„Wir brauchen einen angemessenen, der technischen Entwicklung angepassten Werkzeugkasten.“

Ein Interview mit dem Vizepräsidenten des Bundesamtes für Verfassungsschutz *Thomas Haldenwang

Foto: *Bundesamt für Verfassungsschutz*

Thomas Haldenwang hat in Marburg an der Lahn Rechtswissenschaften studiert. Das Referendariat im OLG-Bezirk Düsseldorf beendete er 1991 mit dem 2. juristischen Staatsexamen. Von 1991–2000 war er als Referent in der Dienstrechtsabteilung sowie als Personalreferent im Bundesministerium des Innern tätig. Im Jahr 2000 wechselte er als Referatsgruppenleiter in das Bundesverwaltungsamt, wo er für Fachaufgaben verschiedener Bundesministerien zuständig war.
2006 kehrte er in das Bundesministerium des Innern zurück. Er leitete dort das Referat „Laufbahnrecht“ und übernahm die Geschäftsführung des Bundespersonalausschusses. Seit 2009 ist Herr Haldenwang im Bundesamt für Verfassungsschutz (BfV) tätig. Er leitete bis Ende 2012 die Zentralabteilung und wurde sodann zum Ständigen Vertreter des Vizepräsidenten bestellt. Seit dem 1. August 2013 ist er Vizepräsident des BfV.

Bonner Rechtsjournal (BRJ): *Herr Haldenwang, Deutschland hat sich in den letzten Jahren Bedrohungen aus vielen verschiedenen Richtungen ausgesetzt gesehen. Was sind Ihrer Meinung nach die größten Herausforderungen für das BfV?*

Haldenwang: Der islamistische Terrorismus bleibt die größte Bedrohung für die Sicherheit in der Bundesrepublik Deutschland. Von Einzeltätern und sogenannten „Jihad-Rückkehrern“ geht eine schwer kalkulierbare und vor allem langfristige Gefahr aus. Auf den IS steigt durch seine Gebietsverluste in Syrien der Druck, durch Anschläge – auch in Europa – seine Drohkulisse aufrecht zu erhalten.
Die Zahl der Extremisten in Deutschland ist auch im vergangenen Jahr gestiegen. Die massiven Ausschreitungen beim G20-Gipfel in Hamburg haben in aller Deutlichkeit – und: in aller Brutalität – gezeigt, dass Linksextremisten in der Lage sind, Gewalt zu mobilisieren und diese auch organisiert auszuüben. Die gestiegene Gewaltbereitschaft bei allen Extremisten in Deutschland – auch im Rechtsextremismus und Ausländerextremismus – gibt Anlass zur Sorge. Daneben gehören Cyberangriffe zu den größten Bedrohungen, denen wir in Deutschland ausgesetzt sind. Es geht dabei längst nicht mehr nur um wirtschaftliche Verluste deutscher Unternehmen, die Opfer von Ausforschungen oder Sabotage werden. Cyberangriffe attackieren die Grundfeste unseres Zusammenlebens: unsere Demokratie. Zwar wurde die Bundestagswahl 2017 ohne größere Störungen durchgeführt. Dennoch sind Desinformationskampagnen und Cyberangriffe – zum Beispiel auf Regierungsnetze oder kritische Infrastrukturen – zentrale Herausforderungen, denen wir uns noch stärker stellen müssen.

BRJ: *Worauf lässt sich die Entwicklung so diverser Bedrohungsherde von vergleichbarer Bedeutung und Intensität zurückführen?*

Haldenwang: Angesichts der geopolitischen Lage erstaunt dies nicht. Die Lage in Syrien ist nach wie vor kritisch. Zudem droht ein globaler Handelskrieg. Die Instabilität nimmt deutlich zu, die alte Weltordnung gilt nicht mehr und frühere Gewissheiten lösen sich auf. Es gibt instabile Staaten – und das alles hat Auswirkungen auf Deutschland. Außerdem

* Das Interview wurde von Marie Moritz und Jülide Kaya vorbereitet; die Fragen wurden am 22.08.2018 schriftlich beantwortet.

haben wir auch in Europa interne, innerstaatliche Stabilitätsprobleme, die etwa mit dem Austritt Großbritanniens aus der EU oder dem Aufkommen von Rechtspopulismus zusammenhängen. Zudem beschleunigt sich durch die Digitalisierung Vieles. Ein schnellerer Informationsaustausch bedingt auch schnellere Reaktionen.

BRJ: *Eine Veränderung des gesellschaftlichen Klimas ist spürbar, nicht zuletzt in Gestalt des Phänomens, dass sich die Bevölkerung mit der ständigen Möglichkeit von Terroranschlägen an Orten des täglichen Lebens, sog. „weichen Zielen", gewöhnt hat. Das wäre vor ein paar Jahren in dieser Form nicht denkbar gewesen. Was tut das BfV konkret, um solche Anschläge zu verhindern?*

Haldenwang: Islamistische Gruppierungen setzen bei der Auswahl potenzieller Ziele für terroristische Aktivitäten auf ein breit gefächertes Spektrum. Symbolhafte und „weiche" Anschlagsziele stehen dabei im Vordergrund. Jihadistisch motivierte Attentate in europäischen oder westlichen Staaten werden zudem zunehmend mit leicht zu beschaffenden und einzusetzenden Tatmitteln und weniger komplex ausgeführt.
Dass es im Jahr 2017 nur zu einem islamistisch motivierten Terroranschlag in Deutschland kam, ist unter anderem auf erfolgreiche bundesweite Aufklärungsarbeit der Sicherheitsbehörden zurückzuführen. So wurden bspw. in 2017 – auch unter Mitwirkung des BfV – in einer Vielzahl von Fällen Anschlagsplanungen tatgeneigter Islamisten frühzeitig aufgedeckt oder Anschlagsvorhaben vereitelt, die sich bereits in einem konkreten Vorbereitungsstadium befanden. Erinnert sei auch an die erfolgreiche Aufklärung des Rizin-Falls in Köln-Chorweiler. Auch die nationale und internationale Zusammenarbeit wird ständig verbessert. Auf nationaler Ebene findet ein täglicher Austausch im Gemeinsamen Terrorismusabwehrzentrum (GTAZ) in Berlin statt. Auf europäischer Ebene wurde Anfang 2017 mit der Eröffnung einer operativen Plattform der Counter Terrorism Group (CTG) ein sehr großer Schritt nach vorne gemacht. Mitarbeiter der teilnehmenden Nachrichtendienste tauschen dort regelmäßig ihre Erkenntnisse aus. Die Plattform hat sich bereits als ein wirkungsvolles Instrument bei der Bekämpfung des islamistischen Terrorismus erwiesen. Mehrere mutmaßliche islamistische Terroristen und Unterstützer des IS konnten verhaftet werden, nicht zuletzt aufgrund der in der Plattform ausgetauschten Erkenntnisse.
Den größten Teil der Informationen gewinnt der Verfassungsschutz allerdings aus offenen, allgemein zugänglichen Quellen. Insbesondere das Internet spielt hier eine große Rolle. Aber auch die Anwendung nachrichtendienstlicher Mittel ist für die Informationsgewinnung unverzichtbar. Dazu gehören das Führen von V-Leuten (angeworbene Personen aus der extremistischen Szene), die Observation und die von einem parlamentarischen Gremium kontrollierte Brief- und Telefonüberwachung.

BRJ: *Welche Auswirkungen hat die Schwächung des IS durch immense Gebietsverluste in Syrien und Irak auf die Sicherheitslage in Deutschland?*

Haldenwang: Durch die militärischen Niederlagen in Syrien steigt der Druck auf den IS, durch Anschläge – auch in Europa – seine Drohkulisse aufrecht zu erhalten. Der IS bereitet sich auf die „Zeit danach" vor und treibt seine Strategie des Terrors gegen „weiche Ziele" voran. Die Propaganda des IS hat sich von Aufrufen zur Ausreise und Kampfteilnahme dahingehend verlagert, dass zu Einzeltäteranschlägen in westlichen Ländern aufgerufen wird.

BRJ: *Sind Rückkehrer aus den Gebieten des Islamischen Staats (IS) als „Gefährder" einzustufen?*

Haldenwang: Bei dem Begriff des „Gefährders" handelt es sich um eine rein polizeiliche Begrifflichkeit. Die Verfassungsschutzbehörden identifizieren das islamistischterroristische Personenpotenzial, das die Zahl der Gefährder beinhaltet. Dieses beläuft sich aktuell auf rund 2.220 Personen. Das Thema „Umgang mit Rückkehrern aus Kampf-Gebieten, insbesondere aus Syrien bzw. Irak" steht derzeit im Fokus der Sicherheitsbehörden. Auch wenn immer noch keine massive Rückreisebewegung erkennbar ist, muss damit gerechnet werden, dass ein beträchtlicher Teil dieser Personen sukzessive versuchen wird, nach Deutschland zurückzukehren. Von diesen Rückkehrern, auch von Frauen und Kindern, könnte ein erhebliches Bedrohungspotenzial ausgehen, weshalb Maßnahmen der Deradikalisierung eine wesentliche Rolle spielen. Etwa ein Drittel der in Richtung Syrien/Irak ausgereisten Personen befindet sich gegenwärtig wieder in Deutschland. Nicht alle der insgesamt 1.000 Ausgereisten versuchen jedoch nach Deutschland zurückzukehren: Einige weichen in benachbarte Regionen aus, andere versuchen in andere Jihad-Gebiete (z.B. in Richtung Afghanistan) weiterzureisen. Hinzu kommen Todesfälle und Gefangennahmen durch andere Konfliktparteien. Das von Rückkehrern ausgehende Gefährdungspotenzial ist differenziert und im Einzelfall zu betrachten. Es gibt Rückkehrer, die völlig „desillusioniert" und abgewandt von ihrer früheren Einstellung wieder nach Deutschland einreisen. Andere könnten weiterhin hoch radikalisiert sein. Relevant für deutsche Sicherheitsbehörden ist außerdem, dass diese Personen oft über Erfahrungen im Umgang mit Waffen und Sprengstoff sowie über Kontakte zu anderen jihadistischen Kämpfern und zu terroristischen Organisationen verfügen. Im Umgang mit Rückkehrern kommt es vor allem auf einen umfassenden Informationsaustausch aller Sicherheitsbehörden, eingehende Beurteilung der Personen und die Abstimmung der zu treffenden Maßnahmen an.

BRJ: *Die in diesem Kontext notwendig zu erhebenden Informationen werden aus offen zugänglichen Quellen oder mit sogenannten nachrichtendienstlichen Mitteln gewonnen.[1] Wie bewerten Sie das Spannungsfeld zwischen Terrorismusabwehr und Datenschutz, insbesondere vor dem Hintergrund des Inkrafttretens der europäischen Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018?*

Haldenwang: Es ist notwendig, dass wir die Befugnisse der Nachrichtendienste mit Augenmaß ausstatten. Aktuell können wir trotz steigender Datenmengen, letztlich als Nebenfolge der digitalen Entwicklung, – wir nennen das Phänomen „going dark" – weniger Erkenntnisse von überwachten Personen gewinnen. Als Sicherheitsbehörde müssen wir aber relevante Daten zügig und zuverlässig erfassen und auswerten. Dazu brauchen wir einen angemessenen, der technischen Entwicklung angepassten, Werkzeugkasten.
Vor diesem Hintergrund ist es wichtig, das Spannungsverhältnis zwischen Datenschutz und Schutz vor Terrorismus nicht statisch zu sehen, sondern jeweils entsprechend der Sicherheitslage in Übereinstimmung zum Grundrechtsschutz neu auszutarieren. Das ist mitunter mühselig, lohnt sich aber, wenn wir weiterhin Freiheit in Sicherheit genießen wollen. Da die europäische DSGVO nur im Kompetenzrahmen der Europäischen Union gilt, die gemäß Art. 4 Abs. 2 Satz 3 EUV keine Regelungskompetenz für die Angelegenheiten der nationalen Sicherheit und damit für den Bereich des Verfassungsschutzes besitzt, findet die DSGVO bei der spezifischen Aufgabenerfüllung des BfV keine Anwendung.

BRJ: *Der Tätigkeitsbereich des BfV wird unter anderem durch das verfassungsrechtlich gewährleistete Staatsprinzip des Föderalismus geprägt, es gibt neben Ihrer Behörde 16 Landesämter für den Verfassungsschutz. Ist das nicht in Anbetracht zunehmender Vernetzung und Mobilität der zu überwachenden Personen zur Wahrnehmung Ihrer Aufgabe eher hinderlich?*

Haldenwang: Die Landesämter und das BfV sind als Verfassungsschutzverbund gut miteinander vernetzt und stehen in einem ständigen Austausch miteinander. Die Präsenz des Verfassungsschutzes in der Fläche bietet viele Vorteile. So kann durch einen Verfassungsschutz „vor Ort" bedarfsgerecht auf regionale und kommunale Spezifika der jeweiligen Phänomenbereiche eingegangen werden. Eine zentrale Steuerung und Koordinierung der Aktivitäten der Verfassungsschutzbehörden ist aber zwingend geboten. Die Zentralstellenfunktion des BfV gewährleistet schnellere Entscheidungs- und Meldewege und einheitliche Standards – gerade in Gefährdungslagen, aber auch bei der Bearbeitung einzelner Gefährdungshinweise. Diese koordinierende Rolle des BfV muss auch zukünftig weiter gestärkt werden. Derzeit wird mit den LfV an der Weiterentwicklung gemeinsamer Standards innerhalb des Verfassungsschutzverbundes gearbeitet. Angestrebt ist eine Harmonisierung des gesetzlichen und untergesetzlichen Rechtsrahmens. Vereinheitlicht werden sollen daneben auch die verwendeten Termini, sowie die Speicherpraxis in gemeinsamen Dateien.

BRJ: *Der Tätigkeit des BfV werden außerdem durch das Trennungsgebot von Polizei und Nachrichtendiensten Grenzen gesetzt, welches auf Bundesebene in § 2 Abs. 1 und § 8 Abs. 3 BVerfSchG geregelt ist und auf den Polizeibrief der alliierten Militärgouverneure aus dem Jahr 1949 zurückgeht. Es werden dennoch Wege der Kooperation gesucht und beschritten, so z.B. das „Gemeinsame Terrorismusabwehrzentrum", welches mit dem Ziel behördenübergreifender Zusammenarbeit auf Grundlage des geltenden Rechts zur effektiveren Terrorismusbekämpfung bereits 2004 eingerichtet wurde. Sehen Sie in Konfrontation mit der weiter veränderten Gefahrenlage den Bedarf bzw. die Legitimität, für spezielle Gefahrenbereiche Modifikationen an den gesetzlichen Rahmenbedingungen vorzunehmen? Ist es nicht vielleicht sogar an der Zeit, über 70 Jahre nach dem Ende des Dritten Reichs im Rahmen eines konsolidierten demokratischen Rechtsstaats das Trennungsgebot in seiner Grundkonzeption zu überdenken und z.B. dem BfV auch Ermittlungsbefugnisse zu gewähren, oder wie könnten Modifikationen Ihrer Ansicht nach ausgestaltet sein?*

Haldenwang: Historisch betrachtet ist das Trennungsgebot sinnvoll und wichtig. Es beinhaltet eine Trennung der Befugnisse und der organisatorischen Einrichtung. Mit dem Urteil des BVerfG zum Antiterrordatei-Gesetz aus dem Jahr 2013 hat das BVerfG festgestellt, dass sich das Trennungsgebot auch auf eine informationelle Trennung erstreckt. Seitdem ist der Informationsaustausch zwischen den Nachrichtendiensten und Polizeibehörden an strengere Voraussetzungen geknüpft. So sind zum Beispiel die Voraussetzungen des § 19 Abs. 1 BVerfSchG (Übermittlung von personenbezogenen Daten des BfV an inländische öffentliche Stellen) verschärft worden. In Zeiten eines erkennbaren Anstiegs an Terrordrohungen und Cyberangriffen sind allerdings institutionalisierte Wege des Informationsaustausches der zentralen Sicherheitsbehörden zwingend erforderlich. Denn Verfassungsschutz funktioniert nur durch informationelle Zusammenarbeit. In den zurückliegenden Jahren sind daher Foren und Plattformen geschaffen worden, die die Zusammenarbeit der Sicherheitsbehörden im Rahmen der vom BVerfSchG geschaffenen Voraussetzungen institutionalisieren. Das BfV arbeitet

[1] *Anm. d. Red.*: Die rechtliche Grundlage für die Informationsgewinnung bildet das BVerfSchG, welches materielle Voraussetzungen für die verschiedenen Maßnahmen regelt. Maßnahmen zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses sowie die anschließende Verarbeitung und Nutzung der dadurch erlangten personenbezogenen Daten unterliegen außerdem dem Artikel 10-Gesetz, sog. G 10-Gesetz. Sie sind von einer zu beantragenden Entscheidung über die Zulässigkeit und Notwendigkeit einer Maßnahme durch die G 10-Kommission abhängig. Die G10-Kommission wird vom Parlamentarischen Kontrollgremium als unabhängiges Kontrollgremium für die Dauer einer Wahlperiode bestellt.

hier unter Berücksichtigung des Trennungsgebotes eng mit den beteiligten Behörden zusammen. Plattformen wie das „Gemeinsame Terrorismusabwehrzentrum" stellen für alle Behörden eine wichtige Einrichtung dar, um einen zeitnahen und effektiven Informationsaustausch auf Grundlage der jeweils geltenden Übermittlungsvorschriften zu garantieren und so einen Beitrag zur öffentlichen Sicherheiten zu leisten.

BRJ: *Das Internet, insbesondere das Darknet, ist ein existenzsicherndes Medium für den IS-Terrorismus aber auch für andere Formen des Extremismus und Terrorismus. Wie effektiv kann das BfV seine Aufgaben dort wahrnehmen; sind z.B. überhaupt Personen identifizierbar und ist eine Zuordnung von Vorgängen und Transaktionen möglich?*

Haldenwang: Für eine umfassende Aufgabenerfüllung des BfV ist eine gezielte Informationserhebung im Internet von besonderer Bedeutung. Die offen einsehbaren Online-Aktivitäten von Extremisten und Jihadisten können gezielt nachvollzogen, erfasst und bewertet werden. Den nachrichtendienstlich relevanten Teil stellen die nicht offen einsehbaren Online-Aktivitäten dar, da die Mehrheit der Szeneangehörigen mittlerweile sensibler und verborgener im Internet agiert und die Nutzer ihre Identität und Absichten zunehmend verschleiern. Ein großer Teil der Kommunikation findet in geschlossenen, „privaten" Nutzer-Gruppen statt, die nicht für jedermann zugänglich sind. Um diese Aktivitäten beobachten zu können, erfolgt die Informationserhebung insbesondere mithilfe des Einsatzes nachrichtendienstlicher Mittel. Das Phänomen „going dark" ist eine besondere Herausforderung für die Sicherheitsbehörden. Vorgänge und Transaktionen zu überwachen kann allerdings nur mit enormen zeitlichem und personellem Aufwand geleistet werden. Oftmals handelt es sich dabei um die bekannte Nadel in einem riesigen Heuhaufen.

BRJ: *Wie beurteilen Sie die Bedrohung durch Cyberangriffe und droht die zunehmende Digitalisierung staatlicher Institutionen aber auch der Wirtschaft zum Einfallstor für derartige Angriffe zu werden, sodass empfindliche Informationen zum Mittel politischer Wirkmacht werden können?*

Haldenwang: In den letzten Jahren hat sich insbesondere die Spionage durch Cyberangriffe zum Standardwerkzeug für einige Nachrichtendienste entwickelt. Diese Entwicklung geht einher mit einem hohen Gefährdungspotential für potenzielle und tatsächliche Opfer. Dabei beobachten wir große Angriffskampagnen nicht nur auf deutsche Regierungsnetze und Konzerne, sondern auch Angriffe auf kleine und mittelgroße Unternehmen. Besonders die Nachrichten- und Sicherheitsdienste der Russischen Föderation, der Volksrepublik China und des Iran entfalten dabei in großem Umfang Spionageaktivitäten gegen Deutschland. Deren Schwerpunkte orientieren sich an den politischen Vorgaben ihrer Regierungen. Hierzu gehört auch der gesetzliche bzw. staatliche Auftrag mit nachrichtendienstlich beschafften Informationen die eigene Volkswirtschaft zu unterstützen. Auch sind Cyberangriffe ein hervorragendes Mittel, Desinformations- und Einflussnahmekampagnen zu unterstützen. Etwa um Einfluss auf Wahlergebnisse oder andere gesellschaftlich relevante Ereignisse zu nehmen. Dass die zunehmende Digitalisierung diese Gefährdungssituation noch deutlich verstärkt, liegt auf der Hand.

BRJ: *Der bayerische Verfassungsschutz unterhält ein Cyber-Allianz-Zentrum (CAZ), das die Aufgabe hat, Wirtschaftsunternehmen zu helfen, die Opfer von Spionage und Sabotageangriffen geworden sind. Wäre das auch eine Option für das BfV?*

Haldenwang: Auf Bundesebene haben mehrere Behörden Zuständigkeiten im Cyberbereich. Daher ist das Nationale Cyber-Abwehrzentrum (Cyber-AZ) eine mögliche Anlauf- und Koordinierungsstelle. Das BfV selbst stellt sich der zunehmenden Bedrohung durch Beschreiten neuer, innovativer Wege. So verfügen wir zum Beispiel über mobile Cyberteams, die nach einem Cyberangriff bei Betroffenen vor Ort forensische Analysen vornehmen können. Auch ist das BfV bei IT-Sicherheitsvorfällen in der Lage, durch die Bereitstellung sog. „Indicators of Compromise" schnell erste Hilfe zu leisten. Mit diesen Informationen unterstützen wir betroffene Unternehmen, ihren Schutz vor Cyberangriffen zu erhöhen. Daneben verfährt das BfV auch nach dem Konzept „Verfassungsschutz durch Aufklärung". Hier versuchen wir z.B. durch Sensibilisierungsmaßnahmen in Verwaltung, Wirtschaft und Wissenschaft ein entsprechendes Problembewusstsein zu schaffen. Außerdem werden durch Veröffentlichung eines „Cyber-Briefs" regelmäßig gezielt Warnmeldungen und Berichte an Behörden und in die Wirtschaft gesteuert.

BRJ: *Zum Abschluss würden wir gerne einen Blick in die Zukunft wagen: Denken Sie, dass die Vielgestaltigkeit und Vielschichtigkeit der Bedrohungen, z.B. durch die Nutzung des Internets als weltverbindendes Medium, das uns bekannte Gefüge der freiheitlich demokratischen Rechtsordnung auf Dauer verändern wird?*

Haldenwang: Neue Bedrohungen strapazieren auch die freiheitliche demokratische Grundordnung. Als Teil der Sicherheitsarchitektur gehört es zu den Kernaufgaben des BfV die freiheitlich demokratische Rechtsordnung auch weiterhin zu schützen. Damit wir künftigen Herausforderungen gewachsen sind, hat die Politik reagiert und uns Ressourcen zur Verfügung gestellt, die uns ertüchtigen auch in Zukunft abwehrbereit zu sein.

BRJ: *Herr Haldenwang, wir bedanken uns sehr für das Interview!*