

KI kann im Kampf gegen Desinformation helfen



Jacqueline Mayrdorfer und Jannik Steinwender vom Bundesverband Sicherheitspolitik an Hochschulen schildern hier, wie man sich mit Künstlicher Intelligenz (KI) gegen Operationen kognitiver Kriegsführung wehren kann.

Hybride Angriffe manifestieren sich alltäglich und in zahlreichen Formen. Ein wesentlicher Teil ausländischer Multi-Domain-Operationen ist kognitive Kriegsführung: Die Instrumentalisierung digitaler Plattformen zur gezielten Einflussnahme. Diese Kampagnen bedienen sich der Manipulation von Fakten, also der fehlerhaften Darstellung von Sachverhalten und der narrativen Steuerung durch die forcierte Verbreitung eigener Standpunkte.

Der heutige Informationsraum ist somit kein neutraler Ort mehr, sondern vielmehr ein umkämpftes Operationsgebiet, in dem rein manuelle Beobachtungen für ein belastbares Lagebild nicht mehr ausreichen. Desinformation kann sich durch globale Vernetzung und durch algorithmisch verstärkte Echokammern in Echtzeit nahezu ungehindert verbreiten. Hyperrealistische Deepfakes sowie die KI-gestützte Skalierung von Texten ermöglichen eine neue Qualität und Quantität von Desinformation, die von authentischem Content kaum noch zu unterscheiden ist. Psychologisch resultiert daraus eine Masse an Informationen, die die kognitive Belastung von Bevölkerung und Analysten erhöht und langfristig zu einer Erosion des gesellschaftlichen Vertrauens führt.

Europa verliert im heutigen Informationsraum zunehmend die Oberhand: Desinformationskampagnen werden aufgrund Personalmangels, fehlender Zuständigkeiten oder ineffizienter Kommunikationswege meist zu spät oder gar nicht aufgearbeitet. Hier setzen spezialisierte KI-Plattformen an. Sie schaffen mit gezielter Suche und Monitoring die Basis für ein erschöpfendes Lagebild. In der



Der Informationsraum ist umkämpft.

Weiterverarbeitung unterstützt KI-gestützte Gesichts-, Objekt- und Texterkennung dabei, die schiere Datenmenge effizient zu bewältigen und den personellen sowie zeitlichen Aufwand erheblich zu reduzieren. Während Längsschnittanalysen Trends in der Prävalenz (statistisches Maß für die Häufigkeit an einem bestimmten Zeitpunkt) ausgewählter Narrative sichtbar machen, verdeutlichen Netzwerkgraphen die Beziehungen zwischen Akteuren und Ereignissen. Softwaregestützte KI-Systeme ermöglichen die (teil)automatisierte Erstellung von Berichten nach analytischen Standards.

Da Desinformation nur selten an der Quelle gestoppt werden kann, ist die fachliche Einordnung für und durch Medien und Institutionen entscheidend. Einerseits dienen sie der Aufklärung von Falschinformationen, die die traditionelle mediale Berichterstattung behindern und diskreditieren. Andererseits ermöglichen sie es, Desinformation zum Gegenstand der Berichterstattung zu machen und die Bevölkerung präventiv aufzuklären. Desinformationskampagnen in der Wählerschaft können das Vertrauen in demokratisch gewählte Vertreter unterminieren. Werden solche Kampagnen frühzeitig identifiziert und aufgearbeitet, können politische Akteure gezielter auf Sorgen und Stimmungen reagieren. Für Institutionen wie Behörden oder Ministerien bilden diese Analysen zudem eine

zentrale Grundlage für politische Bildung und den Aufbau gesellschaftlicher Resilienz. Trotz dieser Potenziale wird die KI-gestützte Aufarbeitung von Desinformation durch strukturelle Hürden begrenzt. Häufig darf Wissen aufgrund rechtlicher Rahmenbedingungen, vertraglicher Vorgaben oder Quellenschutzes nicht an Dritte oder die Öffentlichkeit weitergegeben werden. Andererseits bedürfen diese KI-Tools gezielter Schulungen und Einarbeitungszeiten, für die oft keine Zeit vorgesehen ist. Häufig werden Daten auch mehrfach erhoben, jedoch isoliert voneinander verarbeitet. Es entstehen fragmentierte Netzwerke, die Doppelarbeit erzeugen, die Umsetzung von Erkenntnissen in konkrete Handlungen verlangsamen und strategische Aussagen sowie Attributionen verwässern. Ein effektiveres Teilen von Analyseergebnissen, eine engere Zusammenarbeit der relevanten militärischen, zivilen und behördlichen Bedarfsträger und ein agiler Umgang mit neuen Technologien ist hier vonnöten, um einen entscheidenden Vorsprung gegenüber kognitiver Kriegsführung zu gewinnen.

Jacqueline Mayrdorfer/Jannik Steinwender

Jacqueline Mayrdorfer studiert im letzten Semester „International Relations and Management“ an der OTH Regensburg und legt hier ihren Schwerpunkt auf Intelligence Studies sowie Schnittstellenmanagement öffentlicher Bedarfsträger. Parallel dazu ist sie bei einem Softwareanbieter im Bereich Open Source Intelligence (OSINT) tätig, wo sie praktische Erfahrungen an der Schnittstelle zwischen Technologie und Sicherheitsbehörden sammelt.

Jannik Steinwender promoviert im Themengebiet der hybriden Angriffe an der Professur für Internationale Politik und transatlantische Beziehungen. Das Hauptaugenmerk seiner Arbeit liegt hierbei auf russischer Cognitive Warfare und Spionage.