Bundesministerium
Landwirtschaft, Regionen
und Tourismus

exploreAI

Studie zum Einfluss von AI auf das Militärwesen im österreichischen Kontext

Tobias Dam

FFG
Forschung wirkt.

FORTE

Bundesministerium
Landesverteidigung


A.I.

Projektziele

- Analyse bestehender Programme anderer Staaten
  - Kleine vs. große Player
- Explorative Szenarienanalyse
  - Methodik
  - Use-Cases
  - Szenarien & Auswirkungen
- Applikationen und sicherheitskritische Gaps
  - Aus den Szenarien und Use-Cases,
  - Rating
- Beschaffungsleitfaden
  - Ziel: Wichtige/Richtige Fragen stellen
  - Triage – „Sinnlose" Angebote frühzeitig erkennen

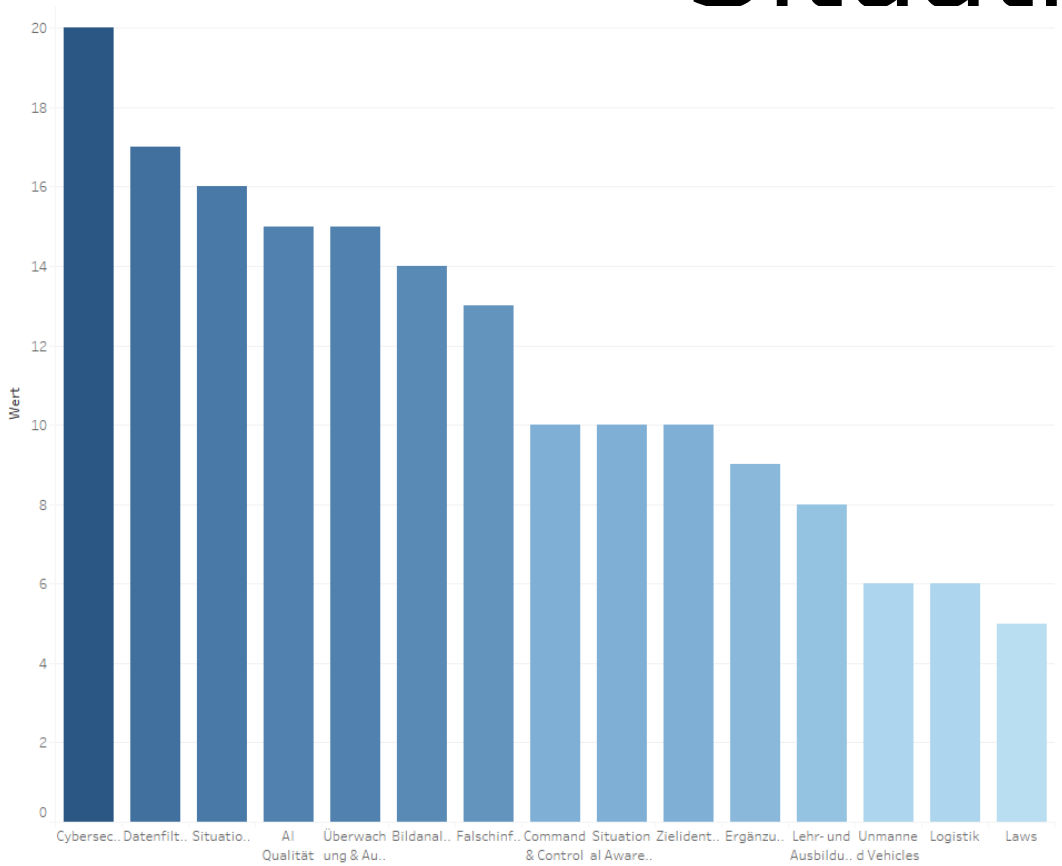
Situationsanalyse

- Fokus auf öffentlich bekannte Programme
  - Unterscheidung zwischen kleinen und großen Staaten
- Analyse der Vorhaben
  - Punktesystem: Steht im Fokus (2), wird positiv erwähnt (1), wird als Nichtziel deklariert (0)
  - Aggregation zusammengehöriger Vorhaben zu Kategorien

Nr.	Cybersecurity	Zielidentifikation	Situationsvorhersage & Prävention	Situational Awareness	Spracherkennung & Übersetzung	Logistik	Lehr- und Ausbildungszwecke / Wargaming	LAWS	Unmanned Vehicles
1	1	1	1	1	1	1	1	1	1
2	1	2	1	0	0	0	2	0	0
3	1	2	1	1	0	0	2	0	0
4	2	1	2	0	0	0	2	0	0
5	0	0	0	2	0	0	2	0	0
6	1	2	1	1	0	0	2	0	0

Bundesministerium
Landwirtschaft, Regionen
und Tourismus

Situationsanalyse



- Cyber-Security
- Datenfilterung und -visualisierung
- Situational Awareness
- AI-Qualität
- Überwachung & Aufklärung
- Bildanalyse, Gesichts- und Mustererkennung
- Falschinformationen erkennen
- Command & Control
- Situationsvorhersage und Prävention
- Zielidentifikation
- Ergänzung menschlicher Fähigkeiten
- Lehre & Ausbildung
- Autonome Vehikel und Robotersysteme
- Logistik und Instandhaltung
- Lethal Autonomous Weapon Systems (LAWS)

FFG
Forschung wirkt.

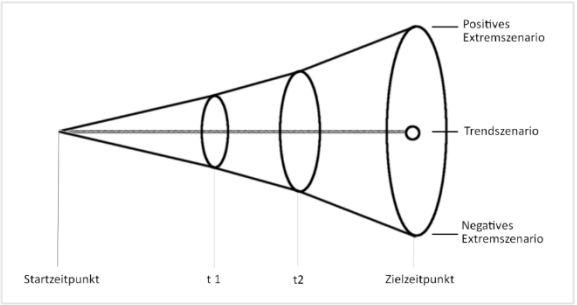
FORTE

Bundesministerium
Landesverteidigung

Explorative Szenarienanalyse

- Ausgangsposition: Qualifizierte Expert*innen-Interviews

- Szenariengenerierung
  1. Sammlung potenziell relevanter Faktoren basierend auf den folgenden Dimensionen:
     1. Dimension: Verteidigungsaufgaben des Bundesheeres
     2. Dimension: Gesellschaftliche Trends
     3. Dimension: Technologien im Bereich KI
  2. Auswahl prioritärer Faktoren
  3. Kombination der Faktoren in einem zweidimensionalen Feld
  4. Bewertung der Faktorkombinationen zur Auswahl von Use-Cases
  5. Identifikation zentraler Use-Cases



Ein Szenario & Use-Cases

- Szenario 1:
  - Starke Urbanisierung mit verarmenden Zentren
  - Starke Zunahme der Nutzung von AI und Robotik, auch im Privaten
  - Sharing-Community (auch im wirt. / milit. Bereich)

- Use Cases:
  - Penetration Testing AI & Robotics
  - Wargames
  - Cyber Defense Centers
  - Intrusion Detection Systems

- Daraus: Identifikation von Trends und Sicherheitsproblemen

Applikationen und Gaps

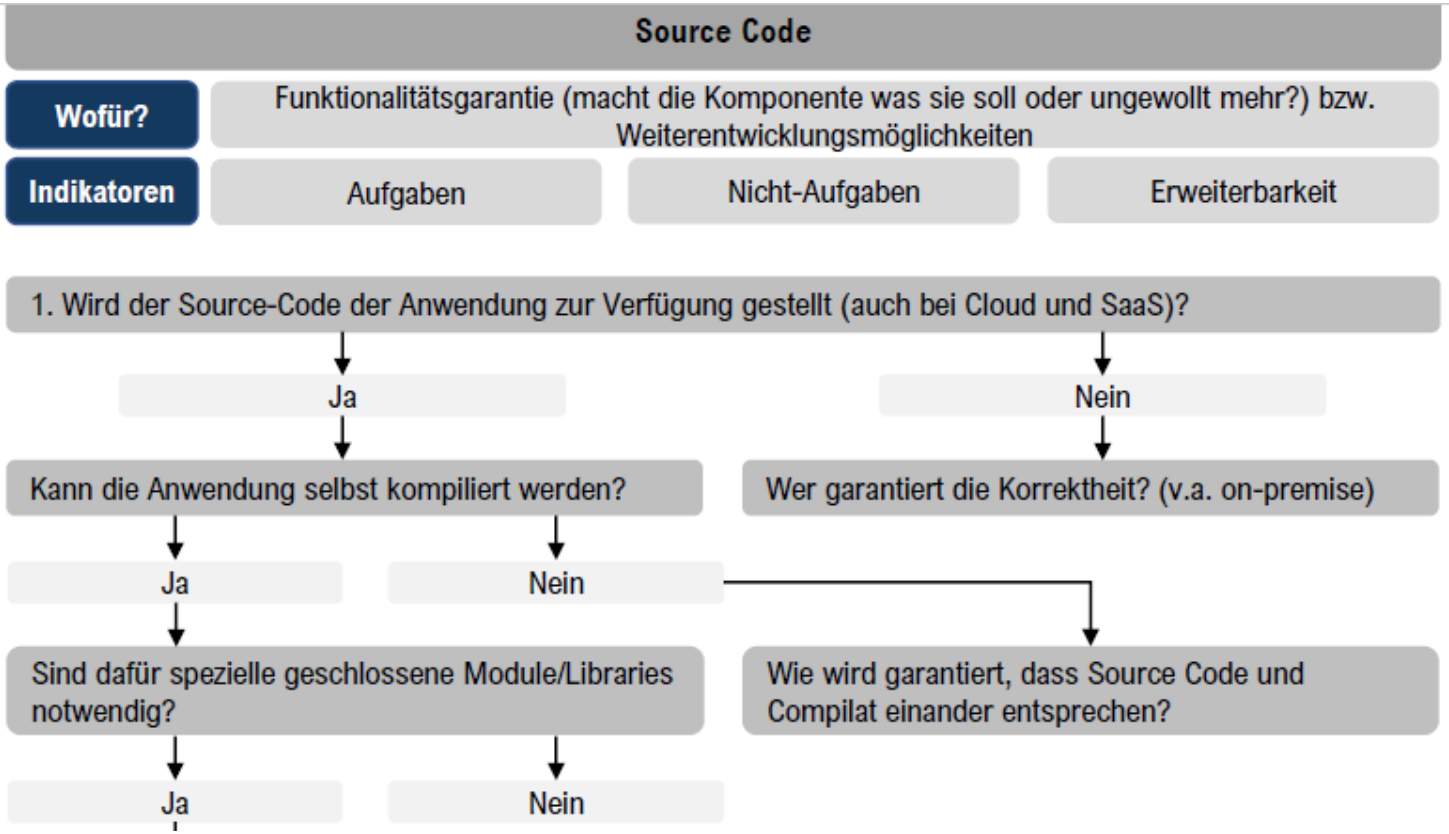
- Grundidee – AI ermöglicht viele neue Applikationen und Vorgangsweisen
  - Diese wiederum erzeugen neue Gefahren
  - Abschätzung von sicherheitskritischen Gaps alleine aus den Szenarien daher nicht sinnvoll
- Studie zu möglichen neuen Applikationen
  - Basierend auf treibenden Faktoren und Szenarien
  - Befragung externer und interner Expert*innen
  - Scoring in Bezug auf Relevanz für das BMLV
- Gap-Analyse
  - Welche sicherheitstechnischen Probleme entstehen durch die neuen Applikationen, aber auch den Einsatz von AI an sich.
  - Qualifizierung dieser Gaps
  - Scoring in Bezug auf (a) Applikations-Scoring und (b) genereller Gefahrenseinschätzung

Beschaffungsleitfaden AI

- **Ziel**: Unterstützung bei der Beschaffung
  - „Die Spreu vom Weizen trennen“
  - Wichtige sicherheitsrelevante Fragen aufwerfen

- **Nichtziele**:
  - Festzustellen, ob AI das richtige Werkzeug für die Lösung einer Fragestellung im BMLV ist.
  - Festzustellen, ob AI überhaupt eingesetzt werden soll und oder darf (bspw. aufgrund rechtlicher Vorbehalte).
  - Zu entscheiden, ob ein spezifisches Produkt ausreichend für den Zweck ist.
  - Zu entscheiden, welches Produkt das für ein Problem am besten geeignete ist.
- Das Resultat ist ein **lebendes Dokument**.

Beschaffungsleitfaden AI



Weitere (technische) Themen

- **Data Cleansing**
  - Vorverarbeitung der Daten, Behandlung von fehlerhaften und unvollständigen Daten
  - Problem des Erzeugens von Artefakten in den Daten, je nach Data Cleansing Strategy

- **AI Act**
  - Derzeit Draft-Status auf EU-Ebene
  - Zwar nicht grundsätzlich gültig für militärische AI, formt allerdings die Produktentwicklung im Allgemeinen

- **Penetration Testing AI**
  - Problem der fehlenden Explainability in vielen AI-Techniken
  - Testabdeckung, (autonome) Veränderlichkeit des Systems

Bundesministerium
Landwirtschaft, Regionen
und Tourismus

Kontakt

PL: Peter Kieseberg
Institut für IT Sicherheitsforschung
Fachhochschule St. Pölten
Peter.kieseberg@fhstp.ac.at

FFG
Forschung wirkt.

FORTE

Bundesministerium
Landesverteidigung