"Parlamentarische Kontrolle ist nützlich"

Digitalisierung stellt Nachrichtendienste vor zahlreiche neue Herausforderungen

(BS/Marco Feldmann) Die fortschreitende Digitalisierung geht einher mit einem erhöhten Gefährdungspotenzial. So werde der Kreis möglicher Opfer immer größer und es böten sich vermehrt Möglichkeiten zur Datenausspähung sowie zur Desinformation und zum Datenmissbrauch. Davor warnte der kommissarische Präsident des Bundesamtes für Verfassungsschutz (BfV), Thomas Haldenwang.

Diskutierten über eine effektive parlamentarische Kontrolle von Nachrichtendiensten (v.l.n.r.): Dr. André Hahn (Linke), Uli Grötsch (SPD), Dr. August Hanning (Moderator), Armin Schuster (CDU) und Dr. Konstantin von Notz (Bündnis 90/Die Grünen). Fotos: BS/Feldmann

Des Weiteren erhöhe die Digitalisierung, und insbesondere die verstärkte Nutzung Sozialer Netzwerke, das Mobilisierungspotenzial des politischen Extremismus hierzulande. Die Kraft des politischen Extremismus zur Mobilisierung und Radikalisierung hänge auf das Engste mit der Digitalisierung zusammen. Zudem werde eine immer enthemmtere Sprache genutzt. "Digitale Kommunikationsmittel befeuern den politischen Extremismus. Bekanntlich laden digitale Plattformen und Chat-Communities zwar zur Meinungsäußerung ein, dienen aber nicht unbedingt der Kompromissbildung und nur selten der sachlichen Debatte", zeigte sich *Haldenwang* alarmiert. Und er warnte: "Die Grenze zwischen dem rechtsextremen und dem bürgerlichen Lager verwischt immer mehr. Alle Phänomenbereiche erleben durch die Digitalisierung eine Dynamisierung." Sie erleichtere anonymisierte Hetze und Propaganda, die Mobilisierung von Anhängern, die Rekrutierung von Zielgruppen sowie verschlüsselte Kommunikation zwischen Szeneangehörigen. Das hätten nicht zuletzt die jüngsten Ereignisse in Chemnitz gezeigt. Durch das Internet werde aus dem politischen Gegner der ideologische Feind. Außerdem konstatiere man vermehrt Erosionen zwischen rechtsextremistischen und nicht-extremistischen Positionen.

Zwiespältige Datenflut

Für diese Feststellung erhielt er Zuspruch vom Leiter des brandenburgischen Verfassungsschutzes, *Frank Nürnberger*. Auch dieser warnte vor einer immer stärkeren Nutzung Sozialer

Der kommisarische BfV-Präsident Thomas Haldenwang warnte vor den Folgen der Digitalisierung.

Netzwerke durch Extremisten und einer Fragmentierung der Gesellschaft durch den Verlust von Konstanten. *Haldenwang* wies aber noch auf ein weiteres Problem hin: alternative Fakten. Diese erschwerten den politischen Diskurs massiv. Schließlich gelte: "Sicherheit kann erst entstehen, wenn aus Daten Fakten und aus Erkenntnissen Lagebilder werden." Die Datenflut der modernen Gesellschaft sei für Nachrichtendienste "zugleich Segen und Fluch". Noch nie seien derart viele Informationen so leicht abrufbar gewesen. Es sei bisher aber auch noch nie so aufwendig gewesen, aus dieser täglichen Datenlawine Relevantes von Irrelevantem und Zutreffendes von Unzutreffendem zu unterscheiden, so der komissarische Behördenleiter. Fakten und Fake News würden im Datenstrom verschwimmen. Denn: Soziale Medien sorgten für eine virale Verbreitung alternativer Fakten.

Torsten Voß, der derzeit auch Vorsitzender des für Verfassungsschutzangelegenheiten zuständigen Arbeitskreises vier in der Innenministerkonferenz (AK IV der IMK) ist, unterstrich zudem: "Die Nachrichtendienste müssen rechtlich und technisch die Möglichkeit haben, Extremisten immer zu überwachen." Da diese oftmals verschlüsselte Kommunikationswege, etwa in Form entsprechender Messengerdienste, nutzten, sei das jedoch momentan nicht durchgängig der Fall. Aus diesem Grunde verlangte *Voß*, dass die Befugnisse der Verfassungsschutzbehörden mit dem technischen Fortschritt und der geänderten Bedrohungslage Schritt halten müssten. Dies gelte insbesondere für den Bereich der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). *Voß* forderte auf der Nachrichtendienst-Konferenz des Behörden Spiegel in Berlin: "Wir benötigen Sicherheit durch und trotz Verschlüsselung."

BND nutzt integrierten Ansatz

Der Beigeordnete Nato-Generalsekretär, *Arndt Freiherr Freytag von Loringhoven*, wiederum zeigte sich davon überzeugt, dass es in Zukunft mithilfe Künstlicher Intelligenz (KI) möglich sein werde, militärische Ziele schneller, besser und genauer zu erfassen.

Der Bundesnachrichtendienst (BND) verfolge bei der Informationsbeschaffung einen integrierten Ansatz, der mehrere Elemente umfasse. Außerdem setze die Behörde bei der Bewertung von Quellen auf ein skaliertes System. Dadurch erhalte jede Quelle einen individuellen Wert hinsichtlich ihrer Glaubwürdigkeit im konkreten Fall, berichtete der für militärische Angelegenheiten zuständige BND-Vizepräsident, Generalmajor *Werner Sczesny*. Der integrierte Ansatz erlaube es, verschiedene Informationen miteinander zu verknüpfen und gegeneinander zu gewichten. Er gab jedoch auch zu bedenken, dass dieses Modell sowohl personell als auch technisch aufwendig sei. Immerhin würden dabei Elemente der Analyse von Informationen aus frei verfügbaren Quellen (OSINT), der Führung menschlicher Quellen (HUMINT), der Auswertung von Satellitenbildern (IMINT) sowie der Fernmeldeaufklärung (SIGINT) miteinander kombiniert. Gleichzeitig habe dieser Ansatz einen unschätzbaren Vorteil: Er erlaube die Erstellung aussagekräftiger Analysen, so *Sczesny*, der sich freute, dass der BND-Umzug von Pullach nach Berlin nach mehreren Jahren nunmehr abgeschlossen ist.

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), *Arne Schönbohm*, warnte davor, dass die neue Angriffsqualität im Cyber-Raum die Gefährdungslage auf ein neues Niveau hebe. Diese Entwicklung erfordere flexible Gegenmaßnahmen, da Attacken inzwischen nicht mehr nur auf die Soft-, sondern auch auf die Hardware erfolgten. Angesichts dessen meinte *Schönbohm*: "Cyber-Sicherheit ist Voraussetzung für die erfolgreiche Digitalisierung und eine gesamtgesellschaftliche Aufgabe, die nur durch zwischenbehördliche Zusammenarbeit erreicht werden kann." Diese Kooperation scheint verbesserungsbedürftig zu sein. Darauf lassen zumindest die Aussagen von *Christian Grusemann* von der Bechtle AG schließen. Er forderte, die Zeitspanne, in der Cyber-Angriffe auf Unternehmen in aller Regel entdeckt würden, deutlich zu verringern. Bisher betrage sie noch bis zu 200 Tage.

Andreas Könen, Leiter der Abteilung Cyber- und Informationssicherheit im Bundesinnenministerium (BMI), wiederum warnte: "Verbrechen findet heute digital statt. Die Angriffe und die Gefahren aus dem Cyber-Raum werden zunehmen." Aus diesem Grunde brauche es ein Cyber-Abwehrzentrum plus, in dem die Gesamtlage zur Cyber-Sicherheit abgebildet werden könnte. Schließlich machten Wissenschafts- und Technologiespionage bereits mehr als die Hälfte der Tätigkeit ausländischer Nachrichtendienste hierzulande aus, warnte *Prof. Dr. Helmut Müller-Enbergs*. Dabei setzten die Agenten auf verschiedene Strategien, so der Leiter der Spionageabwehr im Land Berlin und Mitverfasser des Behördengutachtens über Gregor Gysi im Jahre 1996 für den Immunitätsausschuss des Deutschen Bundestages. Zum einen infiltrierten sie IT-Systeme oder gründeten im Ausland eigene Unternehmen, um Teil der Lieferketten deutscher Firmen zu werden. Zum anderen übernähmen sie mithilfe von Strohmännern Unternehmen in der Bundesrepublik und versuchten dann, das Know-how abfließen zu lassen. Darüber hinaus seien Fälle bekannt, in denen Fachleute in Firmen eingeschleust wurden, um Daten zu stehlen, so *Müller-Enbergs*, der auch als Gutachter zur Staatssicherheit der ehemaligen DDR tätig war.

Gegen diesen Datenabfluss könne man sich allerdings schützen, erläuterte *Anton Kreuzer*. Sein Unternehmen setze dabei auf eine zunehmende Automatisierung. Denn: "Das höchste Sicherheitsrisiko ist der Mensch." Durch Machine Learning könnten Algorithmen Anomalien erkennen, Datenabflüsse stoppen und Geräte schützen, erklärte der CEO von DriveLock.

Einheitlichen Rechtsrahmen schaffen

Nicht zuletzt um gegen alle Formen der Spionage im Speziellen, aber auch gegen Bestrebungen gegen die freiheitlich-demokratische Grundordnung im Allgemeinen effektiver vorgehen zu können, bräuchten zumindest die Verfassungsschutzbehörden hierzulande einen einheitlichen Rechtsrahmen. Das verlangte der Vorsitzende des Parlamentarischen Kontrollgremiums (PKGr), *Armin Schuster* (CDU). Einen anderen Ansatz verfolgte *Dr. André Hahn*, PKGr-Mitglied für die Linksfraktion im Deutschen Bundestag. Er verlangte, dass die Nachrichtendienste die parlamentarische Kontrolle ihrer Arbeit als etwas Nützliches und Sinnvolles betrachten müssten. Und *Uli Grötsch* (SPD), Vertreter der Sozialdemokraten forderte eine Beobachtung der "Alternative für Deutschland" (AfD) durch den Verfassungsschutz. Eine solche Beobachtung sei ein "schmaler Grat" gab der Grünen-Bundestagsabgeordnete *Dr. Konstantin von Notz* zu bedenken.