

KI und Sicherung von Kernmaterial und nuklearen Anlagen

Sarah Case Lackner, Ph.D.
Senior Fellow, VCDNP

Sicherung $\neq$ Sicherheit

- Sicherheit schützt Menschen vor der Anlage — Sicherung schützt die Anlage vor Menschen
- 4 Funktionen: abschrecken · erkennen · verzögern · reagieren
- 2 Prinzipien: Defence in depth (mehrere unabhängige Schichten)
- Graded approach (Schutz auf das Wertvollste konzentrieren) Plus internationaler Rechtsrahmen + gelebte Sicherheitskultur
- Heute: nichtstaatliche Akteure · Fokus auf Anlagen
- *Der Rahmen wurde für Zäune, Wachen, Sensoren & Papier gebaut — jetzt kommt KI dazu.*

Kein Kraftwerk — trotzdem betroffen

- Österreich = keine kommerziellen KKW → das Thema ist trotzdem nicht abstrakt U
- Umgeben von nuklearen Anlagen
- Österreichs Sicherheit hängt an der Sicherung der Nachbarn — *der Standard in Prag & Bratislava schützt Wi*
- Grenzen halten nichts auf: Strahlung zieht mit dem Wind
- Es ist auch IHRE kritische Infrastruktur

Eingebaute KI — Chance und Einfallst

- Wird ernsthaft geprüft
- Chance (Betrieb): mehr Daten als ein Mensch → schnelleres, genaueres Bild (normal & abnormal), bessere vorausschauende Wart
- Gefahr: größere Angriffsfläche · Trennung innen/außen verschwimm Modelle täuschbar · Datensicherheit & Faktor Mensch
- *Sicherheit & Sicherung von Anfang an mitdenken — nicht vom „neuen Spielzeug“ überholen lassen.*

KI in der Anlage (1/4)

- Wird ernsthaft geprüft
- Chance (Betrieb): mehr Daten als ein Mensch → schnelleres, genaueres Bild (normal & abnormal), bessere vorausschauende Wartung
- Gefahr: größere Angriffsfläche · Trennung innen/außen verschwimmt · Modelle täuschbar · Datensicherheit & Faktor Mensch
- *Sicherheit & Sicherung von Anfang an mitdenken — nicht vom „neuen Spielzeug“ überholen lassen.*

KI bei böswilligen Akteuren (2/4)

- Frontier-Modelle: öffentliche Daten bündeln · Schlüsse ziehen · Muster, Lücken, Schwachstellen erkennen
- Viele Anlageninfos sind ohnehin schon öffentlich
- Kernpunkt: KI hebt weniger versierte Angreifer auf Spezialisten-Niveau (auch Lieferketten-Angriffe)
- Beobachtung: größter Sprung bei Zielauswahl & Angriffsplanung — beschleunigt bestehende Wege, ändert die *Art* (noch) nicht
- Open-Source-/Open-Weight-Modelle machen besonders Sorgen
- Empfehlung: Sicherung an ein *dynamisches* KI-Risiko anpassen — bewegliches Ziel



KI als Werkzeug für den Verteidiger (3/4)

- Viel kurzfristiger als KI im Betrieb/Safety (Letzteres noch weitgehend verboten)
- Schon im Einsatz: KI in Perimeterkameras & Überwachung in der Cyberabwehr (erkennt Eindringlinge/Anomalien schneller als ein Mensch)
- Tempo-Logik: Was dem Angreifer hilft, hilft auch uns → Maschine gegen Maschine
- Empfehlung: Behörden (national & international) sollten laufend aktuelle, praktische Leitlinien entwickeln & teilen

Das Problem einordnen (4/4)

- Cybersicherheit ist bereits in ALLE Bereiche der Sicherung eingewoben — KI treibt das weiter
- Sicherheit und Sicherung verschwimmen (dieselben vernetzten KI-Systeme tragen beide Risiken)
- Mein Ziel heute: das Problem benennen und Richtung anbieten — nicht abschließend lösen

Was Österreich tun kann

1. Sich Gehör verschaffen — lauter. Dieselbe starke Stimme wie bei Abrüstung & Nichtverbreitung.
2. Fachwissen aufbauen. Einfluss hängt von Wissen ab technisch und politisch.
3. KI auf der eigenen Seite nutzen — mit offenen Augen. Nationale Erkennung & Reaktion stärken.
4. Die Nachbarn beobachten. Neue KI in Anlagen? KI-Tools bei Mitarbeitern?

Danke

Thank you

Sarah Case Lackner, Ph.D.
Senior Fellow

scaselackner@vcdnp.org