



Bericht

# Palantir Technologies Inc.

Fokusthema

Operative Einsatzbereitschaft in Echtzeit kontrollieren und optimieren mit  
Palantir Asset Readiness

Bern, 4. Dezember 2024

**Schweizer Armee**



## Inhaltsverzeichnis

<b>1</b>	<b>Zusammenfassung.....</b>	<b>3</b>
<b>2</b>	<b>Einleitung.....</b>	<b>5</b>
<b>3</b>	<b>Unternehmen Palantir Technologies Inc. ....</b>	<b>6</b>
3.1	Gründung .....	6
3.2	Entwicklung .....	6
<b>4</b>	<b>Kernprodukte und Lösungen .....</b>	<b>7</b>
4.1	Palantir Gotham .....	7
4.2	Palantir Foundry .....	8
4.3	Artificial Intelligence Platform (AIP) .....	8
4.4	Palantir TITAN.....	9
4.5	Palantir Readiness Solution Suite .....	9
4.5.1	Modul Asset Readiness .....	9
4.5.2	Modul Personnel Readiness .....	9
4.5.3	Modul Financial Readiness .....	10
4.5.4	Zusammenfassung .....	10
4.6	Gebrauch in Europa .....	10
4.6.1	Nutzung durch Streitkräfte .....	10
4.6.2	Nutzung durch die Polizei .....	11
4.6.3	Nutzung in der Schweiz .....	11
<b>5</b>	<b>Fokusthema: Operative Einsatzbereitschaft mit Asset Readiness .....</b>	<b>11</b>
5.1	Fallstudie U.S. Army.....	12
5.1.1	Lösung mit Palantir for Readiness Solution Suite.....	12
5.1.2	Auszug einzelner Ergebnisse .....	13
5.2	Daten als Voraussetzung .....	13
5.3	Details zum Modul Asset Readiness .....	14
5.3.1	Kern der Lösung .....	14
5.3.2	Digital Twin der Ressourcen und Arbeitsabläufe .....	15
5.3.3	Verschiedene 360-Grad-Ansichten .....	16
5.3.4	Analysis, Reporting and Operational Decisions.....	17
5.4	Nutzen des Moduls Asset Readiness .....	17
5.5	Kostenschätzungen.....	18
<b>6</b>	<b>Herausforderungen .....</b>	<b>19</b>
6.1	Risiken wie Datenhoheit, Souveränitätsverlust und Abhängigkeiten .....	19
6.2	Datenschutz und ethische Aspekte .....	20
6.3	Strengere technische und rechtliche Regelungen .....	20
6.4	Transparenz und Verantwortung .....	20
<b>7</b>	<b>Empfehlungen .....</b>	<b>21</b>
7.1	Überprüfung von Alternativen .....	21
7.2	Intensivierung von Kooperationen .....	21
7.3	Beantwortung zentraler Fragen .....	21

## 1 Zusammenfassung

### *Gründung und Entwicklung*

Palantir Technologies Inc. wurde 2003 von Alex Karp, Peter Thiel und weiteren Partnern gegründet und ging 2020 an die Börse. Ursprünglich auf Regierungsbehörden und den Sicherheitssektor fokussiert, hat Palantir sein Angebot mit der Plattform Foundry auf kommerzielle Kunden erweitert. 2023 erzielte das Unternehmen erstmals einen operativen Gewinn. Die starke Nachfrage nach KI-gestützten Lösungen, wie der Artificial Intelligence Platform (AIP), führte 2024 zu einem Umsatzanstieg um 30% auf 725,5 Mio USD und einem Nettogewinn von 144 Mio USD. Mit einer Marktkapitalisierung von fast 100 Mrd USD zählt Palantir zu den grössten Softwareunternehmen, obwohl Analysten die Bewertung als hoch einschätzen.

### *Kernprodukte und Lösungen*

Palantir bietet eine Reihe hochspezialisierter Softwarelösungen an, die entwickelt wurden, um Echtzeitanalysen, datenbasierte Entscheidungsfindungen, strategische Planungen sowie die Optimierung der Einsatzbereitschaft von Ressourcen zu unterstützen.

- *Palantir Gotham*: Entwickelt für militärische und nachrichtendienstliche Anwendungen, integriert diese Plattform Daten aus verschiedenen Quellen, analysiert sie in Echtzeit und liefert umsetzbare Erkenntnisse. Funktionen wie Geospatial Intelligence, Risikobewertung und visuelle Analysen machen Gotham zur zentralen Lösung für die Aufklärung und Überwachung.
- *Palantir Foundry*: Diese Plattform dient der Optimierung von operativen Abläufen in Unternehmen und Organisationen. Sie kombiniert Daten aus diversen Quellen, bereinigt und analysiert sie in Echtzeit und unterstützt so fundierte Entscheidungen in Bereichen wie z B der Logistik.
- *Artificial Intelligence Platform (AIP)*: Diese Plattform nutzt maschinelles Lernen und KI, um Muster zu erkennen, Risiken vorherzusagen und Entscheidungsprozesse zu automatisieren. Sie ist besonders wertvoll für Organisationen, die grosse Datenmengen in Echtzeit analysieren müssen.
- *Readiness Solution Suite*: Diese Suite umfasst mehrere Module zur Optimierung der Einsatzbereitschaft militärischer Ressourcen. Dazu gehören *Asset Readiness* (für die Einsatzbereitschaft der Ausrüstung), *Personnel Readiness* (für die Einsatzbereitschaft von Personal) und *Financial Readiness* (zur finanziellen Planung und Ressourcenzuweisung).

### *Fokusthema: Operative Einsatzbereitschaft mit Asset Readiness*

Das Modul *Asset Readiness* bietet Unternehmen und Organisationen eine umfassende Lösung, um ihre Ressourcen und Ausrüstung effizient zu verwalten und deren Einsatzbereitschaft zu maximieren. Die Plattform vereint leistungsstarke Datenintegration, Echtzeitüberwachung und intelligente Analysen, um betriebliche Abläufe zu optimieren und fundierte Entscheidungen zu ermöglichen. Fragmentierte Datenquellen werden in einer zentralen Plattform zusammengeführt, die zuverlässige und nachvollziehbare Informationen bereitstellt. Dabei gehören zu den Kernfunktionen die Erstellung eines digitalen Zwillings (Digital Twin), der ein ganzheitliches Abbild aller Ressourcen und Prozesse liefern. Mit 360°-Ansichten erhalten Nutzer detaillierte Einblicke in den Zustand, die Nutzung und die Wartungshistorie einzelner Komponenten, Geräte oder ganzer Flotten. Automatisierte Berichte und interaktive Analysen unterstützen bei der Planung und Umsetzung von Wartungen, der Ressourcenzuweisung und der Vorhersage von Engpässen.

Die Kosten für die Softwarelösungen variieren stark. Die einmaligen Kosten umfassen die Implementierung, Anpassung und Datenmigration, die je nach Projekt mehrere Millionen € betragen können. Wiederkehrende Kosten beinhalten Lizenzgebühren und Wartungsaufwand, oft gestaffelt nach Nutzerzahl und Funktionalität. Die Polizei Nordrhein-Westfalen zahlte zum Beispiel 22 Mio € für eine fünfjährige Lizenzfrist, zusätzlich 660 000 bis 1,1 Mio € jährlich für

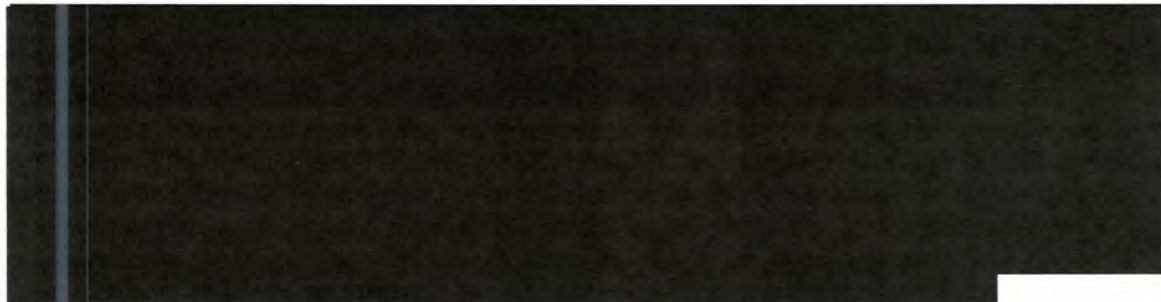


Wartung und Support. Insgesamt können Projekte aufgrund hoher Sicherheitsanforderungen und Datenqualität deutlich teurer werden als geplant.

Trotz der Vorteile gibt es auch Herausforderungen. Palantir *Asset Readiness* ist stark auf die Verfügbarkeit qualitativ hochwertiger Echtzeitdaten angewiesen, deren Bereitstellung problematisch sein kann, wenn z B die für die Datenübertragung erforderlichen Kommunikationssysteme nicht verfügbar sind oder Risiken durch SIGINT-Bedrohung (Signals Intelligence) im Einsatzgebiet bestehen. Um den Zustand und die Verfügbarkeit von Ressourcen zu überwachen, sind zudem Sensoren und IoT-Geräte<sup>1</sup> notwendig. Zudem gibt es strategische Herausforderungen, wie die Abhängigkeit von einem US-amerikanischen Anbieter, die potenziell den Verlust der Datenhoheit und der nationalen Souveränität zur Folge haben kann. Das Datenschutzgesetz und ethische Aspekte verstärken diese Problematik, da umfassende Datensammlungen und deren Analyse möglicherweise in die Privatsphäre eingreifen und damit rechtliche und ethische Fragen aufwerfen.

### *Empfehlung*

Die Schweizer Armee sollte Alternativen zu Palantir in Betracht ziehen. Es gibt europäische Unternehmen, die vergleichbare Lösungen anbieten und mit den Datenschutz- und Sicherheitsanforderungen besser vertraut sind.<sup>2</sup> Die Prüfung von Open-Source-Optionen oder die Entwicklung und Integration eigener Datenanalyseplattformen könnten Wege sein, um die Kontrolle über kritische Systeme zu behalten und Abhängigkeiten zu reduzieren. Die Entwicklung sollte dabei nicht im Alleingang, sondern mit Kooperationspartnern erfolgen, die offen, vertrauenswürdig, integer und souverän erscheinen, um eine sichere, nachhaltige und produktive Zusammenarbeit zu gewährleisten.



In diesem Kontext sind unter anderem folgende zentrale Fragen zu klären: Wie wird die technologische Unabhängigkeit der Armee gewährleistet, und wie lässt sich der Schutz sensibler Daten garantieren? Welche Alternativen zu externen Anbietern stärken die Souveränität und minimieren Risiken? Zugleich müssen die ethische und rechtliche Vereinbarkeit externer Lösungen sowie ihr langfristiges Kosten-Nutzen-Verhältnis bewertet werden. Schliesslich sind geopolitische Risiken und strategische Abhängigkeiten in internationalen Kooperationen kritisch zu analysieren, um eine nachhaltige und unabhängige Strategie zu entwickeln.

*Aus den genannten Gründen empfehlen die Gutachter, auf Lösungen des Unternehmens Palantir Technologies Incorporated zu verzichten. Die Thematik der operativen Einsatzbereitschaft wird 2025 im Rahmen der spezifischen KI-Strategie der Armee durch die Armeepanung behandelt.*

<sup>1</sup> Internet of Things (IoT), im militärischen Kontext auch bekannt als Internet of Military Things (IoMT), bezeichnet ein Netzwerk von physischen Objekten, die über das Internet oder einem militärischen Netz miteinander verbunden sind. Diese Objekte können Daten sammeln, austauschen und oft auch automatisiert handeln.

<sup>2</sup> z B SAP Defense & Security oder Accenture (BGÖ, Art 7, Abs 1, Bst f).

## 2 Einleitung

Eine Schweizer Delegation mit dem Staatssekretär für Sicherheitspolitik, Markus Mäder (Delegationsleiter), dem Chef der Armee, Korpskommandant Thomas Süssli, sowie dem Schweizer Botschafter in Singapur, Frank Grütter, haben vom 31. Mai bis zum 02. Juni 2024 am 21st IISS Shangri-La Dialog (SLD) von Singapur teilgenommen.

Im Rahmen dieses Anlasses wurde die Delegation von einem Vertreter der Palantir Technologies, Louis Mosley, angesprochen. Mosley ist Executive Vice President für Grossbritannien und Europa bei Palantir Technologies. Er leitet die Geschäfte von Palantir in Grossbritannien und Irland, einschliesslich der Zusammenarbeit mit der britischen Regierung.

Unter seiner Führung hat Palantir mehrere Projekte in Europa durchgeführt, darunter die Unterstützung der britischen Regierung bei der Bewältigung der COVID-19-Pandemie und die Zusammenarbeit mit dem National Health Service (NHS) zur Verbesserung der Datenintegration im Gesundheitswesen. In einem Interview betonte Mosley zudem die Rolle von Palantir in der Ukraine, wo das Unternehmen Technologien bereitstellt, die der ukrainischen Regierung bei der Verteidigung und beim Wiederaufbau des Landes helfen ([Bloomberg](#)).

Im Shangri-La unterhielt sich Mosley mit der Schweizer Delegation über das Interesse der Schweizer Armee an Lösungen, um Algorithmen oder KI auf Daten anwenden zu können. Er erklärte, dass Palantir bereit wäre, eine Demonstration der bestehenden Möglichkeiten durchzuführen, und erwähnte insbesondere eine Anwendung zur «Messung der Verfügbarkeit von militärischen Verbänden», die im Kontext der Gesamtverteidigung nützlich ist. (BGÖ, Art 7, Abs 1, Bst c und d).

### Auftrag

**«Evaluer l'intérêt de la solution de mesure de la disponibilité opérationnelle proposée par Palantir Technologies.»**

Mit der Betrachtung der «Operativen Einsatzbereitschaft» bildet die *Palantir for Readiness Solution Suite* mit dem Modul *Asset Readiness* das Fokusthema im Bericht. Er geht dabei nicht ausschliesslich auf dieses Modul ein, sondern auch auf das Unternehmen, die Hauptplattformen mit ihren jeweiligen Herausforderungen und auf die öffentliche Wahrnehmung. Zudem gibt der Bericht eine Empfehlung für das weitere Vorgehen ab.



### 3 Unternehmen Palantir Technologies Inc.

#### 3.1 Gründung

Palantir<sup>3</sup> Technologies Inc. ist ein US-amerikanisches Softwareunternehmen, das 2003 von Alex Karp, Peter Thiel sowie weiteren Partnern gegründet wurde und am 30. September 2020 an die Börse ging. Im Porträt der New York Times wird Alex Karp, CEO und Mitbegründer von Palantir Technologies, als schillernde und kontroverse Figur beschrieben. Karp ist bekannt für seine kritische Haltung gegenüber dem Silicon Valley und betont häufig die Bedeutung von Datenschutz und Privatsphäre. Diese Haltung steht jedoch im Widerspruch zur Nutzung von Palantir-Technologien, die selbst zur Überwachung eingesetzt werden und teils tief in die Privatsphäre der Bürgerinnen und Bürger eingreifen. Karp anerkennt die ethischen Bedenken, hat jedoch mehrfach klargestellt, dass ihm der Schaden an «Feinden der USA» durch Palantir-Software keine moralischen Probleme bereitet. Diese Haltung wirft Fragen nach den moralischen Grenzen der Datennutzung und Überwachung in sicherheitspolitischen Konflikten auf (Berliner Zeitung).

Eine zentrale Rolle bei der strategischen und ethischen Ausrichtung von Palantir spielt auch Peter Thiel, Mitbegründer und deutsch-amerikanischer Unternehmer und Investor. Thiel ist bekannt als Unterstützer konservativer Politiker wie Donald Trump. Er plädiert für weniger staatliche Eingriffe und mehr individuelle Freiheit, was ihm vielfach Kritik eingebracht hat (businessinsider.de). Seine Ansichten zur Demokratie, die er als unvereinbar mit absoluter Freiheit sieht, sowie seine Anlehnung an den umstrittenen Staatsrechtler Carl Schmitt, der autoritäre Strukturen befürwortet, haben ebenfalls Kontroversen ausgelöst (taz.de).

Mit Karp und Thiel stehen zwei gegensätzliche Persönlichkeiten an der Spitze des Unternehmens: Karp tritt als visionärer und idealistischer CEO auf, dem prowestliche Werte und eine technologische Verteidigung der USA wichtig erscheinen, während Thiel eine individualistische Linie vertritt, die gegen staatliche Intervention und für konservative Ideologien steht. Beide teilen jedoch das Ziel, den Westen durch technologische Überlegenheit zu stärken. Palantir sehen sie als zentralen Akteur im globalen Sicherheitsgefüge. Das Unternehmen arbeitet eng mit US-Geheimdiensten zusammen und stellt Technologien zur Verfügung, die westliche Interessen und Werte verteidigen sollen, auch wenn dies umfassende Überwachungsmaßnahmen und militärische Massnahmen bedeutet.


Für Thiel und Karp steht fest, dass Palantirs Technologien sowohl die nationale Sicherheit der USA als auch die strategischen Interessen ihrer Verbündeten unterstützen sollen. Das bedeutet, dass Palantir explizit keine Geschäfte mit Ländern macht, die den USA feindlich gesinnt sind, wie Russland oder China. Trotz unterschiedlicher politischer Präferenzen sind sich Thiel und Karp einig, dass der Westen durch technologische Überlegenheit und eine entschlossene Haltung gegenüber potenziellen Bedrohungen gestärkt werden muss (Das Erste).

#### 3.2 Entwicklung

Palantir Technologies hat seit seiner Gründung im Jahr 2003 eine beachtenswerte Entwicklung durchlaufen. Anfangs konzentrierte sich das Unternehmen auf die Bereitstellung von Datenanalyse-Software für Regierungsbehörden, insbesondere im Sicherheits- und Verteidigungssektor. Mit der Einführung der Plattform Foundry erweiterte Palantir sein Angebot auf kommerzielle Kunden, wie z. B. Banken und Organisationen im Gesundheitswesen, und erzielte dabei signifikante Erfolge (Börse Online).

Im Jahr 2023 verzeichnete Palantir erstmals einen operativen Gewinn, was das Vertrauen der Aktionäre stärkte und zu einem Anstieg des Aktienkurses führte. Die Nachfrage nach den KI-gestützten Lösungen des Unternehmens, insbesondere der Artificial Intelligence Platform (AIP), trug massgeblich zu diesem Erfolg bei (Time). Im dritten Quartal 2024 übertraf Palantir

<sup>3</sup> Der Firmenname Palantir stammt von der Bezeichnung Palantiri, die sehenden Steine, in J. R. R. Tolkiens Fantasy-Saga «Herr der Ringe».



die Erwartungen mit einem Umsatz von 725,5 Millionen US-Dollar, was einem Anstieg von 30 % im Vergleich zum Vorjahr entspricht. Der Nettogewinn verdoppelte sich auf 144 Millionen US-Dollar. Diese Ergebnisse wurden durch eine starke Nachfrage nach KI-Tools sowohl im US-amerikanischen Handelssektor als auch im Regierungssektor angetrieben (Financial Times). Die Marktkapitalisierung des Unternehmens nähert sich 100 Milliarden US-Dollar, was Palantir zu einem der grössten Softwareunternehmen weltweit macht (MarketWatch). Trotz dieser beeindruckenden Leistungen bleiben einige Analysten vorsichtig und weisen auf die hohe Bewertung des Unternehmens hin (InvestmentWeek).

## 4 Kernprodukte und Lösungen

Palantir bietet eine Reihe hochspezialisierter Softwarelösungen an, die entwickelt wurden, um Echtzeitanalysen, datenbasierte Entscheidungsfindungen, strategische Planungen sowie die Optimierung der Einsatzbereitschaft von Ressourcen zu unterstützen. Vier Plattformen bilden dabei die Kernprodukte.

### 4.1 Palantir Gotham

Palantir Gotham<sup>4</sup> ist die wichtigste Plattform des Unternehmens. Sie ist darauf ausgelegt, sehr grosse Datenmengen, die aus unterschiedlichen Quellen stammen, zu integrieren, zu verarbeiten und in umsetzbare Erkenntnisse umzuwandeln. Gotham wird von militärischen und nachrichtendienstlichen Organisationen aber auch von Sicherheitsbehörden wie z B der Polizei eingesetzt und bietet eine leistungsstarke Lösung zur Aufklärung und Überwachung. Die wichtigsten Funktionen dabei sind:

- *Datenintegration:* Gotham ermöglicht es, Daten aus verschiedenen Quellen, wie z B Drohnen, Satelliten, nachrichtendienstlichen Berichten und sozialen Medien, zu kombinieren. Die Plattform verarbeitet diese heterogenen Datenströme in Echtzeit und erstellt ein kohärentes Gesamtbild.
- *Visuelle und räumliche Analyse:* Die Plattform stellt Verbindungen zwischen verschiedenen Datenpunkten visuell dar, was es Analysten und Entscheidungsträgern ermöglicht, schnell Muster und Beziehungen zu erkennen. Zum Beispiel können Netzwerke von Akteuren visualisiert und geografische Bewegungen verfolgt werden.
- *Erweiterte Such- und Abfragefunktionen:* Gotham bietet leistungsstarke Suchwerkzeuge, die es Nutzern ermöglichen, spezifische Informationen in grossen Datenmengen zu finden. Diese Suchanfragen können fein abgestimmt und gefiltert werden, um die Daten gezielt nach relevanten Kriterien zu durchsuchen.
- *Risikobewertung und Bedrohungsanalyse:* Durch die Kombination von Daten aus der Vergangenheit<sup>5</sup> und Echtzeitinformationen können potenzielle Bedrohungen frühzeitig erkannt werden. Gotham erlaubt es Analysten, Bedrohungen in Echtzeit zu bewerten und Risiko-szenarien zu simulieren.
- *Geospatial Intelligence:* Militärische Operationen erfordern oft präzise geografische Informationen. Gotham integriert kartographische Darstellungen und ermöglicht die Überlagerung von Daten auf geografische Karten, um Bewegungen, Positionen und Hotspots besser zu analysieren.

Im militärischen Einsatz wird Gotham als zentrale Lösung für die Aufklärung und Überwachung genutzt und unterstützt die schnelle Entscheidungsfindung, die für taktische Operationen erforderlich ist.

<sup>4</sup> Vgl auch Webseite [Palantir Gotham](#).

<sup>5</sup> Wie z B: Berichte über Sicherheitsvorfälle, Angriffe oder andere Bedrohungen. Beobachtungen von typischen Mustern bei Personen, Gruppen oder Organisationen, die in der Vergangenheit Bedrohungen darstellten. Karten, frühere Einsatzorte oder bekannte Hotspots für Bedrohungen. Bewegungen von Personen, Gütern oder Fahrzeugen in der Vergangenheit. Alte Nachrichten, Gespräche oder E-Mails, die analysiert wurden.



## 4.2 Palantir Foundry

Palantir Foundry<sup>6</sup> ist eine Plattform und für Unternehmen und Organisationen gedacht, die operative und logistische Abläufe optimieren möchten. Sie erlaubt es, Daten aus unterschiedlichen Bereichen wie Produktion, Lieferkettenmanagement, Logistik und weiteren operativen Prozessen zu kombinieren. Durch ihre Fähigkeit, Daten in Echtzeit zu verarbeiten und zu visualisieren, schafft Foundry Transparenz und unterstützt fundierte Entscheidungen. Die wichtigsten Funktionen dabei sind:

- *Nahtlose Datenintegration:* Foundry sammelt Daten aus verschiedenen Quellen, wie z B Bestandslisten, Einsatzplänen, Logistiknetzwerken und Ressourcenverwaltungssystemen. Durch die Kombination all dieser Daten entsteht ein vollständiges Bild der operationellen Ressourcen.
- *Transformation und Bereinigung von Daten:* Die Plattform bietet eine Vielzahl von Tools, um Daten zu bereinigen, zu standardisieren und für die Analyse vorzubereiten. So können auch unstrukturierte Daten in eine einheitliche Struktur überführt werden, was für Organisationen, die verschiedene Datenquellen nutzen, sehr wertvoll ist.
- *Echtzeitanalyse und Berichterstellung:* Foundry erlaubt es z B Materialflüsse zu überwachen, Bestände nachzuverfolgen und Engpässe frühzeitig zu identifizieren. Es erstellt Berichte in Echtzeit, die sich bei Änderungen automatisch aktualisieren. Sie lassen sich flexibel anpassen und teamübergreifend nutzen.
- *Modellierung und Simulation:* Die Plattform erlaubt es Nutzern, Simulationen auf Basis von Datenmodellen zu erstellen, um zukünftige Szenarien zu planen. Für militärische Organisationen kann dies besonders wertvoll sein, um z B logistische Herausforderungen und Szenarien in Friedenszeiten zu simulieren und entsprechend vorbereitet zu sein.
- *Zusammenarbeit und Teamarbeit:* Foundry unterstützt eine kollaborative Arbeitsweise, bei der mehrere Nutzer gleichzeitig an Datensätzen und Analysen arbeiten können. Diese Funktion ermöglicht eine bereichsübergreifende Zusammenarbeit und fördert schnelle Abstimmungsprozesse, die in komplexen militärischen Einsätzen unerlässlich sind.

Im militärischen Bereich wird Foundry häufig zur Verwaltung der Logistik, der Versorgung und zur Planung von Einsätzen verwendet, was die operative Effizienz steigert und die Ressourcenverteilung optimiert.

## 4.3 Artificial Intelligence Platform (AIP)<sup>7</sup>

Die Artificial Intelligence Platform (AIP) von Palantir wurde entwickelt, um grosse Sprachmodelle (Large Language Models, LLMs) und KI-Anwendungen in Unternehmen und Organisationen zu integrieren. Obwohl AIP ursprünglich für militärische Anwendungen konzipiert wurde, wird sie auch in kommerziellen Bereichen eingesetzt. Die zentralen Punkte dabei sind:

- *Datenintegration und -sicherheit:* AIP ermöglicht die Verarbeitung grosser Datenmengen innerhalb abgeschotteter Netzwerke, was für militärische Anwendungen entscheidend ist, um sensible Informationen zu schützen.
- *Einsatzkoordination:* Die Plattform unterstützt die Entscheidungsfindung in Echtzeit, beispielsweise durch die Analyse von Multi-Domain-Operations und die Visualisierung taktischer Szenarien.
- *Automatisierung und Effizienzsteigerung:* Militärische Einheiten können mithilfe von AIP datenbasierte Entscheidungen treffen, von der Ressourcenallokation bis zur Planung von Einsätzen.

<sup>6</sup> Vgl auch die Webseite [Palantir Foundry](#).

<sup>7</sup> Vgl auch die Webseite [Palantir Artificial Intelligence Platform](#)



AIP ist besonders im Kontext der Modernisierung von Streitkräften und der Anwendung von Künstlicher Intelligenz zur Verbesserung der strategischen und taktischen Entscheidungsfindung von Bedeutung.

#### 4.4 Palantir TITAN

TITAN (*Tactical Intelligence Targeting Access Node*), ist ein bodengestütztes System auf einem LKW, das die Fähigkeiten der US-Armee im Bereich der Aufklärung und Zielerfassung modernisieren soll. Das System integriert verschiedene Sensoren wie z B aus Weltraum-, Luft- und terrestrischen Quellen, um Echtzeitinformationen für präzise Langstreckenangriffe bereitzustellen. Im März 2024 erhielt Palantir den Auftrag der US-Armee im Umfang von 178,4 Millionen USD zur Entwicklung und Lieferung von zehn TITAN-Prototypen. TITAN ist die nächste Generation einer Bodenstation für die Nachrichtengewinnung, Überwachung und Aufklärung. Sie nutzt Künstliche Intelligenz, um Sensordaten aus den verschiedenen Quellen schnell zu verarbeiten. TITAN wird gemäss Firmenangabe nachrichtendienstliche Unterstützung für die Zielerfassung und das Lageverständnis bieten und soll die Zeitspanne vom *Sensor-to-Shooter* verkürzen, womit Multidomain-Operationen unterstützt werden.<sup>8</sup>

#### 4.5 Palantir Readiness Solution Suite

Palantir Readiness<sup>9</sup> ist eine Softwaresolution Suite, die darauf abzielt, die Verfügbarkeit und Einsatzbereitschaft der physischen und finanziellen Mittel sowie des Personals in Organisationen effizient zu verwalten und zu optimieren und die strategische Planung zu verbessern. Sie nutzt Datenintegration und -analyse, um Entscheidungsprozesse in Echtzeit zu unterstützen. Die Suite besteht aus den drei Modulen: *Asset*, *Personnel* und *Financial Readiness*.

##### 4.5.1 Modul Asset Readiness

Das Modul *Asset Readiness* ist eine Softwarelösung, die Organisationen dabei unterstützt, jederzeit einen umfassenden und aktuellen Überblick über ihre physischen Mittel (*Asset*) zu erhalten. Durch die Integration und Harmonisierung fragmentierter Datenquellen wird ein digitales Abbild (*Digital Twin*) der *Asset* erstellt. Dieses digitale Modell ermöglicht es, den Zustand der *Assets* zu analysieren, Trends zu identifizieren und fundierte Entscheidungen zu treffen. Die zentralen Punkte dabei sind:

- *Zustandsüberwachung und Wartung*: Echtzeitüberwachung des Zustands aller physischen Mittel wie z B Panzer, Flugzeuge oder Kommunikationsausrüstung, um frühzeitig Wartungsbedarfe zu erkennen und die Verfügbarkeit zu maximieren.
- *Bestandsmanagement*: Nachverfolgung von Mitteln und deren Bewegungen, um sicherzustellen, dass kritische Mittel jederzeit verfügbar sind.
- *Lebenszyklusmanagement*: Analyse und Optimierung der Lebenszyklen von Ausrüstungen, um eine kosteneffiziente Nutzung zu gewährleisten.

Mit dem Modul *Asset Readiness* können militärische Organisationen die Einsatzbereitschaft ihrer Ausrüstung jederzeit sicherstellen und gleichzeitig die effiziente Nutzung der Ressourcen optimieren.

##### 4.5.2 Modul Personnel Readiness

Das Modul *Personnel Readiness* konzentriert sich auf die Einsatzbereitschaft des Personals, einschliesslich der Verfügbarkeit und des Gesundheitszustands der Truppen. Es unterstützt die Zuweisung und Verwaltung von Personalressourcen und hilft sicherzustellen, dass die richtigen Personen zur richtigen Zeit verfügbar sind. Die zentralen Punkte sind:

<sup>8</sup> Vgl auch die Webseite Palantir [TITAN](#).

<sup>9</sup> Vgl auch die Webseite [Palantir Readiness](#)

- *Verfügbarkeits- und Kapazitätsmanagement*: Verfolgung der Einsatzbereitschaft des Personals und Planung von Einsätzen basierend auf dessen Verfügbarkeit.
- *Kompetenz- und Ausbildungsmanagement*: Überwachung und Planung von Schulungen, um sicherzustellen, dass das Personal die erforderlichen Fähigkeiten und Qualifikationen besitzt.
- *Gesundheits- und Fitnessüberwachung*: Verwaltung von Gesundheits- und Fitnesstraining, um den Zustand und die Leistungsfähigkeit des Personals zu optimieren.

Mit dem Modul *Personnel Readiness* können militärische Organisationen ihre Einsatzkräfte effizienter verwalten und sicherstellen, dass jederzeit gut ausgebildetes und gesundes Personal verfügbar ist.

#### 4.5.3 Modul Financial Readiness

Das Modul *Financial Readiness* konzentriert sich auf die finanzielle Planung und Budgetierung, um die Einsatzbereitschaft in allen Bereichen sicherzustellen. Es erlaubt Organisationen, Kosten effektiv zu überwachen, Mittel optimal zuzuweisen und Ausgaben in Echtzeit zu kontrollieren. Die zentralen Punkte dabei sind:

- *Budgetierung und Planung*: Erstellung und Überwachung von Budgets für verschiedene militärische Programme und Einsatzgebiete.
- *Kostenkontrolle und -verfolgung*: Echtzeitanalyse von Ausgaben, um finanzielle Mittel effektiv zu verteilen und unnötige Kosten zu vermeiden.
- *Ressourcenzuordnung und Effizienzmanagement*: Optimierung der finanziellen Mittel für Personal, Ausrüstung und Betrieb, um die Einsatzbereitschaft innerhalb des verfügbaren Budgets zu maximieren.

Das Modul *Financial Readiness* hilft militärischen Organisationen, finanzielle Ressourcen zielgerichtet zu nutzen und finanzielle Risiken zu minimieren, um die langfristige Einsatzbereitschaft zu gewährleisten.

#### 4.5.4 Zusammenfassung

Insgesamt ermöglicht die Readiness Solution Suite den militärischen Organisationen, ihre Einsatzbereitschaft ganzheitlich zu verwalten und zu optimieren. Die Module *Asset Readiness*, *Personnel Readiness* und *Financial Readiness* wirken zusammen, um eine vollständige und integrale Sicht auf die Verfügbarkeit und Effektivität von Ressourcen zu bieten, was für eine erfolgreiche Einsatzplanung und -durchführung entscheidend ist.

### 4.6 Gebrauch in Europa

#### 4.6.1 Nutzung durch Streitkräfte

Die britischen Streitkräfte gehören zu den prominentesten Anwendern von Palantir-Lösungen in Europa. Sie setzen sowohl Palantir Gotham als auch Palantir Foundry ein. Unter anderem arbeitet Palantir seit 2022 eng mit der Royal Navy zusammen, um das Personal- und Flottenmanagement für mögliche künftige Konflikte zu optimieren. Inwieweit hier *Palantir for Readiness* oder die *Palantir Artificial Intelligence Platform (API)* genutzt werden, ist nicht öffentlich bekanntgegeben worden.

Über den Einsatz von Palantir-Technologie in anderen Armeen, wie z B Frankreich, Österreich, Norwegen, Schweden oder Finnland, liegen ebenfalls keine öffentlichen Berichte vor, die auf eine Verwendung hinweisen. Sicher ist, dass die deutsche Bundeswehr keine Palantir-Technologie verwendet. Vermutlich ist die militärische Nutzung von Palantir-Software in Europa noch sehr begrenzt.



#### 4.6.2 Nutzung durch die Polizei

In einigen europäischen Ländern jedoch wird Palantir im Bereich der inneren Sicherheit eingesetzt. Einige deutsche Polizeibehörden, wie etwa in Hessen, Nordrhein-Westfalen und Bayern, nutzen die Plattform Gotham zur Unterstützung bei der Datenanalyse in kriminalpolizeilichen Kontexten (Netzpolitik). Eine bundesweite Einführung dieser Analyseplattform wurde hingegen verworfen, weil sie mit zu grossen Risiken in Verbindung gebracht werden. Der Hauptgrund, der gegen eine bundesweite Einführung von Palantir spricht, liegt in datenschutzrechtlichen Bedenken und in der Präferenz für eigenständige, europäische Lösungen. Kritiker, darunter Innenpolitiker und Datenschutzexperten, befürchten eine Vermischung von staatlicher Tätigkeit mit privatwirtschaftlichen Interessen, insbesondere in Hinblick auf die Verarbeitung sensibler Polizeidaten. Daher wird auch eine Eigenentwicklung in Betracht gezogen, die langfristig eine Unabhängigkeit von externen Anbietern erlaubt (Tagesschau, BR). In Norwegen wird Palantir Gotham beim Zoll eingesetzt, um Passagiere und Fahrzeuge zu überwachen und zu kontrollieren. Seit 2017 verwendet die dänische Polizei das POL-INTEL-System, das auf Palantir Gotham basiert. Dieses System erstellt sogenannte «Heat Maps»<sup>10</sup>, um Gebiete mit erhöhten Kriminalitätsraten zu identifizieren, und unterstützt so die präventive Polizeiarbeit (Taylor & Francis).

#### 4.6.3 Nutzung in der Schweiz

In der Schweiz wird Palantir hauptsächlich von Unternehmen in der Privatwirtschaft genutzt. Die Credit Suisse arbeitete seit 2016 mit Palantir zusammen, um ein automatisiertes Compliance-System zu entwickeln. Sie investierte mehrere hundert Millionen Franken in die Integration von Softwarelösungen von Palantir, um ihre Compliance-Prozesse zu optimieren. Dieses Vorhaben erwies sich jedoch als problematisch. Berichten zufolge beliefen sich die Investitionen auf rund 500 Mio CHF, wobei das Projekt letztlich als Fehlschlag betrachtet wurde (Inside Paradeplatz). Nach der Übernahme durch die UBS hat diese beschlossen, die Zusammenarbeit mit Palantir zu beenden. Sie hat die Software auf die sogenannte «Decom-Liste» gesetzt, was bedeutet, dass sie ausgemustert wird (Inside IT).

Auch der Rückversicherer Swiss Re nutzt Palantir-Software für Datenanalysen. Die zukünftige Zusammenarbeit steht jedoch auch hier in Frage, da nach einem Führungswechsel bei Swiss Re die Nutzung von Palantir überprüft wird (finews). Das Medienunternehmen Ringier setzt ebenso auf Palantir. Es nutzt die Software Foundry, um das Potenzial von Daten auszuschöpfen und um die Leserschaft besser zu bedienen und zu informieren (Ringier). Im Rahmen einer fünfjährigen Partnerschaft wird Palantir Technologies Inc. Ringier seine «Artificial Intelligence Platform (AIP)» zur Verfügung stellen, «um die KI-Strategie für die drei strategischen Bereiche der Gruppe – Media, Marketplace und Sports Media – international voranzutreiben und mit der neuesten und verantwortungsvollsten KI-Technologie zu arbeiten» (Ringier).

Eine Nutzung durch Behörden in der Schweiz ist dagegen nicht bekannt. Das Bundesamt für Gesundheit (BAG) lehnte ein Angebot von Palantir zur Unterstützung des Pandemiemanagements ab (WOZ). Im Rahmen der Ausschreibung des Projekts Ik NDA (BÖG, Art 7, Abs 1, Bst c) hat armasuisse ein Angebot von Palantir geprüft. Aufgrund nicht erfüllter MUSS-Kriterien wurde das Angebot für die Shortliste nicht weiter berücksichtigt.

### 5 Fokusthema: Operative Einsatzbereitschaft mit Asset Readiness

Das Modul *Asset Readiness* ist eine Softwarelösung, die Organisationen dabei unterstützt, einen umfassenden und aktuellen Überblick über ihre Assets zu erhalten. Durch die Integration und Vereinheitlichung fragmentierter Datenlandschaften erstellt die Lösung ein digitales Abbild der Assets einer Organisation. Dies ermöglicht es, Fragen zum Zustand der Assets zu beantworten, Trends zu erkennen und fundierte Entscheidungen zu treffen.

<sup>10</sup> Heat Maps werden in der Polizeiarbeit genutzt, um Kriminalitätsdaten und -muster visuell darzustellen und zu analysieren. Sie helfen dabei, sogenannte «Hotspots» zu identifizieren – also geografische Gebiete, in denen bestimmte Arten von Verbrechen häufiger auftreten.

Beispiele dazu sind:

- **Fahrzeugwartung:** Die Software analysiert Daten zu Fahrzeugen wie Panzern, Lastwagen oder Transportfahrzeugen, darunter Wartungshistorie, Betriebsstunden und Sensorinformationen. Dies ermöglicht die frühzeitige Planung von Wartungsarbeiten, um Ausfälle im Einsatz zu verhindern und die Einsatzbereitschaft der Flotte sicherzustellen.
- **Waffen- und Munitionsmanagement:** *Asset Readiness* konsolidiert Daten über Lagerbestände, Abnutzungszustände und Nachschubketten von Waffen und Munition. So können Kommandanten sicherstellen, dass ausreichend einsatzbereite Ressourcen vorhanden sind, um Operationen effizient zu unterstützen.
- **Luftfahrzeuge:** Die Lösung integriert Daten von Flugzeugen, Drohnen und Hubschraubern, um den Zustand von Komponenten wie Triebwerken oder Avionik-Systemen zu überwachen. Dadurch lassen sich Reparaturen und Wartungen rechtzeitig planen, um die Einsatzfähigkeit der Luftstreitkräfte zu maximieren.
- **Logistik und Versorgungsketten:** *Asset Readiness* hilft bei der Überwachung von Lieferketten für kritische Ressourcen wie Treibstoff, Verpflegung oder Ersatzteile. Dies sorgt dafür, dass Versorgungsgüter rechtzeitig an die Einsatzorte gelangen und operationelle Engpässe vermieden werden.

Durch die Nutzung von *Asset Readiness* kann eine militärische Organisation ihre Ressourcen ganzheitlich und effizient managen. Die Lösung bietet eine präzise Entscheidungsgrundlage, verbessert die Einsatzbereitschaft und minimiert Ausfallzeiten.

## 5.1 Fallstudie U.S. Army

Im Jahr 2018 mussten sich die obersten Führungskräfte der US-amerikanischen Armee mit ihrem kritischsten Problem befassen: der Einsatzbereitschaft oder der Verfügbarkeit und Einsatzfähigkeit einer bestimmten Einheit, eines Soldaten oder eines Ausrüstungsteils zur Erfüllung einer Mission. Selbst die Beantwortung scheinbar einfacher Fragen im Zusammenhang mit der Einsatzbereitschaft, z. B. wie viele Panzer einsatzbereit oder wie viele Panzerfahrer ausgebildet sind, war enorm komplex, da die Informationen über Hunderte von Datenquellen oder auf den Desktops und in den Köpfen verstreut waren.<sup>11</sup>

### 5.1.1 Lösung mit Palantir for Readiness Solution Suite

Die Plattform *Palantir for Readiness* übernimmt eine zentrale Rolle bei der Kontrolle und Optimierung der Einsatzbereitschaft der Assets und des Personals der U.S. Army. Sie integriert Daten aus über 160 Quellsystemen und mehr als 30'000 Datentabellen. Dadurch ermöglicht sie die Erstellung eines digitalen Zwillings (Digital Twin). Dieser umfasst Informationen aus den Bereichen Finanzen, Logistik, Personal und Einsätze und dient der effizienten und skalierbaren Verknüpfung umfangreicher Datenquellen. Im Bereich der Einsatzbereitschaft und Entscheidungsunterstützung ermöglicht die Plattform die Echtzeit-Überwachung von mehr als 65'000 Einheiten, über einer Million Dienstposten und 1,5 Millionen Ausrüstungsgegenständen. Die Verarbeitung grosser Datenmengen in Echtzeit erlaubt eine kontinuierliche Analyse. Ein weiterer Einsatzbereich der Plattform ist die prädiktive Analyse. Durch die frühzeitige Identifikation überschüssiger Mittel konnten im Jahr 2020 mehr als 3,3 Milliarden USD für andere Zwecke freigegeben werden. Dies verdeutlicht die Rolle der Plattform im effizienten Umgang mit Ressourcen. Die Plattform wird so über ihre Funktion als Analysetool hinaus als Entscheidungsunterstützungssystem genutzt. Die Integration grosser Datenmengen und die Bereitstellung von Informationen in Echtzeit bieten Führungskräften der U.S. Army zudem einen umfassenden Überblick über den Status und die Verfügbarkeit von Personal, Material und logistischen Ressourcen. Dies schafft eine Grundlage für datenbasierte Entscheidungen. Darüber

<sup>11</sup> Vgl. Carahsoft, Resources [Asset Readiness Introduction](#), Case Studies Seite 6. Vgl. auch die [Webpage Palantir Blog, Medium](#): Are You Ready? New Palantir modules help enable readiness at the world's most critical institutions, August 11<sup>th</sup>, 2022.



hinaus prognostiziert *Readiness* die Einsatzbereitschaft. Dies ermöglicht die frühzeitige Einleitung von Massnahmen zur Risikominderung. Die kontinuierliche Aktualisierung und Echtzeit-Überwachung unterscheiden die Lösung von statischen Systemen.

### 5.1.2 Auszug einzelner Ergebnisse

Mit *Palantir for Readiness* wird ein umfassendes Verständnis über operative Einsatzbereitschaft vermittelt. Zudem hat die Lösung einen transformativen Einfluss auf die Organisation und unterstützt Einsätze in einer zunehmend unbeständigen Welt. Beispiele dieser Ergebnisse mit Aussagen zur Einsatzbereitschaft sind dabei:

- *Bereitschaftsmetriken und -prognosen für Flugzeuge und Besatzungen.* Durch die Integration massgeblicher Quellsysteme in Echtzeit bietet die Plattform ein integrales Bild der Einsatzbereitschaft von Flugzeugen, Piloten und Besatzungen auf jeder Ebene. Mit dieser Fähigkeit hat sich die Sichtbarkeit von Luftfahrtkennzahlen auf jeder Ebene verbessert und damit auch die allgemeine Lage im Luftbereich. Die Plattform stellt die geplanten Flugstunden und Finanzprognosen der Anzahl effektiver Flugstunden und den dafür aufgewendeten Kosten gegenüber, um zu bestimmen, ob Ressourcenanpassungen erforderlich sind.
- *Metriken zur eigenständigen Überprüfung der Bereitschaft und Ressourcenverfügbarkeit.* Um relevante Aufzeichnungen zu einem bestimmten Mittel (Asset) zu erhalten, mussten zuvor E-Mail-Anfragen an Kommandanten und andere Beteiligte in der Organisation gesendet werden. Es dauerte Tage, bis Antworten eingingen. Selbst die Beantwortung einfacher Fragen, ob beispielsweise ein Ersatz in einer Einheit vorrätig war, konnte einen erheblichen manuellen Aufwand erfordern. Die Plattform bietet den Kommandanten der gesamten Armee eine Self-Service-Lösung, mit der sie auf eine umfassendere, integrale Ansicht zugreifen können, die ihnen einen klaren Überblick über die Verfügbarkeit ihrer Mittel gibt.
- *Einsatzbereitschaft der Truppen und Entscheidungshilfe in Echtzeit.* Vor *Palantir* verbrachten militärische Verbände, wie etwa die 82. Luftlandedivision, schätzungsweise mehr als 500 Stunden pro Monat damit, eine einmalige monatliche Selbsteinschätzung ihrer Einsatzbereitschaft zu erstellen. Dies stellt ein unhaltbares Kosten- und Zeitrisko für eine globale Eingreiftruppe dar, die innerhalb von 18 Stunden überall auf der Welt eingesetzt werden muss. Die Division hat nun über eine verbandsorientierte Anwendung, die ihr Personal, ihre Ausrüstung und andere damit zusammenhängende Kennzahlen zusammenfasst, Zugriff auf Einsatzbereitschaftsdaten in Echtzeit. Über die Lageerkennung hinaus ermöglicht die Plattform den Benutzern, die Ergebnisse im Kontext der Historie anzuzeigen. Diese helfen, die aktuelle Bereitschaftssituation in einen grösseren Kontext zu setzen, und befähigt die Befehlshaber, in Kürze fundierte, datengestützte Entscheidungen zu treffen.

Die Plattform *Palantir for Readiness* dient der U.S. Army als Werkzeug zur Integration umfangreicher Datenquellen, zur Echtzeit-Datenverarbeitung und zur prädiktiven Analyse. Sie ermöglicht die Überwachung von Personal, Material und logistischen Ressourcen, unterstützt datenbasierte Entscheidungsprozesse und trägt zur Optimierung der Einsatzbereitschaft sowie des Ressourceneinsatzes bei.

## 5.2 Daten als Voraussetzung

Für die Bestimmung und Optimierung der Einsatzbereitschaft militärischer Verbände sind verschiedene Datenquellen entscheidend. Erst die Zusammenführung dieser Datenquellen ermöglicht ein umfassendes Bild der Verfügbarkeit, Kapazität und Einsatzfähigkeit der Truppen. Zu den wichtigsten Datenquellen zählen die Personaldaten, welche Informationen zur Personalstärke, Verfügbarkeit, Qualifikation und Einsatzbereitschaft liefern. Dadurch bilden sie die Grundlage für die Planung und Sicherstellung der Verfügbarkeit von qualifiziertem Personal für spezifische Missionen. Des Weiteren sind Logistik- und Materialdaten von zentraler Bedeutung. Sie umfassen Informationen zu Beständen, zum Zustand und zur Verfügbarkeit von Ausrüstung, Fahrzeugen und Waffen. Die Daten erlauben die genaue Überwachung der Material-

verfügbarkeit sowie die frühzeitige Identifikation möglicher Engpässe. Finanz- und Beschaffungsdaten wiederum bieten wertvolle Einblicke in Budgets, in laufende Ausgaben und in den Status von Beschaffungen, was die Überwachung der Finanzierung und die effiziente Ressourcenverteilung erleichtert. Einsatzdaten und Bereitschaftsinformationen, die den Mobilisierungsstand, den Übungsstatus und die Verfügbarkeit von Truppen abbilden, sind ebenfalls unerlässlich, da sie zeigen, wie rasch und in welchem Umfang Verbände einsatzbereit sind. Wartungs- und Instandhaltungsdaten tragen ebenfalls zur Gesamtübersicht bei, indem sie geplante und ungeplante Wartungen sowie die Instandhaltungshistorie und den Reparaturstatus aufzeigen. Dies hilft bei der Vermeidung von Materialausfällen und der Planung der Materialverfügbarkeit. Zudem bietet Geospatial Intelligence (GEOINT) mit geografischen Daten wichtige Lageinformationen und ermöglicht eine gezielte Einsatzplanung. Open-Source Intelligence (OSINT<sup>12</sup>) und Drittanbieter-Datenquellen, die Informationen aus öffentlich zugänglichen Quellen oder von spezialisierten Anbietern, wie z B von Wetterdiensten, umfassen, bieten einen zusätzlichen Kontext für strategische Entscheidungen. Schliesslich liefern Daten zum Ressourcenmanagement und zur Bedarfsplanung aktuelle Informationen über die Verfügbarkeit kritischer Versorgungsgüter, wie etwa Treibstoff, Verpflegung und medizinische Vorräte, und ermöglichen so eine kontinuierliche Sicherstellung des Nachschubs. Palantirs Fähigkeit, all diese Datenquellen in einem einzigen System zu vereinen, ist der zentrale Faktor für seine hohe Leistungsfähigkeit im militärischen Einsatz. Durch die Integration dieser vielfältigen Datenquellen entsteht ein detailliertes Lagebild, das die präzise Bestimmung und fortlaufende Bewertung der Einsatzbereitschaft ermöglicht und Entscheidungsträgern eine fundierte Basis für die Planung und Umsetzung gezielter Massnahmen bietet.

### 5.3 Details zum Modul Asset Readiness

Einen Überblick über die eigenen Mittel und deren Verfügbarkeit zu gewinnen, kann eine komplexe Herausforderung darstellen. Denn die Daten, die eine Organisation benötigt, um sich selbst zu «sehen», sind oft über verschiedene Systeme verteilt. Darüber hinaus sind diese Daten häufig in unterschiedlichen Formaten in Silosystemen gespeichert, sodass eine umfassende manuelle Auswertung erforderlich ist, um zu verwertbaren Informationen zu gelangen. Oft müssen Experten diese Fragen in aufwendiger manueller Arbeit beantworten.

#### 5.3.1 Kern der Lösung

Im Kern handelt es sich bei Asset Readiness um eine Softwarelösung mit offener Architektur, die darauf ausgelegt ist, fragmentierte Datenlandschaften zu vereinheitlichen und dabei bestehende Systeme und Prozesse zu berücksichtigen. Mit integrierten, interpretierbaren Daten und flexiblen operativen Tools können Benutzer nicht nur schneller einen Überblick über den aktuellen Zustand erhalten, sondern auch tiefergehende Fragen beantworten (Abbildung 1).



Abbildung 1: Von fragmentierten Daten über deren Integration zum «Digital Twin» zur Analyse der Ressourcen

Anstatt nur herauszufinden, wie viele Fahrzeuge sich beispielsweise in der Flotte befinden, kann ein Benutzer nun fragen: «Wie viele dieser Fahrzeuge sind auf dem neuesten Stand in

<sup>12</sup> OSINT steht für Open Source Intelligence und beschreibt die Gewinnung und Analyse von Informationen aus öffentlich zugänglichen Quellen wie z B Medienberichte, Social Media, Online-Foren und andere offene Informationsquellen im Internet.



Bezug auf ihre Wartung und wie verteilen sich die nicht einsatzbereiten Fahrzeuge auf neue und alte Modelle?» Das Modul *Asset Readiness* hilft dabei, die Mittel effizient zu verwalten und deren Einsatzbereitschaft zu kontrollieren und zu optimieren. Die Lösung umfasst dabei:

- *Eine zentralen Datenquelle über alle Assets der Organisation:* Die Lösung umfasst eine zentrale, zuverlässige Plattform, auf der alle Daten zu den Mittel (Assets) gesammelt und aktuell gehalten werden. Sie ermöglicht verschiedenen Teams, gemeinsam auf diese Daten zuzugreifen und damit zu arbeiten, wobei klare Regeln festlegen, wer welche sehen oder bearbeiten darf.
- *Messung und Bewertung der Einsatzbereitschaft:* Die Lösung bietet die Möglichkeit, dass Organisationen den Status ihrer Assets in Echtzeit überwachen und auf verschiedenen Ebenen analysieren können – vom Gesamtüberblick bis hin zu einzelnen Komponenten.
- *Untersuchung von Problemen:* Bei auftretenden Problemen ermöglicht die Lösung eine tiefgehende Analyse, um die Ursache zu identifizieren und effektive Massnahmen zur Behebung zu priorisieren.
- *Optimierung der Ressourcenzuweisung:* Es kann bestimmt werden, wo ein Asset am dringendsten benötigt wird, wohin Ausrüstung gesendet werden sollte oder wo Arbeitszeit optimiert werden kann. Die Lösung hilft dabei, Ressourcen effizient zu verteilen, indem sie den Bedarf identifiziert und die Nutzung optimiert.
- *Analyse von langfristigen Trends auf jeder Ebene:* Die Lösung ermöglicht es, zeitliche Entwicklungen im Zustand und in der Einsatzbereitschaft einzelner Assets zu analysieren. Solche Analysen sind sowohl in einer gesamtheitlichen Sicht als auch für die einzelnen Komponenten möglich.
- *Vorwegnahme erwarteter Spitzen und Risiken:* Die Software ermöglicht es, potenzielle Herausforderungen frühzeitig zu erkennen und proaktiv Massnahmen zu ergreifen, um negative Auswirkungen zu minimieren. Dies kann z B bei Trainingsübungen der Fall sein, die einen grösseren personellen oder materiellen Mehraufwand erfordern als geplant.

### 5.3.2 Digital Twin der Ressourcen und Arbeitsabläufe

Es wird ein *Digital Twin* erstellt, der Ressourcen und Arbeitsabläufe der gesamten Organisation widerspiegelt. Dabei werden Daten aus unterschiedlichen Systemen zusammengeführt, bereinigt und so geordnet, dass jeder in der Organisation sie verstehen kann. Dieser Engineering-Prozess ermöglicht es den Nutzern, mit Daten als Objekten zu arbeiten und ihre Eigenschaften sowie ihre Beziehungen untereinander zu verstehen. Die Objekte dienen den Nutzern als interpretierbare Bausteine, welche die Analysen und Arbeitsabläufe auf der gesamten Plattform unterstützen.

Informationen zum Beispiel, die für einen einzelnen LKW relevant, in verschiedenen Daten-systemen gespeichert und typenspezifisch gekennzeichnet sind, werden zentralisiert und in einem einzigen «LKW»-Objekt erfasst. Dieser Ansatz zur Datenmodellierung beschleunigt die Gewinnung von Erkenntnissen und Ergebnissen erheblich und vereinfacht die Nutzung von Daten im gesamten Unternehmen. Jeder, der über einen autorisierten Zugang verfügt, kann mit nur wenigen Klicks Fragen beantworten, ohne dass dafür Kenntnisse im Bereich der Datenverarbeitung erforderlich sind. Die Komponenten dabei sind:

- *Data Connection* schafft einen integralen Überblick über Daten aus verschiedenen Quellen, um fundierte Entscheidungen zu ermöglichen. Dank verschiedener, konfigurierbarer Verbindungsmethoden und offener programmierbarer APIs<sup>13</sup> kann die Lösung mit jeder Datenquelle, jedem Dateisystem, jeder Datenbank oder jeder Drittanbieteranwendung verbunden werden, um Daten unabhängig von Format, Ort und Umgebung zuverlässig zu erfassen.

<sup>13</sup> APIs (Application Programming Interfaces) sind Schnittstellen, die es verschiedenen Softwareanwendungen ermöglichen, miteinander zu kommunizieren. Sie definieren, wie Programme oder Systeme Daten und Funktionen austauschen können, ohne direkt in die interne Funktionsweise der anderen Anwendungen einzugreifen.

- *Data Lineage* (Datenherkunftsverfolgung) stellt sicher, dass Benutzer den Analysen vertrauen können, indem sie die vorgelagerte Datenquelle überprüfen. Die Datenherkunft wird ab dem Zeitpunkt der Datenerfassung automatisch innerhalb der Plattform generiert, sodass Benutzer Daten nachverfolgen und Kontrollen in allen Phasen der Integration, Transformation, Verbreitung und Nutzung durchsetzen können.
- *Data Health* erkennt Datenprobleme proaktiv, bevor Entscheidungen auf der Grundlage fehlerhafter Daten getroffen werden. Benutzer können Datenqualitätsprobleme sowohl durch automatisierte Warnmeldungen als auch durch benutzergesteuerte Zustandsprüfungen überwachen, überprüfen und beheben.
- *Data Engineering* fördert eine Community für Experimente und schnelle Verbesserungen, wobei die Produktion erst geändert wird, wenn die Änderungen überprüft wurden. Benutzer können Daten gemeinsam integrieren, bereinigen, transformieren und modellieren.
- *Data Security* maximiert die Zusammenarbeit zwischen Teams und schützt gleichzeitig die Daten durch die Einhaltung fein abgestufter Berechtigungen. Das Sicherheitsmodell von Palantir bietet mehrere Verschlüsselungsebenen und rollenbasierte, zugriffsbasierte und zweckbasierte Kontrollen bis hinunter auf die Zellebene, die in allen Anwendungen und abgeleiteten Datensätzen nachgelagert bestehen bleiben.
- *Offenheit und Flexibilität*: Dies vereinfacht die Interoperabilität mit vorhandenen Datenquellen und Tools, damit neue Technologien integriert werden können, sobald diese verfügbar sind. Die Verwendung offener APIs und Software Development Kits (SDK) unterstützt mehrere Technologien und Architekturmodelle, die in die Lösung «eingebunden» werden können und die Konnektivität mit Tools von Drittanbietern ermöglichen.
- *Skalierbarkeit*: Die Lösung passt sich bei Änderungen des Datenvolumens und der Anzahl der Benutzer an und optimiert gleichzeitig den Ressourcenverbrauch. Die containerisierte Infrastrukturschicht baut auf Kubernetes<sup>14</sup> auf und sorgt für eine dynamische Skalierung, verbesserte Rechenleistung, erhöhte Kostenkontrolle und verbesserte Sicherheit.

### 5.3.3 Verschiedene 360-Grad-Ansichten

360-Grad-Ansichten bieten Einblicke und Kennzahlen zu jedem Objekt in der Betriebsumgebung, sei es eine Komponente, ein Fahr- oder Flugzeug, eine Flotte, ein Einsatz, eine Wartungsaufgabe oder ein anderes relevantes Konstrukt.

- *Component 360*: Eine detaillierte Ansicht von jedem in der Organisation verfolgten Bauteil in seinem aktuellen und historischen Kontext: der Aus- und Einbau, der Lieferant, die Sensormesswerte, die Restnutzungsdauer (RUL) und mehr.
- *Equipment 360*: Eine umsetzbare und integrierte Ansicht von Plattformen und Grossgeräten, wie z B Fahrzeuge und Maschinen. Verwendet werden Daten über Einsatzbereitschaft, Missionen, Inspektionen, Wartung, installierte Komponenten, Sensorwerte und mehr.
- *Fleet 360*: Die Lösung bietet auch Ansichten auf «Flottenebene», um die Einsatzbereitschaft und Verfügbarkeit sowie das Risiko von Assets über mehrere Plattformen hinweg zu erkennen. Sie integriert Informationen von unterschiedlichen militärischen Systemen, um eine gemeinsame Übersicht zu schaffen, die unterschiedliche Komponenten zusammenführt, unabhängig davon, ob sie zur Luftwaffe, Marine, Armee oder anderen Bereichen gehören.

<sup>14</sup> Kubernetes (kurz oft K8s genannt) ist eine Software, die hilft, die zahlreichen Software-Container einer Plattform zu steuern und zu verwalten. Ein Container enthält dabei z B die eigentliche Applikation, welche Anwender nutzen, und alles was diese Applikation braucht, um zu funktionieren.



### 5.3.4 Analysis, Reporting and Operational Decisions

Benutzer können Daten mit erweiterbaren Analysetools abfragen und Daten sowie Erkenntnisse schnell in interaktive sich in Echtzeit aktualisierenden Berichten präsentieren. Mit flexiblen Metriken, Analysen und Berichten ermöglicht die Lösung, dass Entscheidungen zeitverzugslos und basierend auf einer umfassenden Analyse getroffen werden können.

- *Überwachung der Bestandsbereitschaft* ermöglicht die Analyse und Sicherstellung der Verfügbarkeit, Einsatzbereitschaft und optimalen Nutzung von Ressourcen.
- *Ressourcenzuweisung und Entscheidungsunterstützung*: Modelle für komplexe Entscheidungsprozesse und Hierarchien können digital abgebildet werden. In Szenarien können Ressourcenanforderungen priorisiert und optimiert werden.
- *Trendanalyse basierend auf der Historie* ermöglicht die Untersuchung von Status- und Leistungsmetriken über Zeiträume hinweg, um Muster und Veränderungen zu erkennen, einschliesslich des Vergleichs von Verfügbarkeiten verschiedener Asset-Typen.

### 5.4 Nutzen des Moduls Asset Readiness

Das Modul *Asset Readiness* ist speziell darauf ausgelegt, die operative Einsatzbereitschaft und Verfügbarkeit von Ressourcen in komplexen Organisationen, wie die einer Armee, zu kontrollieren und zu optimieren. Es verbindet fortschrittliche Datenanalyse mit einer zentralisierten Plattform, um Entscheidungsprozesse zu verbessern und die Effizienz in der Ressourcennutzung zu steigern. Im militärischen Kontext bietet das Modul eine Vielzahl von Vorteilen, die auf die speziellen Anforderungen moderner Streitkräfte abgestimmt sind.

- *Zentralisierte Datenbasis*: Das Modul aggregiert und harmonisiert Daten aus unterschiedlichen Quellen, wie etwa Logistiksystemen, Personaldatenbanken oder Wartungsberichten. Diese Informationen werden in einer einzigen Plattform zusammengeführt, damit Entscheidungsträger jederzeit einen vollständigen Überblick über den Status von Personal, Fahrzeugen, Ausrüstung und anderen Ressourcen erhalten. Dies reduziert die Fragmentierung von Daten und vermeidet Inkonsistenzen, die durch getrennte Systeme entstehen könnten.
- *Echtzeit-Überwachung und Situationsbewusstsein*: Eine der Hauptstärken von *Asset Readiness* ist die Möglichkeit, Daten nahezu in Echtzeit zu visualisieren und zu analysieren. Kommandanten und Führungsgehilfen können den aktuellen Zustand und die Verfügbarkeit von Ressourcen einsehen, wodurch sie schneller fundierte Entscheidungen treffen können. Beispielsweise kann ein Kommandant die Einsatzfähigkeit eines Verbands sofort beurteilen und bei Bedarf Anpassungen vornehmen, um seinen Auftrag zu erfüllen.
- *Effiziente Wartungs- und Ressourcenplanung*: Das Modul nutzt Datenanalysen, um Wartungszyklen zu optimieren. Durch die Integration von Nutzungsdaten und Sensorinformationen können mögliche Ausfälle frühzeitig erkannt werden, bevor sie zu grösseren Problemen führen. Dies ermöglicht eine vorausschauende Wartungsplanung, die nicht nur die Verfügbarkeit der Ausrüstung verbessert, sondern auch die Betriebskosten senkt. Gleichzeitig hilft es, Engpässe bei kritischen Ressourcen zu vermeiden.
- *Steigerung der Einsatzbereitschaft*: Das Modul unterstützt die Streitkräfte dabei, die Einsatzbereitschaft auf mehreren Ebenen zu bewerten – von einzelnen Geräten bis hin zu ganzen Verbänden. Diese Bewertungen basieren auf Daten, die automatisch aktualisiert werden, wodurch die Abhängigkeit von manuellen Prozessen verringert wird. Dies ist besonders in dynamischen Einsatzumfeldern entscheidend, wo schnelle Reaktionen und Anpassungen notwendig sind.
- *Transparenz und optimierte Entscheidungsfindung*: Die Plattform bietet visuelle Dashboards und Berichte, die komplexe Daten in verständlicher Form darstellen. Dies erhöht die Transparenz und fördert eine effizientere Kommunikation zwischen verschiedenen Ebenen der Organisation. Führungspersonen können so strategische Entscheidungen besser an aktuelle Gegebenheiten anpassen und die Ressourcennutzung priorisieren.

**Asset Readiness** liefert der Armee eine leistungsstarke Lösung, um die Komplexität des Ressourcenmanagements zu bewältigen. Es unterstützt die Sicherstellung der Einsatzbereitschaft, indem es in Echtzeit den Zustand und die Verfügbarkeit von Assets kontrolliert und steuert. Weiter hilft es dank präziser Analyse und Planung von Ressourcen, die Kosten zu senken, und ermöglicht eine schnelle Reaktion auf sich verändernde Bedingungen im Einsatzgebiet. Damit leistet es einen entscheidenden Beitrag zur effizienten Auftragserfüllung in einem zunehmend datengetriebenen militärischen Umfeld.

## 5.5 Kostenschätzungen

Die Kosten variieren je nach spezifischen Anforderungen und der Grösse der Organisation. Da Palantir keine aktuellen Preislisen bereitstellt, können genaue Beträge nur durch direkte Verhandlungen ermittelt werden. Durch die Analyse von öffentlich zugänglichen Informationen und Erfahrungswerten aus ähnlichen Projekten lassen sich die Kosten aber schätzen.

- **Lizenzkosten und Implementierung.** Ein Bericht des Westdeutschen Rundfunks (WDR) aus dem Jahr 2022 zeigt, dass die Polizei Nordrhein-Westfalen für die Implementierung der Palantir-Software ursprünglich 14 Millionen Euro veranschlagt hatte. Die tatsächlichen Kosten stiegen jedoch auf 39 Millionen Euro, wobei allein die Lizenzkosten für fünf Jahre 22 Millionen Euro betrugen ([Heise online](#)).
- **Preisliste von Palantir.** Ein öffentliches Dokument von Palantir von 2019 listet verschiedene Lizenzmodelle auf. Beispielsweise kostet eine jährliche Lizenz pro Server-Core 66 000 GBP. Lösungsbasierte Lizenzen beginnen bei 250 000 GBP und können je nach Komplexität bis zu 2 Millionen Pfund Sterling betragen ([Notech For Tyrants](#)).
- **Wartungs- und Supportkosten.** In der Regel betragen die Wartungs- und Supportkosten etwa 15–25 % der Lizenzgebühren pro Jahr. Diese Schätzung basiert auf allgemeinen Branchenstandards für Softwarelösungen.

### Einmalige Kosten

- **Implementierung und Anpassung:** Diese Kosten umfassen die Integration des Moduls in bestehende Systeme, die Anpassung an spezifische Bedürfnisse und die Schulung des Personals. Militärische Organisationen haben in der Regel hohe Anforderungen an Sicherheit und Anpassung, was die Kosten in die obere Skala – also bis zu zweistelligen Millionenbeträgen – treiben kann.
- **Datenmigration:** Die Übertragung und Bereinigung vorhandener Daten kann zusätzliche Kosten verursachen, abhängig von der Datenmenge und -komplexität. Ein grosses Risiko bildet die schlechte Datenqualität. Gute Datenqualität ist die Ausnahme, was auch hier die Kosten in die Hunderttausende oder gar Millionen treiben kann.

### Wiederkehrende Kosten

- **Lizenzgebühren:** Palantir arbeitet häufig mit Abonnementmodellen, bei denen jährliche Lizenzgebühren anfallen, die sich in der Regel nach Nutzerzahl, Datenvolumen und Funktionalität staffeln. Auch wenn es sich bei der Polizei von Nordrhein-Westfalen um Palantir Gotham handelt, gibt das Beispiel eine genauere Vorstellung von den Lizenzkosten. Diese belaufen sich auf 22 Mio € über 5 Jahre ([Heise online](#)).
- **Wartung und Support:** Für kontinuierliche Updates, technischen Support und Wartung fallen zusätzliche jährliche Gebühren an, die oft einen Prozentsatz der Lizenzkosten ausmachen. Im Falle der Polizei von Nordrhein-Westfalen wären dies jährliche Kosten für Wartung und Support von 660 000 bis 1 100 000 €.



## 6 Herausforderungen

Palantir *Asset Readiness* bietet wertvolle Unterstützung bei der Kontrolle und Optimierung der operativen Einsatzbereitschaft von militärischen Ressourcen in Echtzeit. Die Plattform ist jedoch stark auf die Verfügbarkeit qualitativ hochwertiger Echtzeitdaten angewiesen, deren Bereitstellung problematisch sein kann, wenn z. B. die für die Datenübertragung erforderlichen Kommunikationssysteme nicht verfügbar sind oder Risiken durch SIGINT-Bedrohung (Signals Intelligence) im Einsatzgebiet bestehen. Um den Zustand und die Verfügbarkeit von Ressourcen zu überwachen, sind Sensoren und IoT-Geräte notwendig. Darüber hinaus ist der Betrieb mit hohen Kosten und einem erheblichen Wartungsaufwand verbunden, was sich auf die Einsatzfähigkeit auswirken und die Budgetplanung der militärischen Organisationen belasten kann. Die Herausforderungen im Detail sind:

- *Datenqualität und -aktualität:* Die Leistungsfähigkeit hängt stark von der Qualität und Aktualität der eingespeisten Daten ab. Wenn die Echtzeitdaten ungenau, unvollständig oder veraltet sind, kann die Plattform keine verlässlichen Informationen über den Zustand und die Verfügbarkeit von Ressourcen liefern, was die Entscheidungsfindung beeinträchtigen kann.
- *Abhängigkeit von Sensoren und IoT:* Um den Zustand und die Einsatzbereitschaft von Ressourcen zu überwachen, nutzt Readiness die Daten von Sensoren und IoT-Geräten, die in die militärischen Systeme und Ausrüstungen integriert werden müssen. In ressourcenarmen oder feindlichen Umgebungen kann die Bereitstellung und Konnektivität dieser Geräte jedoch problematisch sein, was zu Lücken in der Echtzeitüberwachung führen kann.
- *Komplexität der Dateninterpretation:* Obwohl die Plattform visuelle Dashboards und Filteroptionen bietet, hängt ihre Effektivität stark davon ab, wie gut die Daten auf den spezifischen Kontext abgestimmt sind und wie gut die Benutzer im Umgang geschult wurden.
- *Kosten und Wartung:* Die Einführung und Wartung der Plattform sind kostspielig, insbesondere in Bezug auf die Anschaffung und Instandhaltung der benötigten Sensoren und IoT-Infrastruktur. Diese finanziellen und logistischen Anforderungen können eine Herausforderung darstellen, insbesondere in Szenarien, in denen Mittel begrenzt sind oder die Infrastruktur regelmässig wechselt.
- *Abhängigkeit von stabiler Konnektivität:* Die Echtzeitüberwachung setzt eine zuverlässige und stabile Datenverbindung voraus, um eine kontinuierliche Aktualisierung der Plattform zu gewährleisten. In abgelegenen oder konfliktbelasteten Gebieten, wo die Netzwerkinfrastruktur möglicherweise eingeschränkt ist, kann dies zu Problemen führen und den Nutzen einschränken.

Zusammengefasst bietet *Asset Readiness* eine wertvolle Unterstützung zur Überwachung und Optimierung der Einsatzbereitschaft militärischer Ressourcen in Echtzeit. Jedoch erfordert die Plattform eine hochgradig zuverlässige Dateninfrastruktur und eine starke Konnektivität. Die Abhängigkeit von präzisen Echtzeitdaten und sensorbasierten Systemen sowie der Aufwand für Wartung und Betrieb stellen zusätzliche Herausforderungen dar, die den Nutzen in bestimmten militärischen Einsatzszenarien begrenzen können.

### 6.1 Risiken wie Datenhoheit, Souveränitätsverlust und Abhängigkeiten

Der Einsatz von Palantir-Lösungen bietet die Möglichkeit, schnellere datenbasierte Entscheidungsfindungen zu ermöglichen und die Effizienz militärischer Operationen zu steigern. Doch die Bedenken bezüglich Datenhoheit, nationaler Souveränität, Abhängigkeiten sowie ethischer und sicherheitspolitischer Aspekte, sind nicht zu unterschätzen. Palantir ist ein Unternehmen mit Sitz in den USA, bei dem die Möglichkeit besteht, dass sensible Daten durch die amerikanischen Regierung und Geheimdienste eingesehen werden können.

Die Abhängigkeit von externem hochqualifiziertem Personal ist ein weiteres Risiko, da unklar ist, ob für die Implementierung, den Betrieb und die Wartung der Systeme dauerhaft technisches Fachpersonal von Palantir vor Ort benötigt wird. Eine solche Abhängigkeit kann die



Handlungsfähigkeit der Armee in Krisensituationen einschränken, insbesondere wenn das militärische Personal nicht über das erforderliche Know-how verfügt, um die Systeme selbstständig zu betreiben oder gar anzupassen. Sollten Palantir-Spezialisten abgezogen werden oder nicht zur Verfügung stehen, könnte dies die Einsatzfähigkeit der Systeme und damit die Effektivität der militärischen Operationen gefährden. Zugleich wird durch die dauerhafte Anwesenheit externer Spezialisten die Geheimhaltung militärischer Informationen herausgefordert, da sie Zugang zu kritischen Prozessen und Daten erhalten.

## 6.2 Datenschutz und ethische Aspekte

Die umfassende Datenerfassung und -verknüpfung mittels Palantir-Software ermöglicht tiefgehende Analysen und Vorhersagen über das Verhalten von Einzelpersonen oder Gruppen. Kritiker sehen darin das Risiko massiver Eingriffe in die Privatsphäre. So wurde der Einsatz in Deutschland als problematisch bewertet, da in Bayern ein Testbetrieb der Palantir-Software mit echten Personendaten stattfand, was vom Landesdatenschutzbeauftragten als verfassungs- und rechtswidrig eingestuft wurde (BR 24).<sup>15</sup> Ein weiterer Kritikpunkt ist die potenzielle Überwachung und Profilbildung von Bürgern, die ohne deren Wissen oder Zustimmung erfolgen könnte. Die Gefahr, dass bestimmte Personen aufgrund statistischer Zusammenhänge ungewollt ins Visier geraten, ist nicht auszuschliessen.

## 6.3 Strengere technische und rechtliche Regelungen

Am 16. Februar 2023 fällte das Bundesverfassungsgericht ein Urteil, das den Einsatz von automatisierten Datenanalyse-Werkzeugen – in diesem Fall mit Palantir Gotham – bei der Polizei aufgrund von Verletzungen datenschutzrechtlicher Grundsätze beschränkt. Seither sind Art und Umfang der in die Analysesoftware eingespeisten Daten strenger geregelt, die Kennzeichnung der Daten ist vorgeschrieben und eine effektive Kontrolle der Nutzung der Systeme ist vorzusehen. Die Risiken, die mit dem Einsatz solcher Analyseplattformen verbunden sind, wurden im Rahmen der Verfassungsbeschwerde und einer mündlichen Anhörung thematisiert. In der Anhörung wurde deutlich, dass massenhaft Daten von Unbeteiligten, Zeugen oder Kontaktpersonen in diesem Analysesystem landen. Dabei wurde das zwingende Prinzip der Zweckbindung der Daten missachtet. So wurden beispielsweise grosse Mengen von Daten aus Funkzellenabfragen erfasst, die tausende Handy-Nutzer unwissentlich zu Betroffenen machten. Da es möglich ist, dass umfangreiche Persönlichkeitsprofile aus den Informationen erstellt werden, entstehen für die Betroffenen Gefahren für ihr Grundrecht auf informationelle Selbstbestimmung, denen das Urteil Rechnung trägt ([netzpolitik.org](https://www.netzpolitik.org)).

## 6.4 Transparenz und Verantwortung

In der Schweiz ist der Einsatz von Palantir-Software bisher weniger verbreitet. Eine Nutzung muss sorgfältig abgewogen werden, zumal das Unternehmen Palantir in der Kritik steht und in anderen Ländern mit Überwachungsmassnahmen und möglichen Eingriffen in die Privatsphäre in Verbindung gebracht wird. Dieses Misstrauen ist auch in der Schweiz präsent. Die Entscheidung von Palantir, seine europäische Niederlassung im Kanton Schwyz zu etablieren, hat kritische Reaktionen ausgelöst. So zeigte sich die betroffene Gemeinde Altendorf überrascht von der Standortwahl, da die Gemeindebehörden erst aus den Medien davon erfuhr und im Entscheidungsprozess nicht involviert waren ([Inside-IT](#)).

Datenschutzbedenken wurden ebenfalls laut. Hernani Marques vom Verein Chaos Computer Club Schweiz (CCC-CH) wies darauf hin, dass Palantir von Beginn an durch die CIA mitfinanziert wurde und enge Verbindungen zu Geheimdiensten pflegt. Marques äusserte Bedenken, dass die Schweiz im Vergleich zur EU ein weniger strenges Datenschutzgesetz hat, was die Niederlassung von Firmen wie Palantir erleichtere ([srf.ch](https://www.srf.ch)). Darüber hinaus gibt es Kritik an der

<sup>15</sup> Wenn echten Daten von Bürger und Bürgerinnen verwendet werden, spielt es rechtlich keine Rollen, ob es sich um einen Text- oder Regelbetrieb handle, was ohne spezielle Gesetzesgrundlage verfassungswidrig ist.



Intransparenz des Unternehmens. Die enge Zusammenarbeit von Palantir mit Nachrichtendiensten und die Bereitstellung von Big-Data-Analysen für Organisationen wie die CIA und andere Regierungen werfen Fragen zur Transparenz und ethischen Verantwortung auf ([itmarkt.ch](http://itmarkt.ch)). Diese kritischen Stimmen zeigen die Vorbehalte, die bezüglich Palantir bestehen. Sollte die Lösungen von Palantir in Erwägungen gezogen werden, ist eine klare und transparente Kommunikation essenziell, auch wenn sich damit nicht alle Bedenken ausräumen lassen und das Risiko von öffentlichen Protesten und politischen Vorstössen bestehen bleibt.

## 7 Empfehlungen

### 7.1 Überprüfung von Alternativen

Die Schweizer Armee sollte Alternativen zu Palantir in Betracht ziehen. Es gibt europäische Unternehmen, die vergleichbare Lösungen anbieten und mit den Datenschutz- und Sicherheitsanforderungen besser vertraut sind.<sup>16</sup> Die Prüfung von Open-Source-Optionen oder die Entwicklung und Integration eigener Datenanalyseplattformen könnten Wege sein, um die Kontrolle über kritische Systeme zu behalten und Abhängigkeiten zu reduzieren. Die Entwicklung sollte dabei nicht im Alleingang, sondern mit Kooperationspartnern erfolgen, die offen, vertrauenswürdig, integer und souverän erscheinen, um eine sichere, nachhaltige und produktive Zusammenarbeit zu gewährleisten.

### 7.2 Intensivierung von Kooperationen

### 7.3 Beantwortung zentraler Fragen

In diesem Kontext sind unter anderem folgende zentrale Fragen zu klären: Wie wird die technologische Unabhängigkeit der Armee gewährleistet, und wie lässt sich der Schutz sensibler Daten garantieren? Welche Alternativen zu externen Anbietern stärken die Souveränität und minimieren Risiken? Zugleich müssen die ethische und rechtliche Vereinbarkeit externer Lösungen sowie ihr langfristiges Kosten-Nutzen-Verhältnis bewertet werden. Schliesslich sind geopolitische Risiken und strategische Abhängigkeiten in internationalen Kooperationen kritisch zu analysieren, um eine nachhaltige und unabhängige Strategie zu entwickeln.

*Aus den genannten Gründen empfehlen die Gutachter, auf Lösungen des Unternehmens Palantir Technologies Incorporated zu verzichten. Die Thematik der operativen Einsatzbereitschaft wird 2025 im Rahmen der spezifischen KI-Strategie der Armee durch die Armeepanung behandelt.*

<sup>16</sup> z B SAP Defense & Security oder Accenture (BGÖ, Art 7. Abs 1. Bst f).