel Aviv zurückgeführt, bei dem es angeblich zu Gewalteskalation von Seiten der

nutzen sollen. Es hätten auch sonstige nicht überprüfte offene Quellen sein können. Eine der größten Herausforderungen moderner Gesellschaften ist es, die Deutungshoheit über Daten und Informationen zu behalten. Deutungshoheit ist kein Selbstläufer, sondern bedarf bestimmter Richtlinien und Mechanismen, um zum Wohle der Sicherheit und Ordnung eingesetzt zu werden und nicht gegen demokratische Werte wie hier Diskriminierung einer Gruppe basierend auf Biases und Falschinformation zu ermöglichen. Zunehmend wird es schwieriger Datensicherheit zu gewährleisten, Geschäftsgeheimnisse zu wahren und Ver- >

schlussachen vertraulich zu behalten. Die Kehrseite dabei ist, dass strengere Richtlinien und Sicherheitsarchitekturen notwendig sind, um im Zeitalter der Demokratisierung und Digitalisierung von Daten und Informationen noch solch sensible Informationen von der Öffentlichkeit fernzuhalten.

Wie die hier geschilderten Fälle aufzeigen, können geteilte Informationen das Handeln von Menschen beeinflussen. Videos auf Social Media könnten Massenpanik auslösen, manipulierte Geodaten könnten falsche Alarme und Signale geben oder algorithmische Diskriminierung begünstigen. Geleakte Informationen in falschen Händen, ohne richtige Kontexte können eine Gefahr für Sicherheit und Ordnung darstellen – gar eine internationale Krise auslösen.

Intelligence ist effizienter geworden. Sie bietet durch die Demokratisierung von Informationen und durch eine große Anzahl von öffentlichen Quellen eine Möglichkeit der eigenen Validierung von vermeintlichen Fakten. Menschen haben durch den Besitz von Informationen ihre Souveränität und Freiheit in der Hand, müssen aber auch mehr Verantwortung tragen.

Die Privatisierung von Intelligence ist nicht aufzuhalten. Deshalb bedarf es neuer Spielregeln, damit sie ganzheitlich Schutzzielen wie Sicherheit und Ordnung wirklich dient und militärische und politische Entscheidungen an der dafür vorgesehenen Stelle getroffen werden. Mehr Information für alle, aber nicht jede Information für alle. Kritische Schutzbedarfe bleiben als Aufgabe beim Staat. Staatliche Institutionen brauchen neue Governance für den Umgang mit Technologien und stärkere Prüfinstanzen. Die Zusammenarbeit mit nicht-staatlichen Akteuren muss wertebasiert und geregelt ablaufen. Die Informationsflut macht kritisches Denken zur Kernkompetenz unserer Gesellschaft. Moderne, ja demokratische Intelligence funktioniert nur, wenn sie auf digitaler Mündigkeit ruht und der Staat weiterhin die Werte schützt, denen er dient. ■

„Wir verlassen uns zu sehr auf Regulierung“

Cyberangriffe destabilisieren längst den Alltag. Nicht fehlende Gesetze, sondern mangelnde Risikokompetenz machen sie so wirksam, sagt Dennis-Kenji Kipker. Ein Gespräch über hybride Bedrohungen, Vertrauen und die Grenzen technischer Lösungen.

Dennis-Kenji Kipker, was ist aus Ihrer Sicht die besondere Herausforderung hybrider Bedrohungen?

Dennis-Kenji Kipker: Hybride Bedrohungen betreffen nicht nur einen einzelnen Bereich, sondern Gesellschaft, Staat, Wirtschaft und Politik zugleich. Das Problem ist, dass wir noch immer in denken. Zuständigkeiten werden getrennt, statt vernetzt zu handeln.

Woran zeigt sich dieses Silo-Denken, haben Sie ein Beispiel?

Etwa bei Desinformation: Ist der Staat zuständig, die Plattformen, die Schulen oder die Eltern? Diese Trennung greift zu kurz. Hybride Bedrohungen zeigen, dass alte Denkmuster nicht mehr funktionieren. Wir brauchen vernetztes

Denken, mehr Transparenz und vor allem ein Vertrauen zwischen allen Akteuren.

Warum ist Vertrauen so wichtig?

Ohne Vertrauen funktionieren weder Kommunikation noch Zusammenarbeit. Unternehmen fragen sich etwa, ob sie Sicherheitslücken überhaupt an Behörden melden können, ohne Nachteile zu riskieren. Deshalb brauchen wir neue Verifikationsmechanismen und verlässliche Kommunikationsstrukturen.

Was ist Ihr wichtigstes Learning jahrelanger Arbeit in der Cybersicherheit?

Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe. Früher lag der Fokus nur auf kritischen Infrastrukturen. Heute, in einer hochvernetzten



INTERVIEW_ Dennis-Kenji Kipker

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence.institute in Frankfurt a.M. und Vorstand der Strategieberatungsgesellschaft CERTAVO AG. Er forscht an der Schnittstelle von Recht und Technik in der Cybersicherheit, Konzernstrategie sowie zu digitaler Resilienz im Kontext globaler Krisen.

KEY MESSAGES

- **Hybride Bedrohungen** betreffen Staat, Wirtschaft und Gesellschaft zugleich – Silo-Denken verhindert wirksame Gegenstrategien.
- **Vertrauen ist der Schlüssel:** Ohne verlässliche Kommunikations- und Meldewege bleibt Zusammenarbeit zwischen Staat und Wirtschaft brüchig.
- **Cyberangriffe** wirken vor allem psychologisch, weil sie alltägliche Dienstleistungen lahmlegen und institutionelles Vertrauen untergraben.
- **Reine Regulierung** schafft kein Sicherheitsniveau; Best Practices lassen sich nicht per Gesetz verordnen.
- **Nachhaltige Resilienz** entsteht durch Risikokompetenz, konkrete Beispiele und lokale, niedrigschwellige Awareness-Formate.

Welt, entstehen überall Verwundbarkeiten – ohne dass wir ein ausreichendes Sicherheits-Backbone geschaffen hätten.

Wo liegen die größten Versäumnisse?

Wir haben Vernetzung massiv ausgebaut – Internet, Internet of Things, 5G – aber keinen gleichwertigen Schutzmechanismus etabliert. Lange wurde das ignoriert. Erst Ereignisse wie Stuxnet oder Angriffe auf den Bundestag haben das Thema politisch sichtbar gemacht.

Bereich meist auch nicht. Dann bleiben nur Einzelne, die warnen, aber nicht gehört werden. Awareness muss deshalb ganz oben anfangen – in Behörden wie in Unternehmen.

Warum ist das so zentral?

Weil jede Führungskraft auch Bürgerin oder Bürger ist. Es geht nicht um abstrakte Funktionen, sondern um Menschen. Wir müssen die Gesellschaft insgesamt erreichen und in die Fläche gehen. Nur so lassen sich diese Themen

Erst dann wird Cyber greifbar.

Woran scheitert es häufig?

Viele empfinden Cyber als etwas Fernes und Technisches. Daraus entstehen zwei Haltungen: ein Gefühl des Ausgeliefertseins und die Hoffnung, jemand anderes werde sich schon kümmern. Genau das macht Angriffe erfolgreich – weil grundlegende Awareness fehlt.

Angriffe werden schneller und stärker automatisiert. Muss man Threat Intelligence deshalb neu denken?

„Viele Kommunen sind schlecht geschützt, nicht aus bösem Willen, sondern aus mangelnder Sensibilisierung.“

Dennis-Kenji Kipker

Warum sind Cyberangriffe heute so wirkungsvoll?

Es reicht oft schon, digitale Bürgerdienste lahmzulegen, etwa durch DDoS-Angriffe. Das hat eine enorme destabilisierende Wirkung und untergräbt Vertrauen – vom Cyberraum bis in den physischen Alltag.

Wie lässt sich die Zusammenarbeit zwischen Staat und Wirtschaft verbessern?

Neben bestehenden Public-Private-Partnerships brauchen wir neue, regionale Formate. Gerade Mittelständler erreicht man nicht über große Konferenzen. Wir müssen in die Fläche gehen – in Kommunen, Schulen und Betriebe. Nur so entsteht nachhaltige Resilienz und echtes Vertrauen.

Auf welchen Ebenen sehen Sie in Organisationen die größten Probleme?

Entscheidend ist die Leitungsebene. Wenn Führungskräfte das Thema nicht ernst nehmen, tut es der operative

wirklich verständlich und glaubwürdig vermitteln.

Wo zeigt sich das besonders deutlich?

Bei der kommunalen Cybersicherheit. Viele Kommunen sind schlecht geschützt, nicht aus bösem Willen, sondern aus mangelnder Sensibilisierung. Über IT-Budgets entscheiden oft ehrenamtliche Kommunalpolitiker, die im Alltag wenig Berührung mit digitalen Risiken haben. Wenn man sie erreichen will, braucht es lokale, niedrigschwellige Formate.

Was funktioniert aus Ihrer Erfahrung, um Awareness zu schaffen – und was nicht?

Reine abstrakte Schulungen funktionieren kaum. Wenn man nur über Ransomware, Phishing oder DDoS spricht, denken viele: „Mich trifft das nicht.“ Wir müssen konkrete Beispiele zeigen – aus derselben Branche, Region oder Kommune. Welche Folgen hatte ein Angriff? Was hat bei der Abwehr funktioniert?

Reine Threat Intelligence bleibt oft technisch und abstrakt. Entscheidend ist doch: Wie wahrscheinlich bin *ich* betroffen? Verstehe ich das Risiko überhaupt? Informationen müssen zugänglich und einordenbar sein, nicht nur für Experten. Menschen müssen Risiken einschätzen können, sonst entsteht Fatalismus. Wenn jede Meldung nur alarmiert, ohne Kontext zu liefern, schalten viele irgendwann ab.

Wie lässt sich das ändern?

Indem wir Informationen verständlich aufbereiten. Genau deshalb entwickeln wir Formate, die Bürgerinnen und Bürger befähigen, Bedrohungen einzuordnen, etwa bei Datenleaks oder Sicherheitsmeldungen. Nur wenn Menschen verstehen, was wirklich relevant ist, übernehmen sie Verantwortung, statt alles an andere zu delegieren.

Wenn Sie es entscheiden könnten: Was wäre das eine, wichtigste Ding, das Sie ➤

jetzt sofort angehen würden?

Wir verlassen uns derzeit zu stark auf gesetzliche Regulierung. Gesetze schaffen Bewusstsein, aber sie machen weder Staat noch Gesellschaft automatisch sicherer. Auch nach neuen Regelwerken ist objektiv nichts sicherer als am Tag zuvor. Entscheidend sind Best Practices – und die lassen sich nicht einfach per Gesetz verordnen.

„Wenn Risiken abstrakt bleiben, passiert am Ende: nichts.“

Dennis-Kenji Kipker

Woran liegt das?

Unsere Infrastrukturen sind extrem unterschiedlich. Ein lokales Wassernetz lässt sich noch vergleichsweise gut absichern, Strom- oder Bahntrassen über hunderte Kilometer hingegen kaum nach einheitlichen Standards sichern. Dafür fehlen nachhaltige Schutzkonzepte.

Was braucht es stattdessen?

Intrinsische Motivation. Menschen und Organisationen müssen Risiken selbst erkennen und einschätzen können.

Braucht es dafür erst große Krisen?

Krisen passieren ständig, aber ihre Wirkung verpufft schnell. Nach einem Stromausfall wird kurzfristig diskutiert, doch sobald der Alltag zurückkehrt, verschwindet das Thema wieder. Für Prävention braucht es Wissen, Risikokompetenz und Awareness. Wenn Risiken abstrakt bleiben, passiert am Ende: nichts. ■

Sind wir intelligent genug für die Demokratie?

Demokratie scheitert nicht an zu wenig Wahlen, sondern an zu wenig Urteilkraft. Wenn Bürger Politik als bloße Interessensbefriedigung missverstehen, wird der Kompromiss zur Enttäuschung – und autoritäre Lösungen erscheinen verführerisch einfach.

„Sei weich und stark. Sei schlau, lass dich ein und verachte den Sieg.“

Peter Handke

Die Demokratie steht unter Beobachtung, selbst bei denen, die sie für die beste Regierungsform halten. Haben wir es mit einer Krise zu tun? Viele wollen nicht ‚das System‘ abschaffen, sondern die Regierung – eine demokratische Haltung. Der Wechsel der Regierungen gehört zum Grundprinzip des Demokratischen. Die Skepsis gegen die laufenden Regierungen beruht auf Enttäuschung. Die darin aufscheinende Täuschung heißt: Wahlkampfversprechen, die nicht gehalten werden. Aber zunehmend geht es dabei auch um das Empfinden, dass die laufenden Regierungen weder das erreichte Wohlstandsniveau halten noch das Wachstum ankurbeln – es herrscht Verlustangst (im Grunde eine Furcht vor Wachstumsschwäche, wenn Jobs, Lohn- und Einkommenszuwächse verlorenzugehen drohen, KI-ständig neue Anforderungen stellt, etc.). Die damit einhergehende Vermutung der Politikunfähigkeit verbindet sich mit der Meinung, dass die Politik mehr Führung brauche. Führung aber ist eine problematische Kategorie des Demokratischen, denn sie setzt voraus, dass eine Partei die Mehrheit hat, um durchzuregieren. Was aber, wenn eine Partei eine Mehrheit bekommt, um ‚das System‘ abzuschaffen? Wenn sie ‚durch die Demokratie hindurch‘ regiert, wie wir es von der AfD erwarten müssen? >

TEXT_ Birger P. Priddat

Prof. Dr. em. Birger P. Priddat lehrte Volkswirtschaftslehre und Philosophie an der Universität Witten/Herdecke und leitete zuvor an der Zeppelin Universität den Lehrstuhl für Politische Ökonomie. Er ist Senior Research Fellow am Witten/Lab des Studium Fundamentale und veröffentlichte zuletzt das Buch „Der Markt der befreundeten Bürger im reichen Athen“ (2025).

KEY MESSAGES

- **Demokratie** ist kein System der Durchsetzung einzelner Interessen, sondern ein Verfahren der Koordination, Rücksicht und Revision, das Differenzen integriert, statt sie auszuschließen.
- **Politische Enttäuschung** entsteht häufig aus einem Missverständnis: Politik kann in pluralen Gesellschaften nicht „liefern“, ohne zugleich zu enttäuschen.
- **Wählen** setzt Urteilsfähigkeit voraus: Wer Parteien wählt, die demokratische Verfahren abschaffen wollen, wählt die eigene politische Mitbestimmung ab.
- **Autoritäre Angebote** erscheinen attraktiv, weil sie Komplexität reduzieren – sie zerstören jedoch die Möglichkeit politischer Korrektur.
- **Demokratie benötigt heute mehr als Wahlen**: strategische Intelligenz, institutionelles Design und Bürger, die Politik als gemeinsames Projekt verstehen.

Das ist die Sollbruchstelle des Demokratischen: eine legitime Wahl von illegitimer Politik. Einige – insbesondere der rechts-extreme Teil der AfD – wollen das demokratische System abschaffen – eine Haltung, die mit demokratischen Spielregeln nicht konform geht. Denn es wäre eine ‚letzte Wahl‘: danach wäre das Wählen abgeschafft. Wie kann eine Demokratie sichern, dass sie als Demokratie erhalten bleibt? Was macht den Kern des Demokratischen aus? Gibt es einen solchen Kern, und: unter welchen Bedingungen? Verstehen die Bürger die Demokratie?

Es entsteht der Eindruck, dass starke Regierungen eine Politik machen würden, die die Probleme, die die Bürger bewegen und von deren Unaufgelöstheit sie enttäuscht sind, angehen würden. Nur eine Mehrheit einer einzigen Partei könnte das imaginierte Führungsproblem angehen, aber natürlich allein in dem Maße, wie sie ihre Politik durchsetzen kann. Wenn die Wähler aber – demokratisch normal – divers wählen, das heißt keine einzelne Partei mehrheitsfähig machen, sind Koalitionen notwendig. Und in den Koalitionen Kompromisse, die wiederum die Interessen der je spezifischen Parteiwähler enttäuschen. In dem Sinne ist eine demokratisch gewählte Regierung systematisch überfordert, weil sie – gerade in Koalitionen – nicht vollständig ‚liefern‘, kann was den jeweiligen Interessen entspricht. Denn die anderen Interessen müssen mit berücksichtigt werden. Und in dem Sinne sind systematisch die Wähler überfordert, weil diese Konstellationen natürlich enttäuschen müssen, wenn sie dieses demokratische Grundmuster nicht verstehen. Politik ist eine Gestaltungsaufgabe, kein Steuerungsdurchmarsch.

Demokratie sortiert die Interessenvielfalt, hebt sie nicht hegemonial auf. Sie arbeitet mit einer *Synchronisation* von vielfacher Interessensenerfüllung: es geht um die Politik der Gesellschaft, nicht um einzelne Interessenprivilegien. Immer muss mit anderen geklärt werden, was gehen kann und soll – eine demokratische Grundanforderung der *Rücksicht*, die im Politikverständnis der Bürger nicht selbstverständlich verankert ist. Eine Rücksicht darauf, dass die anderen von der jeweiligen Politik nicht ausge-

schlossen werden – ein zugrundeliegendes *Kooperationsmuster*.

Hier von Kooperation zu reden ist ungewohnt, weil die verschiedenen Parteien Werte und Interessengegensätze darstellen, die eher in Opposition beziehungsweise Konkurrenz gedacht werden. Aber letztlich haben sie ein gemeinsames, wenn auch meist verdecktes, Interesse, dass die Demokratie als Verfassung und Verfahren erhalten bleibe, denn das allein ist der Garant dafür, dass sie am politischen Spiel weiter beteiligt werden. Eine autoritäre Regierung würde die Opposition ausschalten beziehungsweise behindern, das heißt das liberale Muster auflösen. Sie würde in einem fundamentalen Sinne *rücksichtslos* werden, keine Rücksicht auf andere als ihre Wähler nehmen, gegen Migranten sogar radikal. An dieser Rücksichtslosigkeit lässt sich der Wert der Demokratie neu ermessen: als ein System der Differenzen, die nicht antagonistisch werden, im dem eine Anerkennung der anderen und ihre Mitberücksichtigung herrscht, nicht ihr Ausschluss.

Denn unabhängig davon, ob die Parteien Koalitionen eingehen, um gemeinsam zu regieren oder ob sie im Spannungsfeld von Regierung und Opposition verbleiben: sie spielen dasselbe Spiel, nur dass die Macht verschieden verteilt ist. Demokratie bedeutet, dass die Macht, die einer erringt, in den nächsten Wahlen überprüft und gegebenenfalls abgewählt wird. Der Wesenskern heißt: keine ‚Tyrannei‘, keine Alleinherrschaft. Die Demokratie muss *Revision* zulassen. Das ist insbesondere gegen Parteien gerichtet, die, wenn sie einmal die Mehrheit gewinnen, das nutzen können, um die anderen auszuschließen oder deren Interessen nicht mit zu berücksichtigen – Exklusion statt *Inklusion*. Anstatt die Differenz als Opposition auszuhalten, machen sie die anderen zu Feinden. Sie spalten die grundsätzliche Gemeinschaftlichkeit in ein Innen und in ein Außen (in ‚Deutsche und Fremde‘ bei der AfD, wobei auch die ‚Deutschen‘ aufgespalten werden in ausgrenzende ‚Linke‘ und ‚Nationale‘).

Die Interessen der anderen mit zu berücksichtigen: *Inklusion*, ist die Kooperation, die in Demokratien gefordert ist und die >

„Demokratie arbeitet mit einer *Synchronisation* von *vielfacher Interessensenerfüllung*.“

Birger P. Priddat

im Kompromiss ihre Form findet – nicht nur ein Kompromiss der Regierungskoalition, sondern auch in einem darüber hinausgehenden Kompromiss in allen Entscheidungen, Gesetzen etc., die anderen mitzudenken, und zwar so, dass der Zusammenhalt der Gesellschaft in den Entscheidungen mitspielt. Denn Politik ist nicht allein das Projekt einer Mehrheitspartei oder einer Koalition, sondern der Gesellschaft insgesamt, so dass auch jene, die nicht in den Regierungen repräsentiert sind, ein Teil davon bleiben und Beachtung finden. Das ist das grundlegende kooperative Moment einer Demokratie. Der Historiker Josiah Ober spricht von einer „Kerndemokratie“ („Demopolis“, 2017), einem normativen Gerüst der demokratischen Politik. Diese Norm muss immer wieder mitentschieden werden, damit die Demokratie Realität bleibt.

Denn Demokratie ist keine Form wechselnder Alleinherrschaft, sondern jede Regierung bewegt sich im Kontext derer, die in der Regierung nicht vertreten sind, um den Zusammenhalt der Gesellschaft zu gewährleisten. Würden sich die Stärkeren durchsetzen, wäre das eine Idee von Freiheit als Willkür, die vergisst, dass die Politik die Gestaltung der ganzen „Polis“ der Gesellschaft umfasst und nicht die Durchsetzung von Interessen einer Gruppe, einer Elite, eines Teils der Bevölkerung. Um das auszuschließen, ist die Demokratie als Selbstorganisation aller Bürger erfunden worden, in der Antike, die im Kern alle an der Politik teilhaben lässt.

Diese Idee ist in den modernen Demokratien verblasst. Viele Bürger sind passive Wähler, verstehen sich gar nicht als politische Bürger, sondern als private Individuen, die sich von Fragen der Gestaltung der Gesellschaft – also von der Politik, nicht mehr angesprochen fühlen. Sie missverstehen Politik als Serviceleistung und fühlen sich nicht oder nur schwach in Verantwortung für das gemeinschaftliche Projekt. In diesem Abstand empfinden sie die Politik beziehungsweise die Regierungen als Eliteprojekte,

an denen sie nicht beteiligt sind, denen sie skeptisch bis offensiv gegenüberstehen, ohne politische Teilnahme, das heißt, genau betrachtet, ohne politischen Einfluss, den sie als Bürger in einer Demokratie haben müssten. Ihnen fehlt ein Grundverständnis des Politischen. Sie machen sich gleichsam zu Untertanen: passiv zur Hinnahme dessen bereit, was regiert wird. Wenn sie – wie viele – der Politik müde sind, nicht teilhaben an dem, was ihre Gesellschaft ausmacht, delegieren Sie das Politische an irgendeine Herrschaft, mit der brisanten Folge, dass, wenn sie diese Herrschaft nicht mehr wollen, sie sie nicht revidieren können.

Diese Einschätzung ist insofern bedeutsam, als beim Wählen in Demokratien mit bedacht werden muss, dass nur Parteien gewählt werden, die das Wählen nicht abschaffen wollen. Der Gedanke ist insofern wenig bekannt, als eben nicht allein das Wählen wichtig ist, sondern dass mit dem Wählen die Demokratie mit erhalten werden muss. Die Wahl von Parteien, die die Demokratie abschaffen wollen, kann insofern nicht demokratisch sein, weil sie die Basis, aufgrund derer sie gewählt werden, aufgeben. Das Prinzip der Demokratie-Nachhaltigkeit wird verletzt. Dabei geht es nicht um Verbote, sondern um die Rationalität von Wählern, beurteilen zu können, was ihre Wahlentscheidungen für Folgen haben können.

In kritischen Phasen, wie im aktuellen rechtspopulistischen Trend, reicht es nicht, einfach (eine Partei) zu wählen, sondern man muss *in einem gewissen Sinne doppelt wählen*: nämlich die Parteien und die Demokratie. Mit der Wahl von Parteien (AfD), die autoritär daran arbeiten, die Demokratie abzuschaffen, indem sie andere ausschliessen wollen („Linke“, Liberale, Migranten etc.), schafft man seine demokratische Potenz ab, wählen zu können und liefert sich den neuen Herrschern aus, *um ins zivilisatorische Nichts zu fallen*.

Es zeigt sich darin ein Bild, dass viele politikmüde sind. Und dass sie die Entscheidung, welche Politik gut und richtig sei, >

„Viele Bürger missverstehen Politik als Lieferung von Interessensbefriedigung und fühlen sich nicht oder nur schwach in Verantwortung für das gemeinschaftliche Projekt.“

Birger P. Priddat

kognitiv überfordert. Und dass man – in einem alten Bild – den ‚guten König‘ regieren lassen möchte. Dabei verschweigt man ein hochbedeutsames Moment. Denn wenn sich der ‚gute König‘ als herrisch und schlecht erweist, dann gibt es kein politisches Verfahren mehr, ihn abzuschaffen, selber nicht mehr die Möglichkeit, einen ‚besseren König‘ zu wählen. Man hätte dann die Gestaltung der Gesellschaft an einen Herrscher einer Partei, eine Elite, delegiert, ohne Rückversicherung, noch einmal wieder Einfluss auf das Politische bekommen zu können. AfD-Wähler geraten in das Risiko, nicht nur eine Partei zu wählen, die ein ‚anderes System‘ will, sondern in das Risiko kommen, in diesem anderen Systeme selber nicht mehr vorzukommen. Ist es intelligent, eine Entscheidung zu fällen, die das künftige Entscheiden entfallen lässt?

In der Antike, bei Aristoteles, war die Politik an die kluge, gebildete Entscheidung in der Gemeinschaftlichkeit (*politike koinonia*) gebunden: die Klugheit (*phronesis*) gehörte zu den dianoetischen Tugenden – als eine notwendige Voraussetzung des politischen Handelns tugendhafter Bürger. Nun sind das antike Bedingungen, die für unsere Moderne nicht bedingungslos gelten. Modern ließe sich diese Gemeinschaftlichkeit als ein *shared mental model* des Politischen formulieren: als eine gemeinsam geteilte Überzeugung, ein Verfahren zu haben, dass Selbstbestimmung ermöglicht. Dabei fällt auf, dass wir häufig Demokratie mit Freiheit und Interessen verbinden, und zwar so, dass wir meinen, im politischen Geschäft unsere Interessen wählen und durchsetzen zu wollen. Der Wille, individuell frei zu wählen, dominiert und konfliktiert mit den Interessen der anderen. Der Wille, frei zu sein, ist ausgeprägt als Vorstellung, dass individuelle Private hochzuschätzen, ohne dass es an ein Interesse für andere gekoppelt ist.

Eine solche Rücksicht scheint unserem Freiheitsverständnis zu widersprechen. Dabei ist der Gedanke, dass das Politische ein Gemeinschaftsprojekt ist, nämlich die eigenen Interessen im Kontext der Interessen der anderen unter Interessen aller zu rea-

lisieren, verloren gegangen. Die Demokratie ist „kein intuitives System. Sie ist ein System, das erfordert, dass Menschen in der Lage sind, miteinander zu streiten und dennoch im Interesse des Landes zusammenzuarbeiten,“ so die Historikerin Anne Applebaum in der FAZ. Das Politische am Demokratischen aber ist gerade die Koordination der Spannung und Differenz der Interessen und die dafür notwendige Kooperation. Der Kompromiss ist ein produktives Moment dieser Art von Kooperation. Was bedeutet, die eigene Freiheit der Wahl in einem Zusammenhang der Freiheit aller zu stellen, nicht als individualistische Durchsetzung, sondern als wechselseitige Kooperation. Sind wir auf eine gewisse Weise nicht intelligent genug, das gemeinschaftliche Moment der Kooperation und Koordination der Interessen zu verstehen?

Nicht intelligent genug heißt: zwischen Meinen und Urteilen nicht unterscheiden gelernt zu haben. Viele meinen, dass bloße Meinung ausreicht, um politisch wählen zu können. Das, was sie meinen, beruht auf zufälligem Wissen, eingebildeten Anschauungen und oft auf Ressentiments anderen gegenüber. Die Meinung wird zur unreflektierten Ressource von Wahlentscheidungen. Viele wählen so, wie andere wählen, d.h. sie haben gar keine eigene Meinung, sondern leihen sie sich. So schließen sich Meinungen zur Entscheidung zusammen, ohne dass geurteilt wird, was zu wählen ist.

Urteilen heißt, Gründe zu haben, sich zur Entscheidung zu entscheiden, informiert zu sein über Zusammenhänge. Politisches Urteilsvermögen bedeutet, wissen zu können, welche Folgen welche Wahl hat, und zwar nicht nur für seine eigenen Interessen, sondern auch für die Kooperation der Gesellschaft und deren Entwicklungen, einschließlich der mitlaufenden Entscheidungen über die Erhaltung der Demokratie. Wählt man seine eigene Kompetenz ab, künftig weiter mitzubestimmen, wird künftig hin das Urteilen wertlos. Opportunistisch schließt man sich dann endgültig dem Meinen an, das herrschaftlich vorherrscht. >

„Bei Aristoteles war die Politik an die kluge, gebildete Entscheidung in der Gemeinschaftlichkeit gebunden.“

Birger P. Priddat

Das alles geschieht bereits in großem Ausmaß in den *social media*. Die ‚alte‘ Öffentlichkeit (Zeitungen, TV), in der noch Themen von vielen gleichzeitig erörtert und ausgetauscht wurden, zersplittet in der *social media* – Kommunikation, in der nicht mehr diskutiert wird, sondern in je eigenen Blasen abgekapselt das erstbeste Meinen kopiert und bestätigt wird. Die Demokratie verliert ihre große politische Arena, in der natürlich Differenzen ausgetragen wurden, aber alle waren am gleichen Thema beteiligt, indem sie sich wechselseitig Gründe und Kritiken lieferten: ein Prozess politischer Bildung – eine Art „einheitsstiftendes Lagerfeuer“ (James Poniewozik). Die *social media* hingegen privatisieren das Öffentliche und jeder bleibt im auseinandersetzungsfreien Raum, in dem Politik nicht mehr als gemeinschaftliches Projekt erscheinen kann. Die Idee des Politischen als gesellschaftliches Projekt, mit dem man sich auseinandersetzt, um tragfähige Konzepte zu gewinnen, entfällt.

Sind wir intelligent genug, unter diesen Bedingungen demokratisch zu sein? Es geht hier nicht um eine abwertende Rede über die Bürger, sondern um eine pragmatische Einschätzung. Vor allem: welche intelligent zugeschnittenen Institutionen würden helfen, die Teilnahmebereitschaft der Bürger zu fördern? Und es geht auch und vor allem nicht nur um die Bürger, die die Komplexität der politischen Entscheidungsnotwendigkeiten selten überblicken, sondern um intelligente Parteipolitik und vor allem um intelligentes *institutional design* des Staates.

Denn bei allem, was bisher erörtert wurde, bleibt übersehen, dass viele Entscheidungen in der Politik nicht mehr dem eigenen Verfügungsrahmen entstammen, sondern als Reaktionen (im besseren Fall Antizipationen) von außerpolitischen Umständen und Bedingungen auftreten (EU-Gesetze, globaler Handel, Geoökonomie der Weltmächte, in der die deutsche Politik keine Rolle spielt, Kriegsandrohungen, Energie- und Ressourcenfragen, Schwäche der EU-Außenpolitik etc. Diese Themen, die die jeweilige Politik mitverarbeiten muss, werden im Wahlkampf kaum

die Rolle spielen, die sie aber für das Regierungsgeschäft und für die Gesellschaft insgesamt bedeuten. Bei den Wählern noch weniger, zumal es nicht nur komplexe Themen sind, die in gesellschaftlichen Fragen überragen, sondern zugleich multiple Problemlagen, die synchron behandelt werden müssen. Die Politik braucht eine Intelligenz, um die inner- und die außerpolitischen Anforderungen zu relationieren.

Die Intelligenz, die hier angefordert wird, beruht wesentlich darauf, sich diesen Themen nicht nur zu stellen, sondern vor allem: sie strategisch anzugehen. Intelligentes *institutional design* bedeutet, Verfahren zur Informationsbeschaffung und Analyse zu haben (Intelligenz in einem strukturierten Sinne), die über die tradierten oder zufälligen Einschätzungen in der Politik hinausreichen, um strategische Entscheidungen produzieren zu können, die daten- und analysefundiert sind und deshalb die strategischen Umbrüche tragen können. Es ginge um Selbstbindung auf der Grundlage strategischer Intelligenz: fundierte Versprechen machen zu können, die auch eingehalten werden können.

Das sind Themen, die keiner Partei oder sollten nur einzelne Interessen zugeordnet werden können, sondern immer die ganze Gesellschaft betreffen. Die strategischen Anforderungen sind ebenso allgemein, das heißt von allen Parteien, soweit sie die objektiven Anforderungen nicht leugnen, anzugehen, so dass sich das, was wir vorhin das Kooperationsprinzip nannten, praktisch wird – dass es auf eine synchronisierte Strategie ankommt, die nicht beim nächsten Wahlgang von einer nächsten Regierung abgebrochen wird, so dass das Land dem internationalen Wettbewerb gänzlich ausgeliefert sein würde bzw. die jeweilig eingeleiteten Entwicklungen wieder abgebrochen würden.

An diesem Punkt lässt sich das Thema Führung neu aufgreifen. Nicht im Sinne einer alleinigen herrschaftlichen Steuerung, sondern im Sinne einer intelligenten Synchronisation der innergesellschaftlichen politischen Interessen im Kontext ihrer außerpolitischen Anforderungen und Problemlagen. Synchronisation wäre eine Kunst des Managements der Problemlagen, was ge- ➤

„Welche intelligent zugeschnittenen Institutionen würden helfen, die Teilnahmebereitschaft der Bürger zu fördern?“

Birger P. Priddat

lingen kann, wenn man einen strategischen Konsensus hat, der angesichts der Änderungen und Problemlagen sowieso ständig agil angepasst werden muss. Führung heißt hier, sich auf einer entworfenen Linie ständig neu intelligent zu arrangieren, und zwar von allen Beteiligten, in einem gewissen Maße auch im Grundkonsens mit anderen Parteien. Und auch die oppositionellen Spannungen müssten sich bewegen. Hier *führt* nicht einer oder eine Partei, sondern alle politisch Beteiligten koordinieren sich in Hinblick auf die Bewältigung der Problemlagen. Das heißt nicht, dass nicht unterschiedliche Entwürfe ins Spiel kommen, aber alle sind auf Lösungen ausgerichtet, nicht auf bloße Differenz. In diesem Spiel der unterschiedlichen Entwürfe bedarf es eines intelligenten Umgangs mit Differenz: Politik wird Differenzmanagement, immer die inner-politischen Unterschiede und die außerpolitischen Anforderungen inkludierend. Weniger wird nicht zu haben sein, außer Erfolglosigkeit und weitere Enttäuschung. Dabei geht es nicht darum, dass eine Partei siegt, sondern vielmehr darum, dass das Projekt Gesellschaft vorangebracht wird.

In den multiplen Problemlagen, inner- wie außerpolitisch, wird die Politik immer wieder neu verhandeln müssen, in den Regierungskoalitionen sowieso, aber auch in den anderen Parteien und der Gesellschaft. Denn die Dynamik der gesellschaftlichen und vor allem wirtschaftlichen Anforderungsänderungen muss mit der Rekursivität der Verhältnisse rechnen, mit denen intelligent umgegangen werden muss. Und zwar weder ideologisch noch konventionell. Die Politik geht Prozesse instabiler Stabilität ein, das heißt einen Politikmodus, der in den Erfahrungswelten der Bürger wie auch vieler Politiker noch wenig ausgeprägt ist. Politische Bildung heißt zu verstehen, wie in dieser Dynamik intelligentes Verhalten zu lernen ist.

Demokratie kann sich nicht auf ihre Strukturen, Verfahren, Verfassung verlassen, auch nicht auf das Rechtssystem, an das Politiker, die nicht zu entscheiden wagen, die finalen Entscheidungen delegieren (ein nicht-demokratisches Verfahren der De-

legation an eine nicht-parlamentarische Instanz), sondern sie braucht ein Verständnis ihrer Koordinationsintelligenz, gerade jetzt in der neuen Welt multipler und polyvalenter Anforderungen – ein Verständnis von Agilität, das immer wieder die Inklusion der divergenten Interessen neu webt, in fortwährender Arbeit am Projekt demokratischer Gemeinschaftlichkeit.

Allerdings wird es schwieriger, denn wir nähern uns einem Scheitelpunkt: in den Untiefen der Oberfläche der KI-Welten droht die Bequemlichkeit der Automatisierung der Politik, der Verlust der demokratischen Souveränität. Es ist ein ganz anderes Einfallstor für die autoritären Regime, wie Curtis Yarvin vom „Tech-CEO-König“ träumt, wie Peter Thiel, Elon Musk, Balaji Srinivasan und Alex Karp die Demokratie für eine tote Kulturtechnik halten und Patrick Deneen ihnen die Idee des „Aristopolismus“ anbietet: die Herrschaft neuer Eliten, die die Bevölkerung im Amazon-generierten Konsum unpolitisch untertänig belassen, mit der *tech-world*-Konsequenz, dass die KI die Stimmungen der Menschen besser erfassen könne als die Wählerstimmen. Wozu dann noch wählen? Das Politische wird für die Bevölkerung zur Lieferung ihrer Konsumbefindlichkeit, gleichsam in einem unkündbaren Abonnement, während die Eliten den unkontrollierten Bereicherungspfad einschlagen – eine Gesellschaft doppelter (gespaltener) *delivery*.

Fatal ist die Übertragung des Intelligenz-Themas an die *artificial intelligence*, die als effiziente Komplexitätsbewältigung verkauft wird, jenseits der demokratischen Politik, deren Inklusions- und Integrationsgebaren überflüssig zu werden droht. Das geht einher mit der Politikmüdigkeit: KI-Politik ist die kulturelle Entlastung von einer polyvalenten Welt und von den Anstrengungen bürgerschaftlicher Selbstbehauptung. Richard Rorty hatte in den 90iger Jahren des letzten Jahrhunderts bereits geahnt, dass die Demokratie nur mehr auf einem *contingent consensus* beruhe, als sei sie eine temporäre geschichtliche Epoche. Wieviel demokratische Intelligenz müssen wir aufwenden, um in der Zivilisations-Geschichte zu bleiben? ■

„Es geht nicht darum, dass eine Partei siegt, sondern darum, das Projekt Gesellschaft voranzubringen.“

Birger P. Priddat

Contributors und Interviewpartner

Dr. Timo Blenk leitet als Senior Partner & CEO die aus der Münchner Sicherheitskonferenz hervorgegangene Strategieberatung Agora Strategy Group AG. Der Geopolitik-Experte berät Industrieunternehmen zu globalen Trends, Markteintritten sowie Optimierung der Beschaffungs- und Produktionsarchitektur.

Dr. Raluca Csernaton ist Fellow bei Carnegie Europe in Brüssel mit Schwerpunkt europäische Sicherheits- und Verteidigungspolitik sowie KI und neue Technologien. Sie leitet dort die Forschung zur Geopolitik von KI, ist Gast- und Visiting Professor an der Vrije Universiteit Brussel, der University of Antwerp und forscht in mehreren EU-geförderten Projekten zu Cyber- und Digitalpolitik.

Prof. Dr. Anna Daun ist Professorin für Politikwissenschaft an der Hochschule für Wirtschaft und Recht (HWR) in Berlin. Sie unterrichtet Sicherheitsthemen in den Studiengängen gehobener Polizeivollzugsdienst (gehPVD) und Sicherheitsmanagement, und ist stellvertretende Direktorin des Forschungsinstituts für öffentliche und private Sicherheit (FÖPS).

Prof. Dr. Jan-Hendrik Dietrich lehrt an der Hochschule des Bundes in Berlin und der Universität der Bundeswehr München. Mit Prof. Dr. Carlo Masala leitet er das Masterprogramm Intelligence and Security Studies, ist Co-Direktor des Center for Intelligence and Security Studies an der Universität der Bundeswehr München sowie „chercheur invité“ bei SciencesPo Paris. Er ist Autor zahlreicher Publikationen zum Sicherheitsrecht.

Ole Donner ist Gründer von Strukturierte Analyse Deutschland und berät staatliche Institutionen, internationale Organisationen und Unternehmen zu Intelligence- und Analysefähigkeiten. Zuvor war er 13 Jahre bei der Bundeswehr als Analyst, Vorgesetzter und Dozent tätig und prägte dort die Analyseausbildung. Er ist Mitautor u. a. des Buchs „Clear Thinking“ (2025) sowie Initiator der German Intelligence Community Conference (GICC).

Dr. Alana Gramm ist OSINT-Spezialistin und Senior Strategy Consultant bei IBM iX. Ihre Schwerpunkte liegen im Bereich Open Source Intelligence an der Schnittstelle von Intelligence, Law Enforcement und Defence. Zuvor war sie neun Jahre beim LKA Berlin tätig, zunächst als OSINT-Analystin im Bereich Terrorismus, später als Koordinatorin der OSINT-Analyse.

Dr. Aviva Guttman ist Lecturer in Strategy and Intelligence an der Aberystwyth University. Zuvor forschte sie am King's College London (King's Intelligence and Security Group) und an der University of Southern Denmark. Sie ist Gründerin und Vorsitzende des Women's Intelligence Network (WIN). Ihre Forschung zu Geheimdiensten, covert action und Terrorismus veröffentlichte sie u. a. in Operation Wrath of God (Cambridge, 2025).

Prof. Dr. Eva Herschinger ist Professorin für Sicherheitsforschung und leitet am CISS der Universität der Bundeswehr München den Forschungsbereich Sicherheit und Intelligence. Die Politikwissenschaftlerin und Germanistin verantwortete zuvor auch den Bereich polizeiliche Prävention von Radikalisierung und Extremismus am Polizeipräsidium Frankfurt am Main.

Prof. Dr. Beatrice Heuser ist Distinguished Professor an der Brussels School of Governance, VUB sowie Head of Strategy Teaching an der Führungsakademie der Bundeswehr. Im Zentrum ihrer Forschung steht die Frage, warum Menschen Kriege führen, welche Mittel und Strategien sie wählen – und wie sie diese rechtfertigen.

Prof. Dr. Holger Janusch ist Professor für Internationale Politik mit dem Schwerpunkt auf Außen- und Sicherheitspolitik der USA am Fachbereich Nachrichtendienste der Hochschule des Bundes für öffentliche Verwaltung in Berlin mit den Forschungsschwerpunkten nationale Sicherheitsstrategien, die Handelspolitik der USA und Macht in Theorien der Internationalen Beziehungen. Er kuratierte den Sonderband „Integrierte Sicherheit für Deutschland?“ (2025).

Prof. em. Loch K. Johnson ist emeritierter Regents Professor für Public and International Affairs an der School of Public and International Affairs (SPIA) der University of Georgia. Er ist Autor oder Herausgeber von mehr als vierzig Büchern, darunter zuletzt The Oxford Handbook of National Security Intelligence (Oxford University Press, 2025) sowie National Security Intelligence, 3. Auflage (Polity, 2024).

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence institute in Frankfurt a.M. und Vorstand der Strategieberatungsgesellschaft CERTAVO AG. Er forscht an der Schnittstelle von Recht und Technik in der Cybersicherheit, Konzernstrategie sowie zu digitaler Resilienz im Kontext globaler Krisen.

Lars König bekämpft als Gründer von Net-Watch weltweit Missbrauchssysteme durch einen gemeinschaftsbasierten Ansatz. Er ist Teil der Customer Advisory Boards von Google und CrowdStrike.

Brendan Kotze ist Chief Delivery Officer bei dem Cybersecurity-Dienstleister Performanta. Mit über 20 Jahren Erfahrung in der IT-Sicherheit war er entlang des gesamten Security-Lebenszyklus tätig, bis hin zur Rolle als CISO. Heute verantwortet er Entwicklung, Automatisierung und Beratung mit Fokus auf praxisnahe Sicherheitslösungen, die Geschäftsrisiken reduzieren und Menschen im digitalen Raum schützen.

Prof. Dr. Rafaela Kraus ist Professorin für Unternehmens – und Personalführung an der Universität der Bundeswehr München. Sie forscht unter anderem über Intrapreneurship und Entrepreneurship, Defense/Dual Use Innovation, Transformation (z.B. Autoindustrie und Verteidigung), Leadership und Organisationskultur.

Prof. Dr. em. Wolfgang Krieger lehrte Neuere Geschichte an der Philipps-Universität Marburg und war Fellow der Universitäten Oxford und Harvard. Er ist Mitglied im „International Institute for Strategic Studies“ und des „Conseil scientifique de la recherche historique de la défense“ des französischen Verteidigungsministeriums sowie Mitbegründer der International Intelligence History Association. 2026 veröffentlichte er „Die Geschichte der Geheimdienste“.

Krista-Marija Läbe ist eine deutsch-ukrainische Kommunikationsstrategin und PR-Managerin bei Quantum Systems. Zuvor arbeitete sie als strategische Kommunikationsberaterin für die ukrainische Botschaft in Deutschland. Sie ist zudem Mitbegründerin und Vorstandsmitglied der Deutsch-Ukrainischen Gesellschaft und engagiert sich dafür, das Bewusstsein für ukrainische Perspektiven im westeuropäischen Diskurs zu schärfen.

Marc Mahlke ist Cybersecurity-Experte mit interdisziplinärem Hintergrund in Informations- und Kommunikationstechnik und IT-Management. Er arbeitet an der Verbindung technischer Sicherheitsanalyse und strategischer Cybersicherheit, mit Schwerpunkten in Penetration Testing, Red Teaming, Governance und Intelligence-Ansätzen auf Organisationsebene.

Luca Manns ist Geschäftsführer der Forschungsstelle Nachrichtendienste der Universität zu Köln. Der Rechts- und Wirtschaftswissenschaftler publiziert regelmäßig in juristischen Fachzeitschriften, berät Regierungsstellen sowie Parlamente. Daneben wirkt er am Aufbau der Adenauer School of Government der Kölner Universität mit und lehrt zum Recht der Digitalisierung.

Prof. Dr. Christoph Meyer ist Professor für Europäische und Internationale Politik am King's College London. Seit über 15 Jahren forscht er zu Frühwarnung, strategischer Überraschung und Lernen aus Krisen. Zu seinen Büchern zählen Warning about War (2020) sowie Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise (2023).

Armin Müller ist Regional Vice President Central Europe bei Veeam. Zuvor war er in Führungspositionen bei Broadcom Software, VMware und Oracle tätig sowie bei IBM und T-Systems. Er verantwortete Wachstum, Cloud-Transformation und Enterprise-Strategien in Europa. Müller hält einen MBA der Henley Business School und ist Diplom-Kaufmann.

Daniel Rainer Neumann ist Politikwissenschaftler mit Scherpunkt Intelligence Studies und Assistenzprofessor am Institute for Security and Global Affairs der Universität Leiden. Er forschte zur Unterstützung der Gemeinsamen Außen- und Sicherheitspolitik der EU durch die Nachrichtendienste der Mitgliedsstaaten, insbesondere gegenüber dem EU Intelligence and Situation Centre (INTCEN).

Dr. Konstantin von Notz ist Mitglied des Bundestages (Bündnis 90/ Die Grünen) und stellvertretender Vorsitzender des parlamentarischen Kontrollgremiums, das die drei Nachrichtendienste des Bundes, den Bundesnachrichtendienst (BND), den Militärischen Abschirmdienst (MAD) und das Bundesamt für Verfassungsschutz (BfV) überwacht. Er war Obmann in der Enquete-Kommission „Internet und Digitale Gesellschaft“, Vorsitzender des Untersuchungsausschusses „NSA“ und Obmann im Ausschuss Digitale Agenda.

Dr. Esther Omlin ist Dozentin für Sicherheitsrecht- und Wirtschaftsrecht an der Ostschweizer Fachhochschule (OST) und war zuvor als Oberstaatsanwältin tätig. Sie forscht zu den Gebieten äußere und innere Sicherheit, internationale Sicherheitspolitik, Weltraum und Außenwirtschaft und bietet dementsprechende Weiterbildungen an. ➤

Niccolò Petrelli, PhD, ist Assistenzprofessor am Fachbereich Politikwissenschaften der Universität Roma Tre, wo er strategische Studien lehrt. 2025 veröffentlichte er das Buch „I servizi segreti italiani e l'Intelligence USA.“ („Die italienischen Geheimdienste und der US-Geheimdienst“), eine Geschichte der wechselseitigen Beziehungen von 1943 bis zur zweiten Hälfte der 1970er Jahre.

Prof. Dr. em. Birger P. Priddat lehrte Volkswirtschaftslehre und Philosophie an der Universität Witten/Herdecke und leitete zuvor an der Zeppelin Universität den Lehrstuhl für Politische Ökonomie. Er ist Senior Research Fellow am Witten/Lab des Studium Fundamentale und veröffentlichte zuletzt „Der Markt der befreundeten Bürger im reichen Athen“ (2025).

Christopher Radler-Morić ist Experte für Corporate Security mit den Schwerpunkten Business Continuity Management, Notfall- und Krisenmanagement, Reisesicherheit sowie Intelligence. Mit nachrichtendienstlichem Hintergrund und einem Masterstudium in Arabistik, Ethnologie sowie Risiko- und Krisenmanagement verbindet er strategische Sicherheitsanalyse mit tiefem kulturellem und geopolitischem Verständnis komplexer Risikolagen.

Dr. Daniela Richterova ist Associate Professor für Intelligence Studies am Department of War Studies des King's College London. Ihre Forschung zu Geheimdiensten im Kalten Krieg sowie zu staatlichen Bedrohungen und Terrorismus erscheint u. a. in International Affairs und Foreign Policy. 2025 veröffentlichte sie Watching the Jackals (Georgetown University Press).

Felix Rieger verantwortet die Öffentlichkeitsarbeit des KI-Kompetenzzentrum Medien (KI.M). In seiner täglichen Arbeit befasst er sich mit Künstlicher Intelligenz, Medieninnovation und Community-Building.

Irina Rosensaft ist Expertin für Digitale Transformation und Cybersicherheit an der Schnittstelle von IT, Organisationsprozessen und Zivilgesellschaft. Mit einem politikwissenschaftlichen Hintergrund und fundierter Erfahrung in Prozessoptimierung, Change Management und Cybersicherheit schlägt sie eine Brücke zwischen Technologie, Governance sowie organisatorischen und gesellschaftlichen Anforderungen.

PD Dr. Frank Sauer ist Politikwissenschaftler und Publizist. Als Forschungsleiter des Metis Institut für Strategie und Vorausschau forscht er zum Nexus zwischen Sicherheit, Technologie und Gesellschaft und berät die Abteilung für Strategieentwicklung im Bundesverteidigungsministerium. Er ist Co-Host des preisgekrönten Podcasts „Sicherheits- halber“ über Aktuelles in der deutschen Sicherheits- und Verteidigungspolitik.

Christina Schäfer unterstützt als Beraterin bei der Agora Strategy Group Unternehmen dabei, geopolitische Risiken zu antizipieren und Resilienz in Lieferketten und Geschäftsmodellen aufzubauen. Zuvor war sie in der Risikoberatung bei PwC sowie im Auswärtigen Amt tätig und absolvierte ihren Master an der Sciences Po Paris.

Oberst a. D. Klaus Schmidt war in leitenden Funktionen im deutschen Sicherheits- und Nachrichtendienstbereich u. a. als Abteilungsleiter und Referatsleiter im Bundesnachrichtendienst tätig und als Referent im Bundesministerium der Verteidigung. Zuvor diente er als Generalstabsoffizier, Bataillonskommandeur der Deutsch-Französischen Brigade und Offizier der Bundeswehr. Er ist Vorsitzender des Gesprächskreis Nachrichtendienste in Deutschland GKND

Dr. Ralf Schneider ist Vorstandsvorsitzender des Vereins Cyber Security Sharing & Analytics e. V. (CSSA) – einem Zusammenschluss 17 deutscher Großunternehmen mit dem Ziel, sich und die öffentliche IT-Infrastruktur gemeinsam besser vor Cyberangriffen zu schützen.

Jim Sengl leitet das KI-Kompetenzzentrum Medien (KI.M), eine gemeinsame Initiative der Medien.Bayern GmbH und der Bayerischen Landeszentrale für neue Medien (BLM). Seine Arbeit im KI.M konzentriert sich auf die Unterstützung der Medienbranche in der rechtssicheren und zukunftssichernden Nutzung von Künstlicher Intelligenz.

Dr. Jennifer E. Sims arbeitete in leitender Funktion im US-Sicherheitsapparat: im United States Senate als Mitglied des Intelligence Community Staff sowie im United States Department of State als Deputy Assistant Secretary of State for Intelligence. Auch lehrte sie an Georgetown University. 2022 veröffentlichte sie das Buch Decision Advantage. Sie ist zudem Künstlerin und Gründerin des Stuart Street Atelier.

Thomas Vašek ist Co-Chefredakteur von „human“. Zuvor war der gelernte Investigativjournalist unter anderem Gründungschefredakteur der Philosophiezeitschrift „Hohe Luft“ sowie der deutschen Ausgabe von „MIT Technology Review“. Zudem ist er Autor mehrerer Sachbücher, darunter Schein und Zeit (2019), Land der Lenker (2019), und Work-Life-Bullshit (2013), ein viel diskutierter Debattenbeitrag über den Wert der Arbeit in unserem Leben.

Dr. Larysa Visengeriyeva ist eine Expertin für AI und MLOps, die es versteht, komplexe Technologien strategisch mit Regulierung und Innovation zu verbinden. Als Autorin des bei O'Reilly erschienenen Fachbuchs „The AI Engineer's Guide to Surviving the EU AI Act“ (August 2025) bietet sie Entwickler:innen einen Leitfaden, um AI-Systeme rechtskonform und verantwortungsvoll in den Markt zu bringen. Als Mitgründerin von Women in Defense Tech treibt sie aktiv die Transformation der europäischen Verteidigungsindustrie voran – mit einem klaren Fokus auf das Konzept der „Combat-Driven Innovation“ und weibliche Führung.

Jeff Watkins ist Founder der Beratung „North Star Intelligence“ und Founding Member der „Business AI Alliance“. Er war CTO der Technologieberatung CreateFuture. Seine Branchenschwerpunkte liegen in den Bereichen Finanzdienstleistungen, Gesundheitswesen und Ölhandel. Als Enthusiast für Cybersicherheit und KI ist er als Podcaster und internationaler Redner aktiv.

Richard Weiss arbeitet an der Schnittstelle von technischer Analyse und strategischer Doktrin. Mit Hintergrund in Mathematik, Physik und Data Science war er u. a. Reverse Engineer im FLARE-Team von Mandiant. Er berät zwei NATO Centres of Excellence (COE) sowie militärische und öffentliche Institutionen und forscht zur Nutzung von KI und LLMs im Intelligence-Tradecraft.

Julian Werner ist ehemaliger Fallschirmjäger und Offizier der spezialisierten Kräfte des Heeres (EGB). Seit 2024 forscht er unter Prof. Dr. Carlo Masala am Center for Intelligence and Security Studies zu Themen wie Urban Warfare und Military Innovation. Sein Buch Urban Warfare – Krieg zu Hause erscheint im April 2026.

Marcus Willett (CB, OBE) war 33 Jahre beim britischen Geheimdienst GCHQ, zuletzt als stellvertretender Leiter mit Verantwortung für Nachrichtengewinnung und Cyberoperationen. Er leitete offensive Cyberprogramm in UK. Seit 2018 ist er Senior Advisor beim International Institute for Strategic Studies (IISS) und berät Regierungen und Unternehmen in UK, USA und andernorts.

Simon Wunder ist in der Volkswagen AG für die Analyse geopolitischer Risiken für Lieferketten verantwortlich. Außerdem ist der Politikwissenschaftler Research Fellow am Center for Advanced Security, Strategic and Integration Studies (CASSIS) der Universität Bonn. Dieser Beitrag gibt seine persönlichen Ansichten wieder. ■

Impressum

Chefredaktion

Dr. Rebekka Reinhard, Thomas Vašek
(v. i. S. d. P.)
human Forward und human Magazin
erscheinen in der philosophy works
GmbH, Dr. Rebekka Reinhard,
Westermühlstraße 13, 80469 München-
info@philosophyworks.de
philosophyworks.de

Contributors

Timo Blenk, Raluca Csernaton, Anna
Daun, Jan-Hendrik Dietrich, Ole Donner,
Alana Gramm, Aviva Guttmann, Eva Her-
schinger, Beatrice Heuser, Holger Janusch,
Loch, K. Johnson, Dennis-Kenji Kipker, Lars
König, Brendan Kotze, Rafaela Kraus, Wolf-
gang Krieger, Krista-Marija Läbe, Marc
Mahlke, Luca Manns, Christoph Meyer,
Armin Müller, Daniel Rainer Neumann,
Konstantin von Notz, Esther Omlin, Niccolo
Petrelli, Birger P. Priddat, Christopher
Radler-Moric, Daniela Richterova, Felix
Rieger, Irina Rosensaft, Frank Sauer, Chris-
tina Schäfer, Klaus Schmidt, Ralf Schneider,
Jim Sengl, Jennifer E. Sims, Thomas Vašek,
Larysa Visengeriyeva, Jeff Watkins, Richard
Weiss, Julian Werner, Marcus Willett, Si-
mon Wunder

Artredaktion & Grafik

Tanja Maus (fr.)

Bildredaktion

Maja Metz (fr.)

Grafik

Christian Talla (fr.)

Kontakt zur Redaktion

human-magazin.de

Wir danken unseren Partnern!



Der CSSA e.V. (Cyber Security Sharing & Analytics) ist ein 2014 gegründeter Zusammenschluss von 17 Wirtschaftsunternehmen. Ziel des Vereins ist es, Mitglieder, Kunden und die öffentliche IT-Infrastruktur nachhaltig vor Cyberbedrohungen zu schützen. Die Förderung vertraulicher Kollaboration ermöglicht es den Mitgliedern sich auszutauschen, voneinander zu lernen und gegenseitig zu unterstützen. Zentrale Bestandteile sind Austauschformate für Cybersecurity-Fachspezialisten, das Teilen von Kompromittierungsindikatoren und Angriffstechniken, individuelle Trainingsangebote für operative Experten sowie Ad-Hoc-Treffen bei Notfällen. Durch gezielte strategische Integration, u.a. von Daten im Bereich „AI/Machine Learning“, können potenzielle Bedrohungen effektiver aufgespürt werden. Dies erlaubt den Unternehmen, sich proaktiv auf Bedrohungen vorzubereiten, ihre Verteidigung zu verbessern und langfristig widerstandsfähiger zu werden.



Das KI-Kompetenzzentrum Medien (KI.M)
der Medien.Bayern GmbH und der
Bayerischen Landeszentrale für neue
Medien (BLM) stärkt systematisch die

KI-Kompetenz bayerischer Medienunternehmen – von lokalen Radiosendern bis hin zu internationalen Medienhäusern. Unser Ansatz verbindet technische Innovation mit rechtlicher Sicherheit: Im KI-Reallabor testen wir die technische Machbarkeit von KI-Projekten und teilen das gewonnene Wissen mit der gesamten Medienbranche. Regional-Workshops bringen KI-Wissen direkt vor Ort. Juristische Orientierungshilfen schaffen Vertrauen in neue Technologien. Technologische Souveränität ist Kernbestandteil einer zukunftsfähigen Sicherheitsarchitektur. Das KI.M begleitet bayerische Medienunternehmen in der KI-Transformation – rechtssicher, praxisnah und zukunftsorientiert.



Veeam, der weltweite Marktführer im Bereich der Data Resilience, ist der Meinung, dass jedes Unternehmen in der Lage sein sollte, nach einer Störung

mit Vertrauen und Kontrolle über alle Daten weiterzumachen, wann und wo auch immer diese benötigt werden. Veeam nennt dies Absolute Ausfallsicherheit, und wir sind fokussiert, innovative Wege zu entwickeln, um unseren Kunden zu helfen, dies zu erreichen. Die Lösungen von Veeam wurden speziell für die Ausfallsicherheit von Daten entwickelt und umfassen Datensicherung, Datenwiederherstellung, Datenfreiheit, Datensicherheit und Datenintelligenz. Mit Veeam haben IT- und Sicherheitsverantwortliche die Gewissheit, dass ihre Anwendungen und Daten in ihren Cloud-, virtuellen, physischen, SaaS- und Kubernetes-Umgebungen geschützt und immer verfügbar sind. Mit Hauptsitz in Seattle und Niederlassungen in mehr als 30 Ländern schützt Veeam weltweit über 550 000 Kunden, darunter 87 Prozent der Fortune 500-Unternehmen, die auf Veeam vertrauen, um ihren Geschäftsbetrieb aufrechtzuerhalten.

*„Man gestehe sich doch so viel ein:
es bestünde gar kein Leben, wenn nicht
auf dem Grunde der perspektivischen
Schätzungen und Scheinbarkeiten ...
Ja, was zwingt uns überhaupt zu der
Annahme, dass es einen wesenhaften
Gegensatz von ‚wahr‘ und ‚falsch‘ gibt?“*

Friedrich Nietzsche

human FORWARD