Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 E

Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer BDSV e.V., Berlin

Stellungnahme für die Anhörung des Innenausschusses des Deutschen Bundestages zum Projekt „VeRA“ am 22.04.2024

Für die beteiligten Mitglieder des Bundesverbandes der Deutschen Sicherheits- und Verteidigungsindustrie e.V. Berlin, nehme ich wie folgt Stellung:

I. Vorbemerkung

1. Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV) umfasst derzeit 218 Mitgliedsunternehmen, denen gemeinsam ist, dass sie Ausrüster staatlicher Sicherheitsorganisationen sind, sei es von Streitkräften oder von Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Unsere Mitgliedsunternehmen erfüllen darüber hinaus die satzungsmäßige Anforderung, wonach sie über sicherheits- oder verteidigungsindustrielle bzw. damit zusammenhängende digitale Wertschöpfung in Deutschland verfügen müssen. Ausländische Unternehmen oder solche mit ihrem Hauptsitz im Ausland können ebenfalls Mitgliedsunternehmen des BDSV sein, sofern sie die o.g. Wertschöpfungsvoraussetzung erfüllen. Die Fa. Palantir war bis zum 31.12.2023 Mitglied des BDSV, ist jedoch aus bei uns nicht bekannten Gründen per Jahresende 2023 aus dem BDSV ausgetreten, so dass wir bezogen auf die Fa. Palantir keiner Interessenbindung unterliegen.

2. Der BDSV kann an dieser Stelle auch deshalb umso überzeugender als Interessenvertretung deutscher digitaler Kompetenzen auftreten, weil es aus unserer Sicht ein klares Ziel der Bundesregierung sein muss, gemeinsam mit der darauf spezialisierten Industrie gerade unter den gegenwärtigen geopolitischen Rahmenbedingungen die technologische Souveränität in wesentlichen Bereichen der staatlichen Sicherheit zu gewährleisten. Dies gilt für alle einschlägigen Bereiche von der Aufbereitung, Speicherung und hochsicheren Übertragung von Daten bis hin zur Analyse großer und kleiner Datenmengen in strukturierter und unstrukturierter Form und aller Formate, angereichert durch modernste Verfahren aus den Bereichen Kryptologie, Künstlicher Intelligenz etc. In diesem Zusammenhang sei daran erinnert, dass gerade die deutschen industriellen Kompetenzen im Bereich Kryptologie und sicherheitsbezogener Künstlicher Intelligenz zu den sog. „Schlüssel-technologien“ gehören, die das von der Bundesregierung am 12.02.2020 verabschiedete „Strategiepapier zur Stärkung der Sicherheits- und Verteidigungsindustrie“ als nationale Souveränitätstechnologien im Sinne von Art 346 AEUV eingestuft hat. Auch dieses Strategiepapier gebietet eine nationale Vergabe von Aufträgen, wenn diese die Beschaffung entsprechender Schlüsseltechnologien für unsere staatlichen Sicherheitsorgane beinhalten. Die derzeit laufende Aktualisierung dieses Strategiepapiers durch die Ressorts BMWK, BMVg und BMI wird im Zweifel sogar noch zu einer Verstärkung der nationalen Bedeutung von Schlüsseltechnologien führen, weil dies wiederum der geopolitischen Lage und den entsprechenden Ableitungen aus der Nationalen Sicherheitsstrategie geschuldet ist. Würde man entgegen diesen strategischen „Pflöcken“ die bestehenden deutschen Kompetenzen in wesentlichen

Bereichen der digitalen Souveränität nicht honorieren, sondern sich stattdessen US-amerikanischen Herstellern anzuvertrauen, wäre dies als geradezu „strategievergessen“ einzustufen.

3. Dies gilt umso mehr, als in Deutschland die Kompetenzen für eine nationale, den Interessen digitaler und technologischer Souveränität genügende Lösung auf Seiten der von uns vertretenen Industrie eindeutig bestehen.

II. Randbedingungen und Gründe für eine nationale Lösung zur Datenanalyse

1. Es gibt nationale Lösungen, welche für andere Bereiche bereits unter Vertrag sind oder zumindest als Projektskizze existieren. Im Verhältnis zu den langlaufenden und wesentlich teureren Projekten der Fa. Palantir ist der vorgeschobene Grund der „Preis-Realisierungszeit“ kein tragfähiges Argument, sondern vielmehr ein weiteres und von Palantir seit Jahren im europäischen Markt vehement platziertes „Verkaufskonzept“.

2. Da – wie bereits erwähnt - die vorliegende Stellungnahme nicht die wettbewerblichen Interessen der Fa. Palantir berücksichtigen muss, können insoweit die Fakten in Bezug auf das Palantir-Produkt „Gotham“ klar benannt werden: „Gotham“ ist eben keine sogenannte „plug-and-play-Solution, also ein Produkt, das unmittelbar nach Kauf vollumfänglich technologisch, datenschutz- und prozesskonform sowie kundenspezifisch passend zur Verfügung steht. Bei allen Projekten der Fa. Palantir in Deutschland (siehe Bundesländer NRW, Hessen, Bayern) handelt es sich um langjährig laufende Entwicklungs- und Anpassungsprojekte, die bereits in der „Bauphase“ durch erhebliche Preissteigerungen gekennzeichnet sind. Hierzu können durch eine simple Internetrecherche („Palantir Kosten“) umfangreiche Informationen gesichtet werden. Insbesondere das Land NRW mit dem dortigen Palantir-Projekt „DAR“ ist ein Beispiel für ein typisches, kostenintensives und intransparent geführtes mehrjähriges Einführungsprojekt. Die fehlenden polizeirechtlichen und datenschutzrechtlichen Anspruchsgrundlagen bilden eine weitere Problematik. Hierzu ist auf die einschlägigen und hinlänglich bekannten Verfassungs-beschwerden zu verweisen. Das Argument, dass mit der Palantir-Lösung „Gotham“ eine sofort einsatzfähige Software zur Verfügung stehen würde, ist demnach eher ein Marketing- und Verkaufsargument und entspricht nicht den Realitäten in den langjährigen Projekten der drei vorgenannten Bundesländer. In Bayern ist man auch Jahre nach der Anschaffung von „VeRA“ noch in der Entwicklungs- und Testphase. Während dieser Phase wurden jedoch jährlich fünf Millionen Euro für nicht im Einsatz befindliche Lizenzen an die Fa. Palantir gezahlt. International ist dies ebenfalls der Fall. Unter anderem aus diesem Grund wurde die Palantir-Lösung bei EUROPOL, aber auch bei vielen weiteren internationale Behörden, wieder gekündigt. Frankreich hat sich vor einigen Monaten komplett von Palantir losgesagt und setzt auf nationale Lösungen.

3. Die wesentlichen Gründe dafür, nochmals Zeit und Geld in einem überschaubaren Rahmen aufzuwenden, um eine nachhaltig tragfähige industrielle und zugleich nationale Umsetzungsmöglichkeit für das Projekt „VeRA“ auf Bundesebene zu schaffen, liegen aus unserer Sicht in folgenden Aspekten:

a) Nationale Lösungen mit einem offenen Plattformansatz, auf Basis von Standardtechnologien, erlauben eine besondere Flexibilität und können je nach Bedarf und Herausforderung angepasst, ergänzt und/oder erweitert werden. Damit können sowohl Behörden im Bereich der Polizeien als auch im Gesamtsystem des militärischen Nachrichtenwesens angesprochen werden; es können dort untereinander fachliche sowie wirtschaftliche Synergieeffekte erzielt werden. Eine Service-Schicht erlaubt die Anbindung der verschiedensten Quellen und Tools, eingebettet in eine hoch-sichere Infrastruktur. Eine Plattform erlaubt auch anderen nationalen Partnern und Unternehmen sowie staatlichen Organisationen weitere Datenquellen und Analysemodule anzubinden und zu integrieren.

b) Es muss im deutschen Interesse liegen, nicht sowohl auf der Länder- wie auch der Bundesebene von einem einzigen Monopolisten Palantir abhängig zu sein. Zwar könnte aus funktionalen Gründen ein Interesse an einer einheitlichen Bund- und Länder-übergreifenden Lösung bestehen; dem müssen allerdings die beim „single sourcing“ üblicherweise anzutreffenden Risiken und Abhängigkeiten gegenübergestellt werden (Kostenrisiken, Risiken des Scheiterns, Risiko einer allmählichen konzeptionellen Abhängigkeit etc.). Hierbei ist auch zu berücksichtigen, dass ein nationaler Anbieter den Transparenzregeln des deutschen öffentlichen Preisrechts unterliegt, während Palantir dies nicht automatisch, sondern nur im Fall einer ausdrücklichen Unterwerfung und Übernahme der Preisrechtsgrundsätze tut. Falls Palantir in Deutschland einen Monopol-Status erreichen würde, wäre Preiserhöhungen Tür und Tor geöffnet.

c) Ein entscheidender Vorteil einer nationalen Lösung besteht in der gesicherten Kontrolle über den Datenfluss (analog zu Frankreich). Es muss ausgeschlossen sein, dass Daten auf Servern in den USA gespeichert werden, d.h. gerade in einem möglichen Krisenfall ein komplett souveräner, unter alleiniger Kontrolle der deutschen Behörden stattfindender Datenzugriff nicht sichergestellt sein mag. Dies wäre im Fall der Beauftragung deutscher Unternehmen anders.

d) Wie aus öffentlich verfügbaren BT-Dokumenten (z.B. Drucksache 20/8390 v. 18.09.2023) hervorzugeht, scheint das Bundesministerium des Innern derzeit für die Umsetzung des Projektes „VeRA“ auf Bundesebene eine behördliche Eigenentwicklung zu präferieren. Solche Eigenentwicklungen sind jedoch zumeist mit Risiken im Bereich der inhaltlichen Umsetzung und der aufzuwendenden Kosten belastet. Daher bietet sich demgegenüber ein privatwirtschaftlich getragener, gleichwohl aber strikt nationaler Ansatz an, um sowohl das Kosten- und Implementierungsrisiko unter Kontrolle zu halten, gleichzeitig aber auch den nationalen Schutzinteressen in vollem Umfang Rechnung zu tragen. Wie langjährige Erfahrungen mit ähnlichen Projekten erwiesen haben, können hoheitliche Souveränitätserfordernisse auch dann gewahrt werden, wenn private Unternehmen an der Projekt-Implementierung beteiligt sind, sofern sie sich dabei entsprechend strengen Geheimschutzanforderungen unterwerfen.

e) Schließlich sei nochmals auf den schon zuvor erwähnten Aspekt des „Strategiepapiers zur Stärkung der Sicherheits- und Verteidigungsindustrie“ vom 12.02.2022 verwiesen (Fundstelle: https://www.bmwk.de/Redaktion/DE/ Downloads/S-T/strategiepapier-

staerkung-sicherits-und-verteidigungsindustrie. pdf?__blob =publicationFile&v=4). In diesem Papier, welches sich im Gefolge der Nationalen Sicherheitsstrategie vom Juni 2023 und der veränderten geopolitischen Herausforderungen aktuell zwischen den zuständigen Ressorts der Bundesregierung in der Überarbeitung befindet, werden die nationalen Technologie-Kompetenzen in den Bereichen Krypto und Künstliche Intelligenz ausdrücklich als nationale Schlüsseltechnologien eingestuft. Dort heißt es: „Die Verfügbarkeit der identifizierten sicherheits- und verteidigungsindustriellen Schlüsseltechnologien ist aus wesentlichem nationalem Sicherheitsinteresse zu gewährleisten." Um dies auch im deutschen Vergaberecht zu konkretisieren, hat die Bundesregierung mittels § 107 Abs. 2 GWB deutlich gemacht, dass „sicherheits- und verteidigungsindustrielle Schlüsseltechnologien" im Fall von Beschaffungen durch die nationalen Sicherheitsbehörden als Fall der Betroffenheit wesentlicher Sicherheitsinteressen nach Artikel 346 AEUV behandelt werden sollen. Dem sollte sich auch das BMI sowie die in der Beauftragung verantwortlichen Bundesländer im Fall „VeRA" verpflichtet fühlen.

III. Fazit der vorliegenden Stellungnahme:

Der BDSV plädiert mit Blick auf die Bearbeitung des Projektes „VeRA" auf Bundesebene für eine stringent nationale Lösung, allerdings nicht auf der Grundlage einer behördlichen Eigenentwicklung, sondern auf der Basis einer nationalen Analyseplattform. nationaler, privater Anbieter mit entsprechendem Track-Record.

Sehr geehrte Ausschuss-Mitglieder, nationale Souveränität bedeutet nicht, alles selbst machen zu müssen, aber es bedeutet, im Zweifel alles selbst machen zu können. Beim Thema Analyseplattform stehen wir gerade an einer Wegscheide, und die Entscheidungen (oder Nicht-Entscheidungen) von heute bestimmen darüber, ob wir morgen souverän handeln können. Bitte setzen Sie sich in diesem Sinne für eine deutsche Lösung ein, und zwar gerade in Zeiten, in denen wir mit Sorge auf eine nächste Präsidentschaft Trumps in den USA blicken.