

**Betreff: Stellungnahme zur Weiterentwicklung der modernen Sicherheitsarchitektur
(Polizei, Verfassungsschutz, Nachrichtendienste, Terrorismusbekämpfung),
Schwachstellenanalyse, Gefahrenabwehr und zukünftigen Sicherheitsgesetze**

Sehr geehrte Damen und Herren,

ich beschäftige mich eigenständig und intensiv mit den Möglichkeiten moderner Gefahrenabwehr sowie mit den **Grenzen und möglichen Schwachstellen bestehender Sicherheitsarchitekturen (Polizei, Verfassungsschutz, Nachrichtendienste, Terrorismusbekämpfung)**. Dabei analysiere ich Mechanismen von Tarnung, Täuschung und Aufklärung nicht nur aus der Perspektive von Sicherheitsbehörden, sondern stelle ihnen bewusst die Perspektive potenzieller Angreifer gegenüber.

Ein eigenständiger Bestandteil meiner Arbeit ist das analytische Konzept „Operation Sentinel“. Darunter verstehe ich eigene theoretische Tests und Belastungsprüfungen zukünftiger Gefahrenlagen sowie eine kritische Betrachtung der tatsächlichen Leistungsfähigkeit moderner Sicherheitsarchitekturen. Dabei untersuche ich auch das Zusammenspiel von Behörden, Gesellschaft, digitalen Infrastrukturen und technischen Systemen. Erkenntnisse aus früheren Sicherheitsanalysen und Tests fließen in diese Betrachtungen ein.

Aus meiner Sicht stellt die Modernisierung der Bundespolizei und der Polizeigesetze der Länder einen wichtigen Schritt dar. Biometrische Verfahren, künstliche Intelligenz, automatisierte Datenanalyse und moderne digitale Ermittlungsinstrumente können Sicherheitsbehörden dabei unterstützen, Gefahren früher zu erkennen und komplexe Kriminalitätsstrukturen besser zu analysieren. Auch Nachrichtendienste müssen technisch mit einer zunehmend digitalisierten Bedrohungslage Schritt halten.

Eine Modernisierung einzelner Instrumente wird jedoch aus meiner Sicht nicht ausreichen. Sicherheitsarchitekturen müssen als Gesamtsystem betrachtet und regelmäßig darauf geprüft werden, ob sie gegenüber neuen Formen von Terrorismus, organisierter und schwerer Kriminalität, Cyberangriffen und hybriden Bedrohungen tatsächlich belastbar sind.

Dazu gehört für mich auch die Frage nach einer rechtssicheren und verhältnismäßigen Speicherung beziehungsweise Zuordnung von IP-Adressen. Eine solche Maßnahme kann aus meiner Sicht ein wichtiges Ermittlungsinstrument sein, muss jedoch mit klaren gesetzlichen Voraussetzungen, Datenschutz, Zweckbindung, richterlicher Kontrolle und wirksamen rechtsstaatlichen Sicherungen verbunden werden.

Besonders wichtig ist dabei die Perspektive des sogenannten „Red Teaming“: Eine Sicherheitsmaßnahme sollte nicht nur danach bewertet werden, wie sie im vorgesehenen Idealfall funktioniert. Ebenso muss untersucht werden, wie Terroristen, schwerkriminelle Strukturen oder andere Angreifer versuchen könnten, ihre Schwachstellen zu erkennen oder auszunutzen.

Genau hier sehe ich eine wichtige Aufgabe unabhängiger Sicherheitsanalysen. Es geht nicht darum, Straftaten praktisch zu fördern oder konkrete Angriffe durchzuführen. Es geht darum, Schwachstellen gedanklich und kontrolliert sichtbar zu machen, bevor reale Täter sie entdecken.

Auch die analoge Welt darf dabei nicht außer Betracht bleiben. Moderne Gefahren entstehen nicht ausschließlich durch technische Angriffe. Menschen, soziale Strukturen, organisatorische Abhängigkeiten und alltägliche Abläufe können ebenfalls Teil komplexer Bedrohungslagen werden. Deshalb müssen moderne Sicherheitsarchitekturen sowohl die digitale als auch die analoge Dimension berücksichtigen.

Mein Ansatz lässt sich daher auf eine einfache Frage reduzieren:

Wie belastbar ist eine Sicherheitsarchitektur tatsächlich, wenn man sie nicht nur aus Sicht des Staates, sondern auch aus Sicht eines potenziellen Angreifers analysiert?

Die Realität zeigt aus meiner Sicht zunehmend, wie weit die Möglichkeiten von Terroristen, schwerkriminellen Strukturen und gewaltbereiten Akteuren bereits heute reichen können. Moderne Kommunikationstechnologien, frei verfügbare Informationen, digitale Infrastrukturen, soziale Strukturen und die gezielte Ausnutzung menschlicher und organisatorischer Schwachstellen können miteinander verbunden werden und dadurch Gefahrenlagen entstehen lassen, die nicht mehr ausschließlich mit klassischen Methoden bewältigt werden können.

Genau darin sehe ich eine besondere Herausforderung für den Staat und seine Sicherheitsbehörden: Sicherheitsstrukturen dürfen nicht erst dann angepasst werden, wenn ein Angreifer eine Schwachstelle bereits erkannt und ausgenutzt hat. Dann besteht die Gefahr, dass staatliche Stellen lediglich auf eine bereits eingetretene Entwicklung reagieren.

Im ungünstigsten Fall erhält der Staat damit nicht einmal die Möglichkeit, rechtzeitig zu reagieren. Ein potenzieller Angreifer kann sich einen Informations-, Zeit- oder Handlungsvorsprung verschaffen, während Behörden zunächst erkennen, bewerten und anschließend rechtlich, organisatorisch und technisch reagieren müssen.

Das bedeutet für mich nicht, dass Sicherheitsbehörden grundsätzlich handlungsunfähig sind. Es bedeutet vielmehr, dass moderne Gefahrenabwehr stärker vorausschauend arbeiten muss.

Genau hier setzt „Operation Sentinel“ an: Sicherheitsarchitekturen (Polizei, Verfassungsschutz, Nachrichtendienste, Terrorismusbekämpfung) sollen nicht nur darauf geprüft werden, ob sie gegen bekannte Bedrohungen funktionieren. Sie müssen auch darauf geprüft werden, was geschieht, wenn ein Angreifer neue Kombinationen aus technischen Möglichkeiten, menschlichen Faktoren, Informationsgewinnung und organisatorischen Schwachstellen nutzt.

Die entscheidende Frage lautet deshalb nicht nur:

„Kann der Staat auf einen Angriff reagieren?“

Sondern auch:

„Erkennt der Staat die Entwicklung früh genug, um überhaupt noch wirksam reagieren zu können?“

Aus meiner Sicht sollte diese Perspektive stärker in die Entwicklung zukünftiger Sicherheitsgesetze, technischer Systeme und behördenübergreifender Sicherheitskonzepte einfließen. Moderne Gefahrenabwehr muss der Entwicklung potenzieller Bedrohungen möglichst einen Schritt voraus sein – und darf nicht dauerhaft darauf angewiesen sein, erst aus dem nächsten realen Angriff zu lernen.

Dabei darf jedoch ein entscheidender Bestandteil moderner Gefahrenabwehr nicht aus dem Blick geraten: die Bevölkerung selbst.

Eine demokratische Sicherheitsarchitektur kann nicht ausschließlich darauf beruhen, dass staatliche Stellen der Bevölkerung vermitteln: „**Wir können euch schützen.**“ Eine solche Vorstellung greift aus meiner Sicht zu kurz. Kein Staat und keine Sicherheitsbehörde kann jede Gefahr erkennen, verhindern oder rechtzeitig abwehren. Die Bevölkerung ist deshalb nicht lediglich das Schutzobjekt staatlicher Sicherheitsmaßnahmen, sondern ein wesentlicher Bestandteil der Sicherheitsarchitektur und zugleich ein tragender Bestandteil der Demokratie. Menschen erleben Entwicklungen und Veränderungen häufig unmittelbar in ihrem Alltag. Sie können Auffälligkeiten wahrnehmen, Hinweise geben, Gefahren melden und damit einen wichtigen Beitrag zur frühzeitigen Erkennung von Risiken leisten.

Dafür braucht es jedoch Vertrauen zwischen Staat und Bevölkerung. Dieses Vertrauen entsteht aus meiner Sicht nicht durch das Versprechen vollständiger Sicherheit, sondern durch **Ehrlichkeit über Möglichkeiten, Grenzen und bestehende Schwachstellen staatlicher Gefahrenabwehr.**

Der Staat sollte deshalb nicht den Eindruck vermitteln, jede Gefahr jederzeit kontrollieren zu können. Eine glaubwürdige Sicherheitsarchitektur muss auch offen benennen können, wo ihre Grenzen liegen, welche Risiken bestehen und an welchen Stellen sie weiterentwickelt werden muss.

Ehrlichkeit währt hier am längsten.

Für mich bedeutet moderne Gefahrenabwehr deshalb nicht nur mehr technische Möglichkeiten, mehr Daten oder neue gesetzliche Befugnisse. Sie bedeutet auch eine ehrliche Partnerschaft zwischen Staat und Bevölkerung, in der beide Seiten wissen, dass Sicherheit eine gemeinsame gesellschaftliche Aufgabe ist.

Genau darin sehe ich einen wesentlichen Bestandteil zukünftiger Sicherheitsarchitekturen: **Staat und Bevölkerung sollten gemeinsam dazu beitragen, moderne Gefahrenabwehr und Strafverfolgung weiterzuentwickeln und zukunftsfähig aufzubauen.** Dabei braucht es Ehrlichkeit über bestehende Möglichkeiten, Grenzen und Schwachstellen. Denn nur wenn Probleme offen benannt werden, können Sicherheitsstrukturen weiterentwickelt und neue Lösungen geschaffen werden.

Aus meiner Sicht wird eine zukunftsfähige Sicherheitsarchitektur deshalb langfristig nicht darauf verzichten können, moderne technische Möglichkeiten konsequent weiterzuentwickeln und unter klaren rechtsstaatlichen Voraussetzungen nutzbar zu machen. Dazu gehören für mich insbesondere **biometrische Verfahren, künstliche Intelligenz, automatisierte Datenanalyse, moderne digitale Ermittlungsinstrumente sowie die rechtssichere Speicherung beziehungsweise Zuordnung von IP-Adressen und anderen relevanten digitalen Spuren.**

Diese Instrumente sollten dabei nicht isoliert betrachtet werden. Entscheidend ist für mich, dass sie in eine Sicherheitsarchitektur eingebettet werden, die technische Leistungsfähigkeit mit rechtsstaatlichen Grenzen, transparenter Kontrolle und dem Vertrauen der Bevölkerung verbindet. Nur so kann moderne Gefahrenabwehr nicht lediglich auf neue Bedrohungen reagieren, sondern sich gemeinsam mit Gesellschaft, Technik und Rechtsstaat vorausschauend weiterentwickeln.

Mit freundlichen Grüßen

Christian Dauck

Seite 3 von 3