

## **Kleine Anfrage**

**der Abgeordneten Andrej Hunko, Heike Hänsel, Anke Domscheit-Berg, Niema Movassat, Thomas Nord, Petra Pau, Tobias Pflüger, Martina Renner, Dr. Kirsten Tackmann, Alexander Ulrich, Kathrin Vogler und der Fraktion DIE LINKE.**

### **Software zur Erkennung von „Radikalisierung“ und „Krisen“**

Das Bundesministerium der Verteidigung (BMVg) testet die Software „IBM Watson“, um durch semantische Analyse großer Datenmengen die Lagedarstellung von krisenhaften Entwicklungen zu unterstützen (Bundestagsdrucksache 19/3459). Die Tests erfolgen im Rahmen der Studie „IT-Unterstützung Krisenfrüherkennung“, in der das Bundesministerium nach einer Softwarelösung sucht, die zukünftig „bei der Vorhersage von Krisen helfen soll“. Die Software gibt dabei „prädiktive Hinweise“, als „Prognosehorizont“ gibt das BMVg einen Zeitraum von sechs bis 18 Monaten an. „IBM Watson“ verarbeitet sogenannte strukturierte und unstrukturierte Daten aus öffentlichen, offenen und als Verschlussachen eingestufte Quellen. Neben Inhalten aus öffentlich und nicht öffentlich zugänglichen Internetforen werden auch sogenannte Ereignisdatenbanken mit Archiven zu politischen Vorkommnissen und Protesten angebunden. Das BMVg nennt hierzu die Plattformen „Armed Conflict Location & Event Data“ (ACLED), „Global Database of Events, Language, and Tone“ (GDELT) und „Global Terrorism Database“ (GTD). Sie sollen durch die Universität der Bundeswehr München im Hinblick auf ihre Zuverlässigkeit evaluiert werden. Alle drei Monate tagt eine Arbeitsgruppe „Krisenfrüherkennung“ der Bundesregierung, die ein zentrales Instrument der „ressortübergreifenden Krisenfrüherkennung“ ist (Antwort der Bundesregierung auf die Schriftliche Frage 24 des Abgeordneten Ottmar von Holtz auf Bundestagsdrucksache 19/5643). Einige der beteiligten Ressorts entwickeln bzw. nutzen computergestützte „Instrumente, deren Ergebnisse in die genannte Ressortzusammenarbeit einfließen“.

Neben der „Krisenfrüherkennung“ werden Informationen aus Internetforen oder Sozialen Medien auch zum Aufspüren von „Radikalisierung“ genutzt. Die Europäische Union finanziert hierzu das Projekt „Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization“, das von der spanischen Firma Insikt Intelligence durchgeführt wird (<http://gleft.de/2Ay>). Das Erkennen von „Cyberpropaganda“ soll die Prädiktion von unerwünschten Ereignissen ermöglichen. Die Software soll außerdem „radikale Inhalte“, „verdächtige Nachrichten“ und „verdeckte „Radikalisierungsprozesse“ erkennen. Vier europäische Strafverfolgungsbehörden sollen bis 2019 ein zu entwickelndes Produkt testen. Eine von der Firma online gestellte Beschreibung ihrer „Aufklärungsplattform“ beschreibt ihre Wirkungsweise beim Aufspüren von „jihadistischen Prozessen“ (<http://gleft.de/2Ax>). Die EU-Kommission finanziert außerdem das Projekt „RED-Alert“, das ebenfalls Soziale Medien auswertet (<http://gleft.de/2Aw>). Genannt werden auch „neue Kanäle wie Telegram und Periscope“, die demnach in

der „Terrorgemeinde“ eine größere Bedeutung erlangen. Auch „Red-Alert“ wird von Strafverfolgungsbehörden getestet (<http://gleft.de/2Av>). Die EU-Kommission hat jetzt weitere 5 Mio. Euro aus dem Fonds für Innere Sicherheit (ISF) für Projekte gegen „Radikalisierung“ aufgelegt (<http://gleft.de/2At>).

Wir fragen die Bundesregierung:

1. Welche Ressorts der Bundesregierung entwickeln bzw. nutzen computergestützte Instrumente zur „Krisenfrüherkennung“, deren Ergebnisse in die genannte Ressortzusammenarbeit einfließen (Antwort auf die Schriftliche Frage 24 des Abgeordneten Ottmar von Holtz auf Bundestagsdrucksache 19/5643), und um welche Produkte welcher Hersteller handelt es sich dabei?
  - a) Wann endet der Studienvertrag „IT-Unterstützung Krisenfrüherkennung“ zum Test der Software „IBM Watson“ für die semantische Analyse von Quelldaten und Lagedarstellung beim Bundesministerium der Verteidigung (Bundestagsdrucksache 19/3459, Antwort zu Frage 10)?
  - b) Welche strukturierten und unstrukturierten Daten aus öffentlichen, offenen und als Verschlussachen eingestuften Quellen werden mit der Software „IBM Watson“ verarbeitet?
  - c) Welche Erläuterungen kann die Bundesregierung zur Anbindung von „IBM Watson“ an die Ereignisdatenbanken „Armed Conflict Location & Event Data“ (ACLED), „Global Database of Events, Language, and Tone“ (GDELT) und „Global Terrorism Database“ (GTD) machen, und in welchem Umfang werden dort vorgehaltene Informationen genutzt?
  - d) Wie zuverlässig sind die Datenbanken nach gegenwärtigem Stand?
  - e) Welche Kosten entstanden für die Forschungs- und Technologiestudie, und wie werden diese übernommen?
2. Auf welcher gesetzlichen Grundlage nutzt die Bundeswehr eine Software zur Krisenfrüherkennung bzw. plant eine entsprechende Nutzung?
3. Worum handelt es sich nach Kenntnis der Bundesregierung bei „technisch-operativen Übungen“ mit dem Titel „DEFNET“ (Ratsdokument 14413/18), die laut des aktualisierten EU-Politikrahmens für die Cyberabwehr vom Europäischen Auswärtigen Dienst, der Verteidigungsagentur und Mitgliedstaaten durchgeführt werden sollen, und welche Szenarien wurden und werden bei den Übungen geprobt?
4. Was ist der Bundesregierung über neue EU-Projekte der DG NEAR im Bereich Cybersicherheit für die Staaten der östlichen Nachbarschaft bekannt, und welche Gelder werden dafür an interessierte Durchführungsorganisationen vergeben?
  - a) Welche Ziele werden dabei verfolgt, und welche Länder sollen gefördert werden?
  - b) Sofern auch die Implementierung der Budapest Convention von den Projekten abgedeckt werden soll, welche Rolle wird dabei der Europarat übernehmen?
  - c) Wann soll nach Kenntnis der Bundesregierung eine Ausschreibung für die Projekte erfolgen?
5. Welche Produkte wurden in der vom Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen (FhI INT) für die für die Bundesregierung durchgeführte Studie „Einsatz kognitiver Systeme“ zur theoretischen und technischen Untersuchung der Anwendung Kognitiver Systeme in der Trendanalyse (Bundestagsdrucksache 19/3459, Antwort zu Frage 2) betrachtet?

6. Welche Schlussfolgerungen zieht die Bundesregierung aus der vom Fraunhofer-Institut FKIE durchgeführten Studie „Information Retrieval – Fake News“ zur Untersuchung der automatisierten Erkennung von „Fake News“ (Bundestagsdrucksache 19/3459, Antwort zu Frage 2)?
7. Welche Schlussfolgerungen zieht die Bundesregierung aus der von der Bundeswehr-Universität in München durchgeführten Studie „Automatisierte Beobachtung von Internetinhalten“, die am Beispiel Twitter einen Fokus auf die „Vernetzung zwischen Ereignissen aus der realen Welt und ihrer Resonanz im Internet“ legt (Bundestagsdrucksache 19/3459, Antwort zu Frage 2)?
8. Welche Schlussfolgerungen zieht die Bundesregierung aus den 2017 von der Beraterfirma IABG beendeten Studien „IT-Unterstützung Krisenfrüherkennung“ und „Bearbeitung der Lage im Informationsumfeld“ (Bundestagsdrucksache 19/3459, Antwort zu Frage 8)?
  - a) Welche technischen Verfahren oder Produkte wurden in den Studien untersucht?
  - b) Welche Handlungsempfehlungen geben die Studien?
9. Welche weiteren Firmen nehmen nach Kenntnis der Bundesregierung derzeit am „EU Internet Forum“ zur Erkennung und Entfernung von unerwünschten Internetinhalten teil, wozu den Fragestellerinnen und Fragestellern derzeit Facebook, Google/Youtube, Microsoft, Twitter, Internet Archive, Justpaste.it, Wordpress, SNAP, Soundcloud, Yellow, Baaz, Dropbox, Mega, Userscloud und Telegram bekannt sind, es sich laut der Bundesregierung aber um „etwa 20 Unternehmen“ handeln soll (Bundestagsdrucksache 19/5731, Antwort zu Frage 12)?
10. Was ist der Bundesregierung über Vorschläge für eine erweiterte „EU-Meldeplattform“ zur Verhinderung der Verbreitung terroristischer Onlineinhalte bekannt, die nach Kenntnis der Fragestellerinnen und Fragesteller eine automatische Erkennung bereits hinterlegter Inhalte gewährleisten und über einen „privilegierten Kanal“ zu den Internetanbietern verfügen soll?
  - a) Welche Haltung vertritt die Bundesregierung zur Notwendigkeit einer solchen Meldeplattform?
  - b) Wie sollte die Plattform mit widersprüchlichen Entfernungsanordnungen umgehen, etwa wenn Strafverfolgungsbehörden oder Geheimdienste verlangen, dass eine Internetpräsenz nicht gelöscht wird, da diese beobachtet wird?
  - c) Inwiefern sollte eine solche Plattform aus Sicht der Bundesregierung auch automatisiert im Internet nach inkriminierten Inhalten suchen?
11. Was ist der Bundesregierung nach dem EU-US-Ministertreffen für die Bereiche Inneres und Justiz am 8. und 9. November 2018 in Washington darüber bekannt, inwiefern bzw. auf welche Weise die USA und die EU gemeinsam gegen die Beseitigung von Terrorpropaganda im Internet vorgehen wollen und welche US-Behörden sich hierzu einbringen wollen?

12. Wann soll die Europäische Kommission nach Kenntnis der Bundesregierung ein Mandat erhalten, um die Beratung und mögliche Verhandlung mit den USA über eine Regierungsvereinbarung nach dem sogenannten CLOUD-Act (Clarifying Lawful Overseas Use of Data Act) zu beginnen und eine gegenseitige Anforderung von elektronischen Beweismitteln zu regeln, damit Herausgabeverlangen von Behörden der EU-Mitgliedstaaten gegenüber Firmen in den USA erleichtert werden?
  - a) Was ist der Bundesregierung darüber bekannt, wann die EU-Kommission die Mandatsentwürfe für die Verhandlung eines Abkommens zwischen der EU und den USA zur Vereinfachung des Zugangs zu elektronischen Beweismitteln sowie zum zweiten Zusatzprotokoll zur Budapest Konvention des Europarats vorlegen will?
  - b) Sofern hierzu noch kein Zeitpunkt bekannt ist, aus welchen Gründen verzögert sich dies nach Kenntnis der Bundesregierung?
13. Mit welchem Personal nahm die Bundesregierung an der Second High-level Conference on Aviation Security der ICAO am 29. und 30. November 2018 in Montréal teil?
  - a) Wie wird die Bundesregierung die dort verabschiedeten Empfehlungen umsetzen, einen gemeinsamen Standard für den Austausch und die Verarbeitung von Passagierdaten zu entwickeln (<http://gleft.de/2Bl>)?
  - b) Welche Software nutzt das Bundeskriminalamt zur Auswertung bzw. zum Profiling von Passagierdaten in der deutschen PNR-Zentralstelle, bzw. welche Software soll hierzu beschafft werden?
14. In welchen Projekten des Sicherheitsforschungsprogramms der Europäischen Union zur Überwachung und Kontrolle an Flughäfen, an denen deutsche Behörden, Firmen oder sonstigen Einrichtungen teilnehmen, wird nach Kenntnis der Bundesregierung auch zum Einsatz von Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen geforscht (Bundestagsdrucksache 18/11952, Antwort zu Frage 1)?
  - a) Welche der im Sicherheitsforschungsprogramm der Europäischen Union geförderten Projekte, die Aspekte einer Risiko- bzw. Verhaltensanalyse von Reisenden aufweisen, forschen auch zu Künstlicher Intelligenz bzw. maschinellem Lernen?
  - b) Welche der im Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit“ beforschten Anwendungen zur „Stärkung bzw. Automatisierung der Luftsicherheitskontrollen“ sollen Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen beinhalten?
15. Inwiefern hat die Bundesregierung mittlerweile eine „generelle Position“ zur computergestützten Auswertung von Sozialen Medien (darunter Twitter, Facebook) erarbeitet (Bundestagsdrucksache 19/3459, Antwort zu Frage 19), und worin besteht diese?
16. Was ist der Bundesregierung über Forschungen der Europäischen Kommission zur „Krisenfrüherkennung“ und zum Aufspüren von „Radikalisierung“ bekannt ([www.woz.ch/-86ae](http://www.woz.ch/-86ae)), und an welchen dieser Projekte sind deutsche Einrichtungen beteiligt?
17. Welche Software nutzen Bundesbehörden zum Aufspüren „extremistischer Ideologien“ oder „Radikalisierungsprozesse“ im Internet (auch sogenannte Bottom-Up-Radikalisierung), und welche Tests oder Studien werden hierzu durchgeführt?

18. Welche Zielsetzung verfolgt das Verbundprojekt „X-SONAR“, mit dem das Bundesministerium für Bildung und Forschung „extremistische Interaktions- und Eskalationsdynamiken in sozialen Onlinenetzen“ erkennen und verstehen will ([www.x-sonar.de](http://www.x-sonar.de))?
- a) Welche „Radikalisierungsprozesse“ welcher Strömungen bzw. welche „Formierung neuer radikaler Gruppen“ soll die Anwendung vorrangig erkennen?
  - b) Welche Angaben soll die in „X-SONAR“ bzw. der dort beforschten Anwendung erstellte Gefährdungsbewertung enthalten?
  - c) Auf welche Weise sollen entsprechende Inhalte im Internet von der Anwendung gefunden werden?
  - d) In welchen Bereichen wird zur Risikoeinschätzung und Gewaltprävention in „X-SONAR“ auch zum Einsatz von Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen geforscht?
  - e) Mit welchen „Endnutzern aus Sicherheitsbehörden“ wollen die Projektbeteiligten ihr „softwaregestütztes Instrument für das Bedrohungsmanagement und [...] Gefährdungsbewertung innerhalb virtueller Kontexte“ zusammen entwickeln bzw. testen (bitte etwaige beteiligte Landeskriminalämter auflühren)?
  - f) Welchen Beitrag erbringt die Deutsche Hochschule der Polizei in „X-SONAR“?
  - g) Wann und wo sollen die Tests nach gegenwärtigem Stand erfolgen?

Berlin, den 13. Dezember 2018

**Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion**





