Deutscher Bundestag **Drucksache 19/7604**

19. Wahlperiode 11.02.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/6981 –

Software zur Erkennung von „Radikalisierung“ und „Krisen“

Vorbemerkung der Fragesteller

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 Verschlusssachen 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 „Aufklä-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 7. Februar 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

rungsplattform“ 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).

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?

Gegenwärtig entwickeln bzw. nutzen das Auswärtige Amt (AA) und das Bundesministerium der Verteidigung Ergebnisse, die aus verschiedenen softwarebasierten Instrumenten zur Unterstützung des betreffenden Fachpersonals bei der Aufgabenwahrnehmung „Krisenfrüherkennung“ gewonnen werden und die auch in die ressortgemeinsame Zusammenarbeit einfließen.

Hierbei arbeitet das BMVg mit der Firma IBM als Auftragnehmer zusammen, die ihre Leistungen unter Rückgriff auf die Produktfamilie „IBM Watson“ erbringen.

Das AA greift in diesem Zusammenhang zurück auf

- die Datenbanksysteme „Sybase“ und „HANA“, das Datenverwaltungssystem „Data Services“ und die Softwaresuites „BI Platform“, „Lumira“, „Design Studio“ und „Predictive Analytics Suite“ (Hersteller: SAP),
- das Visualisierungs- und Analysetool goOSE (Hersteller: data42),
- ein Volltextsuchspeichersystem (Hersteller noch in Evaluation),
- die quelloffenen Programmiersprachen R und Python,
- die quelloffene Sprachanalysesoftware Stanford CoreNLP,
- das kommerzielle Geoinformationssystem ArcGIS (Hersteller: Esri).

a) Wann endet der Studienvertrag „IT-Unterstützung Krisenfrüherkennung“ zum Test der Software „IBM Watson“ für die semantische Analyse von Quellendaten und Lagedarstellung beim Bundesministerium der Verteidigung (Bundestagsdrucksache 19/3459, Antwort zu Frage 10)?

Der aktuelle Studienvertrag endet am 30. Juni 2019.

b) Welche strukturierten und unstrukturierten Daten aus öffentlichen, offenen und als Verschlusssachen eingestuften Quellen werden mit der Software „IBM Watson“ verarbeitet?

Derzeit werden im Rahmen der Studie nur öffentliche Datenquellen verwendet. Hierbei sind sowohl verschiedene unstrukturierte Nachrichtenquellen angebunden, z. B. AllAfrica Latest News, Small Wars Journal, als auch strukturierte Datenquellen, z. B. Ereignisdaten aus der Datenbank „Armed Conflict Location & Event Data“ (ACLED), strukturelle Daten z. B. der Weltbank sowie Grid-Daten z. B. des Deutschen Wetterdienstes. Aktuell befindet sich die IT-Unterstützung

„Krisenfrüherkennung“ im Akkreditierungsverfahren. Bis die Akkreditierung abgeschlossen ist, dürfen keine als Verschlusssachen eingestuften Daten verwendet werden. Nach erfolgter Akkreditierung sollen zusätzlich Daten des Militärischen Nachrichtenwesens der Bundeswehr verarbeitet werden.

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?

Die angeführten Datenbanken sind automatisiert an „IBM Watson“ angebunden. Die dort verfügbaren Datensätze werden ausgelesen und im Anschluss durch die IT-Unterstützung „Krisenfrüherkennung“ für eine weitere Nutzung und Analyse durch das Fachpersonal für Krisenfrüherkennung im BMVg strukturiert und aufbereitet.

d) Wie zuverlässig sind die Datenbanken nach gegenwärtigem Stand?

Die genannten Datenbanken sind das Ergebnis wissenschaftlicher Forschungen und öffentlich verfügbar. Alle aktuell angeschlossenen Quellen werden regelmäßig auch auf ihre Zuverlässigkeit hin überprüft und evaluiert. Nach derzeitiger Bewertung sind die angeschlossenen Quellen grundsätzlich zuverlässig und eignen sich für die weitere zielgerichtete Nutzung im Rahmen der Aufgabenwahrnehmung „Krisenfrüherkennung“.

e) Welche Kosten entstanden für die Forschungs- und Technologiestudie, und wie werden diese übernommen?

Die Forschungs- und Technologiestudien „IT-Unterstützung Krisenfrüherkennung“ in Zusammenarbeit mit der Firma IBM werden bis zum 30. Juni 2019 Kosten in Höhe von rd. 15,1 Mio. Euro verursacht haben. Die Finanzmittel hierfür werden dem Einzelplan 14 entnommen.

2. Auf welcher gesetzlichen Grundlage nutzt die Bundeswehr eine Software zur Krisenfrüherkennung bzw. plant eine entsprechende Nutzung?

Die Krisenfrüherkennung ist Teil des verfassungsrechtlichen Auftrags der Streitkräfte gemäß Artikel 87a des Grundgesetzes. Dies umfasst auch die Nutzung von IT-Unterstützung. Wie bei jedem Vorgehen der Streitkräfte auf dieser Grundlage, können sich im Einzelfall weitere Vorgaben aus den verfassungsrechtlichen Rahmenbedingungen für die Auftragserfüllung der Streitkräfte, dem Völkerrecht, dem Europarecht und aus einfachgesetzlichen Regelungen, insbesondere dem Datenschutzrecht, ergeben.

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 Mitgliederstaaten durchgeführt werden sollen, und welche Szenarien wurden und werden bei den Übungen geprobt?

Der Bundesregierung liegen keine Erkenntnisse vor.

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?

Mit einigen Staaten der östlichen Nachbarschaft ist bei der EU-Kommission (DG NEAR) ein Projekt zur Cybersicherheit und Cyberkriminalität (EU4Digital: Improving Cyber Resilience in the Eastern Partnership countries) in Entwicklung.

a) Welche Ziele werden dabei verfolgt, und welche Länder sollen gefördert werden?

Dieses Programm zielt auf die Verbesserung der Resilienz hinsichtlich Cybersicherheit und Cyberkriminalität durch Unterstützung entsprechenden Kapazitätsaufbaus in den geförderten Ländern. Geförderte Länder sind Armenien, Aserbaidschan, Weißrussland, Georgien, Moldau und Ukraine.

b) Sofern auch die Implementierung der Budapest Convention von den Projekten abgedeckt werden soll, welche Rolle wird dabei der Europarat übernehmen?

Die Budapest Convention stellt für das Projekt der DG NEAR die Benchmark dar. Zu einer Einbindung des Europarates liegen keine Erkenntnisse vor.

c) Wann soll nach Kenntnis der Bundesregierung eine Ausschreibung für die Projekte erfolgen?

Der Bundesregierung liegen keine Erkenntnisse vor.

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?

Vom Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen (INT) wurden im Jahr 2015 drei Produkte hinsichtlich der Eignung zur Technologievorausschau betrachtet. Diese waren das System SCAI-VIEW des Fraunhofer SCAI, das webbasierte Analysetool MAPEGY.RADAR der Firma Mapegy und die Software WATSON EXPLORER der Firma IBM.

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)?

Das Studienergebnis zeigt auf, dass eine automatisierte Erkennung von „Fake News“ mit den derzeitigen wissenschaftlichen Ansätzen zurzeit nicht zuverlässig möglich ist.

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)?

Gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) wird die Antwort zu dieser Frage mit dem VS-Grad „VS – Geheim“ eingestuft und an die Geheimschutzstelle des Deutschen Bundestages gesondert übermittelt.*

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)?

Die aus der Studie „Bearbeitung der Lage im Informationsumfeld“ abgeleiteten Handlungsempfehlungen fließen gegenwärtig in den Beschaffungsprozess einer Analyse- und Bewertungsausstattung für den Aufgabenbereich Operative Kommunikation ein. In Hinblick auf die „IT-Unterstützung Krisenfrüherkennung“ liegt dagegen keine im Jahr 2017 beendete Studie der Firma IABG vor.

a) Welche technischen Verfahren oder Produkte wurden in den Studien untersucht?

Im Rahmen der Studie „Bearbeitung der Lage im Informationsumfeld“ wurde der Einsatz eines Sharepoint-Portals untersucht, um das kollaborative Arbeiten zu verbessern. Des Weiteren wurde der Einsatz der Tools „Brandwatch“ und „Textrapic“ untersucht, um den semiautomatisierten Analyseprozess, in Unterstützung der Analysten, zu beschleunigen und qualitativ zu verbessern.

b) Welche Handlungsempfehlungen geben die Studien?

Aus der Studie „Bearbeitung der Lage im Informationsumfeld“ resultieren Handlungsempfehlungen, die der Weiterentwicklung des Prozesses „Bearbeitung der Lage im Informationsumfeld“ dienen.

Im Schwerpunkt werden Empfehlungen abgegeben

- zur Frage, wie der Analyseprozess semiautomatisiert grundsätzlich ablaufen sollte, um valide Ergebnisse zu generieren;
- zu erforderlichen technischen Voraussetzungen und möglichen Lösungen im Zentrum Operative Kommunikation der Bundeswehr, um den Analyseprozess im Tagesdienst und bei Bedarf schichtfähig umsetzen zu können;
- zu erforderlichen Qualifikationen des eingesetzten Personals;
- zum Umgang mit Schnittstellen zu anderen Bedarfsträgern.

* Das Bundesministerium der Verteidigung hat die Antwort als „Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

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)?

Das EU Internet Forum ist eine Veranstaltungsreihe der Europäischen Kommission. Die in der Antwort zu den Fragen 12 und 12a auf Bundestagsdrucksache 19/5252 genannte Zahl von etwa 20 Unternehmen bezieht sich auf die Angaben der Europäischen Kommission in ihrem Dokument SWD (2018) 408 final, S. 135. Weitere Details sind der Bundesregierung nicht bekannt.

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?

Die Fragen 10 bis 10c werden gemeinsam beantwortet.

Die Europäische Kommission (Dok. E-000025/2018 Antwort von Herrn Avramopoulos im Namen der Kommission) nahm zu Plattformen, die zur Verhinderung der Verbreitung terroristischer Inhalte seitens Europol aktuell genutzt werden können, am 30. März 2018 Stellung. Im Zuge dieses Legislativvorschlages wird auch eine mögliche zukünftige Rolle Europols erörtert. Angesichts der bereits bestehenden Prozesse und Strukturen sind diese Erörterungen aus Sicht der Bundesregierung wichtig. Die konkrete Rolle Europols hängt mithin maßgeblich vom Ergebnis des Gesetzgebungsprozesses ab.

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?

Die österreichische EU-Ratspräsidentschaft berichtete im Rahmen der Sitzung des JI-Rates am 6./7. Dezember 2018 zum Austausch mit den USA im Rahmen des Ministertreffens. Der Bundesregierung liegen keine Kenntnisse vor, die über die zum Ministertreffen am 9. November 2018 veröffentlichte Pressemeldung des Rates der Europäischen Union hinausgehen.

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?

Die Fragen 12 bis 12b werden gemeinsam beantwortet.

Zur Beantwortung der Fragen wird auf den Bericht der Bundesregierung an den Ausschuss für Inneres und Heimat des Deutschen Bundestages zu den Auswirkungen des CLOUD Act auf den Einsatz von US-Online-Diensten in Europa mit Blick auf die europäische Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) und Privacy-Shield sowie zur E-evidence-Initiative der EU-Kommission verwiesen. Wie bereits in diesem Bericht ausgeführt, hat die Kommission angekündigt, in Kürze Mandatsentwürfe vorzulegen und sich von den Mitgliedstaaten zu einer Verhandlungsführung mandatieren zu lassen.

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?

Die Bundesregierung nahm durch die Ratsvertretung des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) bei der Internationalen Zivilluftfahrtorganisation sowie durch einen Vertreter des BMVI 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)?

Die Bundesregierung wird in den einschlägigen Gremien der Internationalen Zivilluftfahrtorganisation mitarbeiten, in denen die Empfehlung hinsichtlich der Schaffung eines PNR-Standards beraten werden wird.

    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?

Aktuell werden die Fluggastdaten gemäß § 4 Absatz 2 Nummer 1 des Fluggastdatengesetzes (FlugDaG) automatisiert mit dem zentralen Fahndungsbestand im Informationssystem der Polizei und dem Schengener Informationssystem abgeglichen. Derzeit erfolgt kein Einsatz von kommerzieller Software zur Auswertung bzw. qualitativen Analyse von Fluggastdaten. Bislang gibt es auch keine konkreten Planungen in Bezug auf die Beschaffung von entsprechender Software.

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)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

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?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

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?

Im Rahmen des Programms „Forschung für die zivile Sicherheit“ werden derzeit keine Vorhaben zur „Stärkung bzw. Automatisierung der Luftsicherheitskontrollen“ gefördert, die sich mit Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen beschäftigen.

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?

Der Geschäftsbereich des BMVg nutzt eine entsprechende Software zur Erweiterung des nationalen Presselagebildes um den Bereich Soziale Medien sowie zur Analyse des Informationsumfeldes gemäß dem Interessenprofil BMVg/Bundeswehr. Weitere Erkenntnisse aus anderen Ressorts konnten nicht gewonnen werden. Das AA hat für seine strategischen Kommunikationsbedarfe erste Überlegungen zum Erkennen von deutsche Außenpolitik betreffenden Desinformationen und Kampagnendynamiken in den sozialen Medien angestellt. Diese könnten in Zukunft auch die datenschutzkonforme computergestützte Auswertung von sozialen Medien umfassen.

16. Was ist der Bundesregierung über Forschungen der Europäischen Kommission zur „Krisenfrüherkennung“ und zum Aufspüren von „Radikalisierung“ bekannt (www.woz.ch/-86ae), und an welchen dieser Projekte sind deutsche Einrichtungen beteiligt?

Der Bundesregierung sind zwei Forschungsvorhaben der Europäischen Kommission zur „Krisenfrüherkennung“ bekannt: einerseits der GCRI (Global Conflict Risk Index) des Joint Research Centre of the European Commission (http://conflictrisk.jrc.ec.europa.eu/), andererseits das Projekt EU-LISTCO (Limited Statehood and Contested Orders, www.eu-listco.net/), das von der EU im Rahmen ihres Programms „Horizon 2020“ gefördert wird. Für Work Package 2 dieses Projekts („Risk scanning and foresight for strategic policy design“) ist das AA Praxispartner.

Zudem werden im Sicherheitsforschungsprogramm der Europäischen Union (Bereich „Sicherheit“ im 7. Forschungsrahmenprogramm und Bereich „Sichere Gesellschaften“ in „Horizon 2020“) gegenwärtig folgende Projekte gefördert, die einen Bezug zu den genannten Schwerpunkten aufweisen:

Akronym	**Titel**	**Projektnummer**
RED-Alert	Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing	740688
INSIKT	Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization	767542
PROPHETS	Preventing Radicalisation Online through the Proliferation of Harmonised Toolkits	786894
DANTE	Detecting and Analysing Terrorist-related Online Contents and Financing Activities	700367
TENSOR	Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition	700024
EWISA	Early Warning for Increased Situational Awareness	608174
COPKIT	Technology, Training and Knowledge for Early-Warning/Early-Action led Policing in Fighting Organised Crime and Terrorism	786687

An folgenden in der Antwort zu dieser Frage aufgeführten Projekten des Sicherheitsforschungsprogrammes der Europäischen Union nehmen deutsche Behörden, Firmen oder sonstige Einrichtungen teil:

Akronym	**Teilnehmer aus Deutschland**
PROPHETS	• Bayerisches Staatsministerium des Innern • Hochschule für den öffentlichen Dienst in Bayern • Freie Universität Berlin
DANTE	• PROMT GmbH
TENSOR	• Cybercrime Research Institute GmbH • Hochschule für den öffentlichen Dienst in Bayern
COPKIT	• Hochschule für den öffentlichen Dienst in Bayern

Das Bundeskriminalamt ist zudem assoziierter Partner im Projekt PANDORA der Universität Marburg.

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?

Derzeit ist das Bundeskriminalamt mit zwei Projekten befasst, die sich mit dem Monitoring und der Untersuchung von Radikalisierungsprozessen im Internet auseinandersetzen. Ziel des Projekts INTEGER ist es, Anforderungen an eine Software-Plattform zur visuellen Entscheidungsunterstützung bei der Auswertung von Daten aus sozialen Netzwerken zur Unterstützung von Sicherheitsbehörden zu definieren und in Lösungsansätze zu überführen. Zur Beteiligung des

Bundeskriminalamtes am Projekt Pandora wird auf die Antwort zu Frage 16 verwiesen. Daneben erprobt das Bundeskriminalamt im Rahmen seiner gefahrenabwehrrechtlichen Zuständigkeiten bestehende Produkte zum sogenannten Web-Scraping im OSINT-Bereich.

Weitere Informationen sind der gemäß § 2 Absatz 2 Nummer 3 VSA als „VS-Vertraulich“ eingestuften Anlage zu entnehmen, die gesondert an die Geheimschutzstelle des Deutschen Bundestages übersandt wird.**

18. Welche Zielsetzung verfolgt das Verbundprojekt „X-SONAR“, mit dem das Bundesministerium für Bildung und Forschung „extremistische Interaktions- und Eskalationsdynamiken in sozialen Onlinenetzwerken“ erkennen und verstehen will (www.x-sonar.de)?

Ziel von X-SONAR ist es, die Entwicklung von Radikalisierungsprozessen in Online-Netzwerken, Blogs und Internetforen zu untersuchen. Dabei werden u. a. menschenverachtende Diskurse sowie strafrechtlich relevante Handlungsweisen analysiert, um Radikalisierungsmuster zu identifizieren und Indikatoren zur Früherkennung radikaler Tendenzen zu erarbeiten.

a) Welche „Radikalisierungsprozesse“ welcher Strömungen bzw. welche „Formierung neuer radikaler Gruppen“ soll die Anwendung vorrangig erkennen?

X-SONAR untersucht vorrangig islamistisch-jihadistische und rechtsextremistische Netzwerkstrukturen sowie die quantitative Verteilung extremistischer Kommunikation in diesen Bereichen.

b) Welche Angaben soll die in „X-SONAR“ bzw. der dort beforschten Anwendung erstellte Gefährdungsbewertung enthalten?

Eine Gefährdungsbewertung ist nicht Ziel der in X-SONAR durchgeführten Forschung.

c) Auf welche Weise sollen entsprechende Inhalte im Internet von der Anwendung gefunden werden?

Radikale und menschenverachtende Inhalte sollen mittels sogenannter Crawler erkannt werden, mit deren Hilfe Inhalte aus sozialen Netzwerken (z. B. Facebook, Twitter) aggregiert werden können.

d) In welchen Bereichen wird zur Risikoeinschätzung und Gewaltprävention in „X-SONAR“ auch zum Einsatz von Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen geforscht?

Eine Forschung zum Einsatz von Anwendungen zu Künstlicher Intelligenz bzw. maschinellem Lernen erfolgt nicht.

** Das Bundesministerium der Verteidigung hat die Antwort als „VS – Vertraulich“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

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 aufführen)?

Am Vorhaben ist das Landeskriminalamt Niedersachsen als direkter Projektpartner sowie das Landeskriminalamt Schleswig-Holstein als assoziierter Partner (beratend) beteiligt.

f) Welchen Beitrag erbringt die Deutsche Hochschule der Polizei in „X-SONAR“?

Das Ziel des Teilvorhabens der Deutschen Hochschule der Polizei (DHPol) besteht in der Aufarbeitung der Wahrnehmung und des Umgangs mit islamistisch-jihadistischer und rechtsgerichteter Online-Radikalisierung bei unterschiedlichen Zielgruppen. Konkret geht es um die Einzelfallanalyse zur individuellen Onlineradikalisierung, die unter Nutzung von Akten des Bundeskriminalamtes zu Syrienreisenden und -rückkehrern durchgeführt wird. Darüber hinaus ist die DHPol an der Analyse zur Wirkung extremistischer Inhalte auf die breitere Online-Community beteiligt, die im Rahmen einer Onlinebefragung realisiert wird. Ein weiterer Schwerpunkt besteht in der Analyse der Vorgehensweisen, Modellvorstellungen zu Radikalisierung bei den Polizeien des Bundes und der Länder, die in Form einer Bestandsaufnahme und Bedarfsanalyse bei diesen Endnutzern durchgeführt wird.

g) Wann und wo sollen die Tests nach gegenwärtigem Stand erfolgen?

Die Ergebnisse des Forschungsvorhabens X-SONAR fließen in Lernformate für die Weiterbildung der Anwender ein. Neben Ermittlungsbehörden und polizeilichen Ausbildungseinrichtungen sind das u. a. Beratungsstellen, wie die Beratungsstelle Gewaltprävention in Hamburg, die als assoziierter Partner am Projekt beteiligt ist.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333