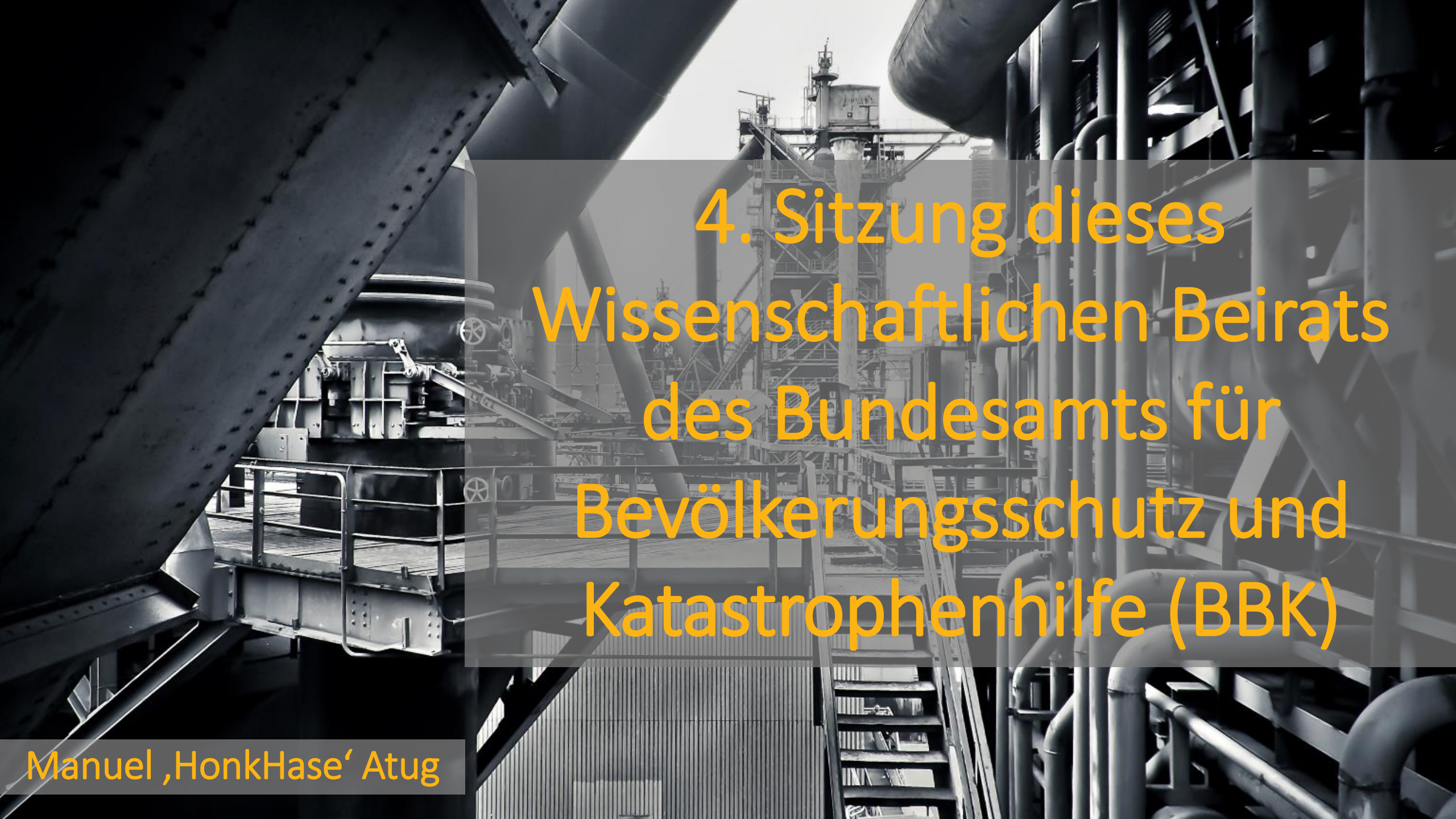


A black and white photograph of an industrial facility, likely a refinery or chemical plant. The image shows a complex network of large pipes, metal walkways with railings, and various industrial structures. In the foreground, a large, dark, riveted pipe curves diagonally across the frame. In the background, there are tall distillation columns and other processing units. The overall scene is industrial and technical.

4. Sitzung dieses Wissenschaftlichen Beirats des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Manuel „HonkHase“ Atug



KI und Zivile Verteidigung

Manuel „HonkHase“ Atug

Was ist KI?



- KI ist Software (und ganz viel Daten)
- Software kann man sicher entwickeln und betreiben. Oder eben auch nicht
- Software kann nicht denken

Wie nutze ich KI?



- Technologiehörigkeit vs Heilsversprechen
- Mittel zum Zweck vs Selbstzweck



Verlust der digitalen Souveränität über 3 Langzeit-Etappen



Hardware

- Speicherung der Daten
- Externe RZ Konzerne



Applikationen

- Verarbeitung der Daten
- Externe Cloud Konzerne



Daten

- Abgabe der Daten
- Externe KI Konzerne



Sicherer, robuster und nachvollziehbarer Einsatz von KI

- **Evasion/Adversarial Attacks**
Durch eine Manipulation von Eingabedaten verleiten Angreifer das KI-Modell im Betrieb zu vom Entwickler nicht vorgesehenen Ausgaben
- **Data Poisoning Attacks**
Manipulation der Trainingsdaten des KI-Modells, so dass dieses auf (bestimmte) Eingaben nicht wie vom Entwickler vorgesehen reagiert



Sicherer, robuster und nachvollziehbarer Einsatz von KI

- **Privacy-Attacks**

Angreifer extrahieren Informationen hinsichtlich der Trainingsdaten aus dem Modell

- **Model Stealing Attacks**

Angreifer extrahieren die Funktionalität des Modells



Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf

>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten
(z. B. Naturgefahren, technologische
Gefahren, etc.) im Rahmen des
Risiko- und Krisenmanagements“

** Hallo BBK*

Und was mache ich, wenn alles nichts hilft?



Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspfluecker.de

