Wie gefährdet ist Deutschland? Lageanalyse aus nachrichtendienstlicher Sicht

Vortrag von Dr. Bruno Kahl, Präsident des Bundesnachrichtendienstes

bei der Konferenz „Deutschlands Sicherheit – Der Beitrag des BND“ von Bildungswerk des Deutschen Bundeswehrverbandes und Gesprächskreis Nachrichtendienste in Deutschland am 28. Juni 2021 in Berlin

GKND-Hintergrundinformation

(Oktober 2021)

Im Rahmen seiner Bemühungen um eine sachgerechte Diskussion von Fragen der nationalen und internationalen Sicherheit und ihren Implikationen für die Nachrichtendienste konnte der GKND zusammen mit dem Bildungswerk des Deutschen Bundeswehrverbands den Präsidenten des Bundesnachrichtendienstes, Herrn Dr. Bruno Kahl, für einen Vortrag auf der Konferenz „Deutschlands Sicherheit – Der Beitrag des BND“ am 28. Juni 2021 gewinnen.

GKND und Bildungswerk danken Herrn Dr. Kahl für diese wertvolle Unterstützung und insbesondere auch für seine freundliche Bereitschaft, den richtungsweisenden Vortrag in schriftlicher Form im Rahmen einer GKND-Hintergrundinformation zur Verfügung zu stellen. Mit der aktuellen Veröffentlichung soll auch einen Beitrag zur weiteren sicherheitspolitischen Diskussion im Nachgang zu den Bundestagswahlen geleistet werden.

Der Vortrag wird nachfolgend in leichter redaktioneller Kürzung und Überarbeitung wiedergegeben.

Drei zentrale Herausforderungen für unsere gesamtstaatliche Sicherheit

Beispielhaft sollen hier drei Herausforderungen für unsere gesamtstaatliche Sicherheit benannt werden, denen sich der deutsche Auslandsnachrichtendienst aktuell gegenübersieht und auf die er angemessen reagieren muss. Natürlich gibt es weitere große Herausforderungen wie etwa Proliferation oder auch die Organisierte Kriminalität, die es sicherlich zu diskutieren lohnt, hier jedoch auch angesichts des limitierten zeitlichen Rahmens hinter Entwicklungen von epochaler Bedeutung zurückstehen müssen.

Sie werden gewiss Verständnis dafür haben, dass meine „Lageanalyse aus nachrichtendienstlicher Sicht“ in einer öffentlichen Veranstaltung wie dieser eher abstrakt ausfallen wird, und ich

entsprechend weniger auf die Frage, wer genau uns angreift, eingehe als vielmehr auf die Frage, wie dies geschieht.

Die Zeiten, in denen sich bei einer Krise zwischen zwei Nationen am Punkt maximaler Konfrontation zwei uniformierte Heere auf freiem Feld gegenüberstanden, um den Konflikt in offener Feldschlacht auszutragen, sind lange vorbei. Heute treten ausländische Akteure, die Böses im Schilde führen, uns in aller Regel nicht offen und in Uniform entgegen, um nach einer offiziellen Kriegserklärung die Kräfte zu messen. Wir haben es vielmehr mit einem bunten Mix aus Bedrohungen unserer Sicherheit zu tun, der sich auf alle gesellschaftlichen Bereiche erstreckt und oft aus dem Verborgenen heraus wirkt.

Wenn aber die Bedrohungen vielfältig, diffus, getarnt und unsichtbar daherkommen, werden wir ihnen nur wirkungsvoll begegnen können, wenn auch wir vernetzt und mit einem breiten Maßnahmenbündel handeln. Die eine große Entscheidungsschlacht, die alle offenen Fragen klärt, gibt es in unserer modernen, globalisierten und digitalisierten Welt nicht mehr. Wir müssen uns also fragen, wer uns wie testet, um adäquat reagieren zu können und die jeweilige Bedrohung erfolgreich abzuwehren.

Cyber-basierter „Information Warfare“ als maßgeblicher Teil des hybriden Bedrohungsspektrums

Die erste externe Herausforderung, die ich ansprechen will, und die unsere Sicherheit schon heute, aber verstärkt noch in der Zukunft gefährdet, sind sogenannte hybride Bedrohungen. Wir sprechen heute vom vielfältigen Spektrum hybrider Bedrohungen, wenn es darum geht, die zahlreichen Versuche von böswilligen Einflussnahmen und Einmischungen von außen in die Geschicke der Bundesrepublik Deutschland in einem Begriff zu bündeln. Oft gehen solche hybriden Angriffe von autokratischen fremden Mächten aus, die Deutschland, Europa und die freie Welt des Westens insgesamt schwächen wollen.

Es ist eine immense Herausforderung, die im Unterschied zur klassischen, historischen Propaganda äußerst anspruchsvollen, komplexen, oft indirekten und klandestinen hybriden Bedrohungen zu detektieren und verlässlich zu attribuieren. Denn die im Cyber- und Informationsraum handelnden Akteure setzen alles daran, eigene strategische Interessen so zu befördern, dass ihre Urheberschaft möglichst gar nicht oder allenfalls nur sehr schwer nachgewiesen werden kann.

Um ihre strategischen Ziele zu erreichen, nutzen sie vor allem drei Wege:

- Sie delegitimieren wesentliche demokratische Prozesse – in erster Linie Wahlen.
- Sie diskreditieren Entscheidungen und Entscheidungsträger – zuletzt etwa im Zusammenhang mit der Corona-Krise.
- Und sie polarisieren, um demokratische Gesellschaften zu spalten – wie es etwa in den USA zu beobachten war, aber auch hier und heute in Deutschland und Europa stattfindet.

Die Akteure unterziehen Staat und Gesellschaft einer Schwachstellenanalyse, um geeignete Angriffspunkte zu finden. Diese nutzen sie anschließend aus, um Einfluss flexibel in möglichst

vielen Dimensionen auszuüben: Politik, Kultur, Medien, Streitkräfte, Ökonomie und Ökologie werden zu Land, zu Luft, zu See, im Informationsraum, im Cyberraum und im Weltraum angegriffen.

Nahezu gewöhnt haben wir uns bereits an ein kontinuierliches „Grundrauschen" der hybriden Bedrohungen in Form eines aktiven und intensiven Bedienens des Informationsraums mit Propaganda, Desinformation und Diskreditierungsansätzen. Dabei können ausländische Akteure auch indirekt wirken, indem sie deutsche Extremisten zum Beispiel durch Propaganda in Auslandsmedien oder auch über die kostengünstigen und nur schwer zu kontrollierenden Sozialen Medien aufstacheln und zum Handeln motivieren. Zudem stellen Deep Fakes in Verbindung mit KI-Anwendungen zur Realisierung umfassender Desinformationsoperationen eine neue Gefahr dar. Auch der immer beliebtere Doppelschritt aus „Hack and Leak" birgt zunehmende Risiken.

Und es ist nicht etwa so, dass die gegenwärtige Corona-Krise die weltweiten Ambitionen aufstrebender Mächte gebremst hätten – ganz im Gegenteil: Sie nutzen die Pandemie sowie deren Folgen geschickt, um verstärkt und verdeckt zu ihren eigenen Gunsten und zum Schaden der freien Welt zu agieren. Seit Beginn der Corona-Krise versuchen sie, hinter der Fassade angeblicher Hilfsbereitschaft wirtschaftliche und politische Einflusssphären auf der ganzen Welt zu vergrößern und zu festigen, indem sie sich als Normgeber präsentieren. Grundsätzlich sollten Politik und Wirtschaft folglich nicht jedes Angebot annehmen, das uns eine andere Seite macht. Vielmehr sollten wir jeweils genau prüfen, was die langfristigen Folgen, Kosten und Abhängigkeiten einer Offerte sein könnten, die uns zunächst als angemessen, großzügig oder gar selbstlos erscheinen mag.

Da wir in Deutschland in wenigen Monaten Bundestagswahlen haben, ist der BND im Verbund mit anderen Sicherheitsbehörden darum bemüht, die Integrität und Sicherheit der Bundestagswahl wie auch des vorausgehenden Wahlkampfs zu gewährleisten und möglichst geeignete Vorkehrungen gegen allfällige Einflussnahmen und Einmischungen von außen zu treffen.

Insgesamt wird der Cyber- und Informationsraum weiter an Bedeutung gewinnen – vor allem wenn es um unklare Konfliktdynamiken und unübersichtliche Bedrohungslagen geht. Soziale Medien und Fake News werden als Wirkmittel immer stärker zur Geltung kommen und Auseinandersetzungen um Narrative entbrennen.

Terrorismus und Migration als geopolitische Destabilisierungsfaktoren und Herausforderung gesamtstaatlicher Sicherheit

Kommen wir zu einer zweiten Herausforderung, die vielgestaltig ist und ein koordiniertes Vorgehen auf verschiedenen Ebenen verlangt: Auch der internationale Terrorismus sowie das – vom Terror mit ausgelöste – massive Migrationsgeschehen bleiben uns in den nächsten Jahren erhalten – und werden dabei entscheidenden Einfluss auf die weitere Destabilisierung traditionell ohnehin eher instabiler Weltregionen wie den Nahen und Mittleren Osten, Nordafrika, die Sahel-Zone oder auch Zentralasien haben. Die Folgen von internationalem Terror und weltweiten Migrationsbewegungen wiederum werden auch auf die Sicherheitslage in Deutschland und Europa ausstrahlen.

Und dann ist da noch ein ganzer Kontinent, dessen Entwicklung nicht vom Rest der Welt abgekoppelt werden kann: Afrika ist groß, jung, vernetzt, fragil und wachsend. Afrika wird eine immer dichter bevölkerte Region sein – nicht allein, was die Zahl seiner Bewohner angeht, sondern auch, was die Zahl der Akteure, der Ideen und Ideologien anbelangt, die sich in Afrika weiter ausbreiten werden. Verschiedene Mächte treiben in Afrika ihr geopolitisches Spiel. Die afrikanische Bevölkerung wächst jedes Jahr um rund drei Prozent. Damit ist Afrika der am schnellsten wachsende Kontinent. Für das Jahr 2050 wird mit einer Verdoppelung der Bevölkerung auf mehr als 2,5 Milliarden Afrikaner gerechnet: Heute stellen die Afrikaner rund 17 Prozent der Weltbevölkerung, in 30 Jahren wird jeder vierte Mensch auf der Welt in Afrika geboren sein.

Wir können und müssen davon ausgehen, dass Probleme, die in Afrika entstehen, nicht in Afrika bleiben, sondern uns immer mehr auch in Europa und Deutschland beschäftigen werden, als sie es zum Teil heute schon tun. Hier spielen auch Ressourcenknappheit und der Klimawandel eine besondere Rolle.

Wenn wir den internationalen Terrorismus, die weltweiten Migrationsbewegungen und die Entwicklung unseres südlichen Nachbarkontinents ignorieren oder nur punktuell betrachten, werden Probleme vermeintlich ferner Regionen rasch unsere gesamtstaatliche Sicherheit herausfordern. Auch hier müssen wir ganzheitlich und nachhaltig handeln, indem wir militärische Optionen mit Möglichkeiten der Diplomatie, der Entwicklungshilfe und auch zivilgesellschaftlicher Initiativen verbinden.

Cyber-Angriffe auf kritische Infrastruktur, eine ebenso disruptive wie existenzielle Sicherheitsbedrohung

Lassen Sie mich noch kurz zu einer dritten großen Herausforderung kommen, mit der sich der BND beschäftigen muss: Einige ausländische Nachrichtendienste betreiben im Verbund mit Hackergruppen Spionage und Sabotage im großen Stil – und zwar nicht nur gegenüber uns, den Sicherheitsbehörden oder Regierungen, sondern auch gegenüber großen, mittleren und kleinen Unternehmen, die in ihren jeweiligen Bereichen Champions sind.

Trends wie das Internet der Dinge werden zu einem Multiplikator für Risiken: Die Manipulation von automatisierten Fahrzeugen, der IT-gestützten Verkehrslenkung oder von IT-Anwendungen im Gesundheitswesen kann ernsthafte Gefahren für Leib und Leben herbeiführen. Gezielte Cyber-Angriffe auf die Infrastruktur von Banken oder die Manipulation von Börsenkursen können zu einer ernsten Gefahr für die Finanzmärkte mit weitreichenden Auswirkungen auf die Wirtschaft werden. Folglich ist der smarte Kühlschrank, der selbstständig Produkte nachbestellt, gesamtgesellschaftlich das kleinere Risiko als eine digitalisierte und automatisierte Wertschöpfungskette, die von einem Wettbewerber oder einem feindlichen Nachrichtendienst gehackt wird.

Bei allen bestehenden Risiken müssen wir – Politik, Wirtschaft und auch ganz konkret die deutschen Sicherheitsbehörden – uns aber dem globalen Wettbewerb stellen. Denn wie wir alle nur zu gut wissen, leben wir in einer Welt, die sich stetig und mit immer größerem Tempo weiterentwickelt. Dabei haben wir es im Bereich der digitalen Technologien mit Innovationen zu tun,

die oft nicht evolutionär, sondern revolutionär und disruptiv auf den Markt kommen und das nachgefragte Angebot fundamental umgestalten. Diese Tendenz zu disruptiven Innovationen ist für uns als Sicherheitsbehörden Risiko und Chance zugleich: Wir können die neuen Möglichkeiten für uns nutzbar machen, gleichzeitig verwenden aber auch unsere Gegner innovative Technologien, um wiederum uns auszutricksen.

Man kann hier von einer Art Wettrüsten sprechen:

- Terroristen, Kriminelle und bestimmte ausländische Mächte finden immer neue Wege, um unsere Mittel und Methoden zur Herstellung von Sicherheit zu unterlaufen.
- Unsere Sicherheitsbehörden investieren im Gegenzug immer mehr in Technik und Köpfe, um dies zu verhindern.
- Man muss aber kein Soldat sein, um zu verstehen, warum der Angreifer hier immer im taktischen Vorteil ist.

Technologische Zukunftsfähigkeit als strategische Herausforderung

Jeder Nachrichtendienst, der seinen Auftrag ernst nimmt, muss seine Prozesse, Strukturen und Produkte laufend selbstkritisch hinterfragen und erneuern, wenn er auf der Höhe der Zeit sein und bleiben will. Denn Terroristen und Kriminelle nehmen genauso wenig Rücksicht auf bürokratische Beharrungskräfte wie der technische Fortschritt oder die revisionistischen Absichten anderer Staaten.

Eine der vielen internationalen digitalen Innovationen, mit denen sich der Bundesnachrichtendienst beschäftigen muss, ist die Künstliche Intelligenz, deren Chancen, aber auch Risiken unsere Gesellschaft deutlich prägen werden. Wir befassen uns intensiv damit, welchen Einfluss KI auf unsere Arbeit als Auslandsnachrichtendienst haben wird – sowohl als Aufklärungsziel wie auch als Faktor, der direkt auf unsere eigene Tätigkeit einwirkt.

KI – oder besser: Machine Learning – wird absehbar zu einer Querschnittstechnologie werden und sich nahezu in allen Bereichen unseres Lebens und Arbeitens voll auswirken. Dabei wird KI uns nicht nur Erleichterungen im Alltag wie selbstfahrende Autos und lernende Maschinen bescheren, sondern auch die internationale Politik verändern. Sie bietet – je nach Perspektive – geopolitische Möglichkeiten und Bedrohungen, die sich konkret nur schwer fassen und vorhersagen lassen, mit denen wir Nachrichtendienste uns aber bis ins Detail auseinandersetzen müssen.

Wenn Deutschland global nicht ins Hintertreffen geraten soll, müssen wir im Bereich technologischer Innovationen agil und leistungsfähig bleiben. Die Politik hat geeignete Rahmenbedingungen zu entwickeln, damit die Innovationskraft der deutschen Unternehmen sich bestmöglich entfalten kann. Aufgabe der Sicherheitsbehörden ist es in diesem Prozess, Risiken frühzeitig zu erkennen und Politik wie Wirtschaft vorausschauend zu beraten.