Deutscher Bundestag **Drucksache 18/540**

18. Wahlperiode 13.02.2014

Kleine Anfrage

der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Annette Groth, Inge Höger, Ulla Jelpke, Stefan Liebich, Frank Tempel, Kathrin Vogler und der Fraktion DIE LINKE.

Computergestütztes Aufspüren von unerwünschtem Verhalten im öffentlichen Raum

Die Industrie hat mittlerweile zahllose „Sensoren“ entwickelt, mit denen der öffentliche Raum überwacht werden kann. Hierzu gehören Videokameras, die mittlerweile in einer neuen Generation montiert werden und hochauflösende Bilder liefern sowie neuere bildgebende Verfahren (das sogenannte Maschinensehen). Hinzu kommen Mikrofone und Bewegungsmelder, aber auch Gasdetektoren zum Aufspüren gefährlicher Stoffe oder erhöhten Alkoholgehalts im Fußballstadion. Für die Verarbeitung der Daten werden große Kapazitäten benötigt. Hier sollen computergestützte Verfahren abhelfen. So können als „verdächtig“ eingestufte Bewegungsabläufe, Geräusche oder Gerüche herausgefiltert werden. Im Falle eines „Treffers“ erhält der Bediener eine Ereignismeldung. Vor einigen Jahren ist hierzu das EU-Forschungsprogramm INDECT bekannt geworden. Dessen Teilnehmerinnen und Teilnehmer entwickeln eine Plattform, um Bilder aus der Videoüberwachung mit Polizeidatenbanken und dem Internet abzugleichen. Berechtigterweise hat das in diesem Sommer endende Projekt viel Kritik auf sich gezogen: Bürgerrechtsgruppen und Netzaktivisten hatten INDECT als „Bevölkerungsscanner“ kritisiert (Bundestagsdrucksache 17/3940). Mehrere Polizeibehörden interessieren sich für das Ergebnis von INDECT, das ebenfalls beteiligte Bundeskriminalamt (BKA) war allerdings ausgestiegen – angeblich wegen des „umfassenden Überwachungsgedankens“ (Pressemitteilung, 13. Oktober 2011).

Nun finanziert die Europäische Kommission weitere Forschungsvorhaben mit ähnlicher Zielsetzung. Wieder steht die Auswertung möglichst vieler Quellen im Mittelpunkt, darunter neben der Überwachung öffentlicher Orte auch soziale Medien. Die Plattformen sollen polizeilich relevante Vorfälle auch vorhersagen. Eines der neueren EU-Programme trägt den Namen PROACTIVE (www.fp7-proactive.eu). Der Name markiert einen neuen Trend in der Strafverfolgung: Im Gegensatz zu „Prävention“ soll die „proaktive Verbrechensbekämpfung“ greifen, wenn die vermeintliche Bedrohung noch gar nicht in Sicht ist. Damit schlägt sich das Konzept von „Gefährdern“ bzw. „Gefahrengebieten“ nach Ansicht der Fragesteller auch in der Sicherheitsforschung nieder. Die Rede ist von „vorhersagenden Schlussfolgerungen und der Einbindung mehrerer Quellen“, als Ziel wird eine „Verhinderung terroristischer Angriffe in städtischer Umgebung“ ausgegeben. Im Originaltitel wird das Wort „Fusion“ benutzt. Gemeint ist die statistische Auswertung polizeilicher Daten in Verbindung mit Informationen von „Sensoren“, die über die ganze Stadt verteilt sein können. Besondere Aufmerksamkeit wird aber dem „Internet der Dinge“ zuteil. Gewöhnlich werden damit

technische Alltagshelfer bezeichnet, die über eine Netzwerkverbindung verfügen. In PROACTIVE sollen sie der Polizei zur Verhaltenskontrolle ihrer Nutzerinnen und Nutzer dienen. Diese Art des Zusammenführens von Daten mehrerer Quellen ist in Deutschland derzeit allerdings nur im Rahmen von Ermittlungen gestattet. Die Europäische Union (EU) finanziert deshalb rechtliche und ethische Forschungen, um die Gesetzeslage in den Mitgliedstaaten zu analysieren und mit den neuen Technologien zu synchronisieren (www.smartsurveillance.eu). PROACTIVE wird angeführt vom italienischen Konzern Vitrociset, der auf zivile und militärische Überwachungs- und Transportsysteme spezialisiert ist. Ebenfalls an Bord ist die polnische University of Science and Technology mit Sitz in Krakau, deren Forscher bereits an INDECT geforscht hatten. Unter den Beteiligten findet sich aber auch die Universität der Bundeswehr München. Die kurze Beschreibung über die Mitarbeit der deutschen Militärforscher lässt darauf schließen, dass die in PROACTIVE entwickelte Plattform auch Drohnen einbinden könnte – oder aber deren autonome Fähigkeit, schnell Entscheidungen zu treffen. Zuständig ist das Institut für Flugsysteme, dessen Arbeiten zur künstlichen Intelligenz unbemannter Luftfahrzeuge durch PROACTIVE gelobt werden. Diese seien geeignet, eine Situation schnell einzuschätzen und Entscheidungshilfen zu geben. Für die Anwendung von PROACTIVE interessieren sich Polizeibehörden und Geheimdienste aus Finnland, Zypern, Ungarn, Rumänien und Polen, aber auch das in Italien ansässige Crime and Justice Research Institute (UNICRI). Das UNICRI ist bei den Vereinten Nationen angesiedelt und beschäftigt sich insbesondere mit Forschungen zur Beherrschbarkeit von Sportereignissen oder Gipfelprotesten. Auch das Bayerische Landeskriminalamt (BLKA) hat mindestens zweimal an Workshops von „Endnutzern“ teilgenommen (www.fp7-proactive.eu/latest-news/conclusions-2nd-end-users-advisory-board).

Während sich PROACTIVE mit „terroristischen Angriffen“ befasst, soll das EU-Programm CAPER die „organisierte Kriminalität“ proaktiv adressieren (www.cordis.europa.eu/projects/rcn/99655_en.html). Der Titel lässt sich als „Gemeinschaftliche Information, Beschaffung, Verarbeitung, Verwertung und Meldung zur Vorbeugung organisierter Kriminalität“ übersetzen. Das System soll Informationstechnologie ausforschen und auswerten. Hierzu gehört insbesondere die „Open Source Intelligence“ (OSINT) des Internets. Gemeint sind öffentlich zugängliche Daten von Webseiten und Sozialen Medien. Angeführt vom auf Sicherheitsanwendungen spezialisierten Softwarehaus S21sec macht auch das Fraunhofer-Institut für Graphische Datenverarbeitung IGD bei CAPER mit. Das Institut erklärt zur Funktionsweise der Plattform, die gewonnenen Daten würden „semantisch analysiert und visuell so aufbereitet, dass Zusammenhänge oder besondere Ereignisse erkannt werden können“. CAPER will Informationen von Diensten wie Twitter mit „Close Source Intelligence“ verbinden. Hinter dem Begriff verbergen sich auch Informationen, die in Polizeidatenbanken lagern. Diese polizeilichen Daten könnten dann mit Analysesystemen verknüpft werden, die Bilder, Videos, verschiedene Sprachen und biometrische Daten verarbeiten. CAPER soll diese Rasterfahndung in verschiedenen Datenquellen derart vereinfachen, dass sie über ein simples Interface vorgenommen werden kann. Auf diese Weise wollen die Ermittler bislang unentdeckte Informationen finden. Schon seit Beginn waren die israelische Polizei und die Mossos d’Esquadra aus Barcelona als „Endnutzer“ von CAPER registriert. Als neue Beobachter sind nun das britische Innenministerium, der rumänische Geheimdienst und das deutsche BKA an Bord (www.fp7-caper.eu/consortium.html). Dies ist also mindestens das zweite Vorhaben, in dem sich die Kriminalisten aus Wiesbaden mit dem Blick in die Glaskugel befassen (Bundestagsdrucksache 17/13441).

Wir fragen die Bundesregierung:

1. Hinsichtlich welcher Forschungsprojekte sind welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes mit der Verbesserung von automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) als Teilnehmende, Beobachterinnen oder auch als Adressatinnen entsprechender Berichte auf deutscher Ebene befasst?

   a) Um welche Projekte handelt es sich dabei konkret, und wer nimmt daran (auch zur Beobachtung) teil?

   b) Welche Beiträge haben private Firmen oder Institute hierfür erbracht?

   c) Wann wurden die Projekte begonnen, wann enden sie, welches Finanzvolumen haben sie, und wie werden sie finanziert?

   d) Welche Plattformen mit welchen gewünschten Funktionsweisen sollen die einzelnen Vorhaben entwickeln?

2. Hinsichtlich welcher Forschungsprojekte sind welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes mit der Verbesserung von automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) als Teilnehmende, Beobachterinnen oder auch als Adressatinnen entsprechender Berichte auf Ebene der EU befasst?

   a) Um welche Projekte handelt es sich dabei konkret, und wer nimmt daran (auch zur Beobachtung) teil?

   b) Welche Beiträge haben private Firmen oder Institute hierfür erbracht?

   c) Wann wurden die Projekte begonnen, wann enden sie, welches Finanzvolumen haben sie, und wie werden sie finanziert?

   d) Welche Plattformen mit welchen gewünschten Funktionsweisen sollen die einzelnen Vorhaben entwickeln?

3. Inwiefern setzen welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes die automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) bereits ein?

4. Inwiefern haben sich auch Bundesbehörden bereits mit Verfahren befasst oder setzen sie bereits ein, wie sie unter anderem „DER SPIEGEL“ über den britischen Geheimdienst GCHQ berichtete und wonach dieser in Echtzeit verfolgen kann, welche Videos auf YouTube angesehen werden, welche Inhalte auf Facebook ein „Gefällt mir“ bekommen, und welche Seiten auf Googles Blogplattform Blogger.com gelesen werden (SPIEGEL ONLINE, 28. Januar 2014)?

   a) Über welche eigenen Erkenntnisse verfügt die Bundesregierung hinsichtlich des Programms „Squeaky Dolphin“ oder ähnlicher Verfahren der US-amerikanischen National Security Agency (NSA) oder des GCHQ zur Social-Media-Analyse, deren Namen noch nicht öffentlich bekannt sind?

   b) Was ist der Bundesregierung über Möglichkeiten bekannt, Daten, die von Smartphone-Apps übertragen werden und die persönliche Informationen enthalten, abzuhören?

5. Welchen Namen tragen die „integrierte[n] Fachanwendungen zur Erfassung und Aufbereitung der im Rahmen einer Telekommunikationsüberwachung aufgezeichneten Daten der Hersteller Syborg und DigiTask“ bei Polizeibehörden des Bundes, die laut der Bundesregierung „aufgezeichneten Rohdatenstrom […] in lesbarer Form zur Verfügung stell[en]“ (Bundestagsdrucksachen 17/14739 und 17/14530), und von welchen Abteilungen deutscher Bundesbehörden werden diese genutzt?
6. Inwiefern haben Bundesbehörden jemals von Diensten der EU-Polizeiagentur Europol Gebrauch gemacht, die eine Auswertung von „Open Source Intelligence“ anbietet und dies im „Europol Work Programme 2014“ als „provision of tailored newsfeeds on cybercrime trends, technological developments and other relevant information“ und „permanent Open Source scanning capability“ bewirbt?
7. Auf welche Weise soll das EU-Programm PROACTIVE „terroristische Angriffe in städtischer Umgebung“ verhindern?
   a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?
   b) Auf welche Weise sollen bei PROACTIVE „vorhersagende Schlussfolgerungen“ erzielt werden?
   c) Welche „Quellen“ werden hierfür eingebunden?
   d) Was ist damit gemeint, wenn bei PROACTIVE auch die Überwachung über das „Internet der Dinge“ beforscht wird?
8. Inwiefern ist eine bei PROACTIVE beforschte „proaktive Verbrechensbekämpfung“ auf Basis der Analyse technischer „Sensoren“ in Deutschland rechtlich durchführbar, bzw. welche Gesetzesänderungen wären hierfür notwendig?
9. Wie bewertet die Bundesregierung die Notwendigkeit von PROACTIVE?
10. Worin besteht der Beitrag der Universität der Bundeswehr München sowie des Instituts für Flugsysteme in München bei PROACTIVE?
    a) Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird dabei zurückgegriffen?
    b) Welche eigenen, ähnlichen Forschungen betreiben die Universität der Bundeswehr München sowie das Institut für Flugsysteme?
    c) Inwiefern wird bei PROACTIVE auch die Einbindung von Drohnen beforscht, und welche Beiträge liefert die Bundeswehr hierfür?
11. Welche konkreten Beiträge haben Polizeibehörden und Geheimdienste aus Finnland, Zypern, Ungarn, Rumänien und Polen nach Kenntnis der Bundesregierung bei PROACTIVE erbracht?
    a) Wie haben diese anvisierten „Endnutzer“ vorab ihren „Bedarf“ definiert?
    b) Auf welche Weise wären die Forschungen der Universität der Bundeswehr München sowie des Instituts für Flugsysteme geeignet, die Bedarfe der „Endnutzer“ zu erfüllen?
12. Was ist der Bundesregierung durch die Mitarbeit der Bundeswehr oder durch eigene Erkenntnisse über die Teilnahme des BLKA an PROACTIVE bekannt?
    a) Welchen Beitrag hat das BLKA im Projekt erbracht, bzw. welches Interesse hat die Behörde vorgetragen?

b) Inwiefern steht das BLKA hierzu in Kontakt mit der Universität der Bundeswehr München oder dem Institut für Flugsysteme?

c) An welchen Workshops von „Endnutzern“ hat das BLKA nach Kenntnis der Bundesregierung teilgenommen, und welche Themen wurden dort behandelt?

13. Auf welche Weise soll das EU-Programm CAPER die „organisierte Kriminalität“ proaktiv adressieren?

a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?

b) Auf welche Weise sollen bei CAPER die „gemeinschaftliche Information, Beschaffung, Verarbeitung, Verwertung und Meldung“ von Informationen optimiert werden?

c) Auf welche Weise sollen nach Kenntnis der Bundesregierung bei CAPER Inhalte „semantisch analysiert und visuell so aufbereitet werden, dass Zusammenhänge oder besondere Ereignisse erkannt werden können“?

d) Auf welche Weise soll hierfür „Open Source Intelligence“ genutzt werden?

e) Auf welche Weise sollen auch Kurznachrichtendienste eingebunden werden?

f) Auf welche Weise sollen bei CAPER auch Informationen einer „Close Source Intelligence“ eingebunden werden, und welche sind damit konkret gemeint?

14. Worin besteht nach Kenntnis der Bundesregierung der Beitrag des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD bei CAPER?

Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird dabei nach Kenntnis der Bundesregierung zurückgegriffen?

15. Welche konkreten Beiträge haben die israelische Polizei, die Mossos d’Esquadra aus Barcelona, das britische Innenministerium und der rumänische Geheimdienst bei CAPER erbracht?

a) Wie haben diese anvisierten „Endnutzer“ vorab ihren „Bedarf“ definiert?

b) Auf welche Weise wären die Forschungen bei CAPER geeignet, die Bedarfe der „Endnutzer“ zu erfüllen?

16. Aus welchem Grund interessiert sich das BKA für die Mitarbeit bei CAPER?

a) Auf welche Weise ist das BKA als Teilnehmer aufgenommen worden, und wer hatte einen entsprechenden Antrag gestellt?

Welchen Beitrag hat das BKA im Projekt erbracht, bzw. welches Interesse hat die Behörde vorgetragen?

b) Inwiefern steht das BKA hierzu in Kontakt mit dem Fraunhofer-Institut für Graphische Datenverarbeitung IGD?

c) An welchen Workshops von „Endnutzern“ hat das BKA teilgenommen, und welche Themen wurden dort behandelt?

17. Inwiefern ist eine bei CAPER beforschte „proaktive Verbrechensbekämpfung“ in Deutschland rechtlich durchführbar, bzw. welche Gesetzesänderungen wären hierfür notwendig?

18. Wie bewertet die Bundesregierung die Notwendigkeit von CAPER?

19. Was ist das Ziel des Projekts „DRiving InnoVation in Crisis Management for European Resilience“ (Driver), an dem laut eigener Aussage auch das Deutsche Zentrum für Luft- und Raumfahrt e. V. (DLR) beteiligt ist (www.dlr.de vom 4. Juli 2013)?

    a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?

    b) Aus welchem Grund interessiert sich das DLR für die Mitarbeit bei Driver?

    c) Worin besteht der Beitrag des DLR?

    d) Inwiefern will das DLR auch Ergebnisse seiner Forschungen zu Drohnen einbringen, etwa aus dem EU-Forschungsprojekt DeSIRE?

    e) Worin besteht nach Kenntnis der Bundesregierung der Beitrag der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. bei Driver?

    f) Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird vom DLR und der Fraunhofer-Gesellschaft nach Kenntnis der Bundesregierung zurückgegriffen?

    g) Wer gilt bei Driver als Koordinator, und wer sind die „Endnutzer“?

    h) Inwiefern ist nach Kenntnis der Bundesregierung beabsichtigt oder wird als Szenario erwogen, Driver auch bei Protesten oder zur „crowd control“ einzusetzen, wie dies nach Kenntnis der Fragestellerinnen und Fragesteller vom DLR auf der Konferenz „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“ der Deutschen Gesellschaft für Wehrtechnik e. V. in Berlin vorgetragen wurde?

20. Wie bewertet die Bundesregierung die Notwendigkeit von Driver?

21. Inwiefern ist das BKA weiterhin mit dem Institut für Sicherheit und Gesellschaft der Albert-Ludwigs-Universität Freiburg oder dem Software-Konzern IBM in Kontakt (Bundestagsdrucksache 17/13441), und zu welchen „weiteren gemeinsamen Aktivitäten“ hat die Besichtigung der „Crime Information Platform“ durch das BKA geführt?

    Welche weiteren „Informationsbesuche“ oder sonstigen „Beobachtungen“ hat das BKA bei anderen Einrichtungen zu „prediktiver Software“ vorgenommen?

22. Worin bestand nach Kenntnis der Bundesregierung der Austausch Europols mit dem Department of Homeland Security zu als „Fusion Center“ bezeichneten „Terrorismusabwehrzentren“ (Bundestagsdrucksache 17/14833)?

23. Auf welche Weise sind Strafverfolgungsbehörden des Bundes mit der Prävention oder Schutzmaßnahmen von Kritischen Versorgungsdienstleistungen der Branchen Elektrizität, Gas und Mineralöl befasst, und welche Kooperationen oder Forschungsprojekte sind die Behörden hierzu mit den Betreibern Kritischer Infrastrukturen sowie deren Fach- und Branchenverbänden eingegangen?

24. Inwiefern treffen Berichte zu, wonach die Bundeswehr mittlerweile über eine neue mobile Überwachungsplattform „Mobiles Geschütztes Fernmeldeaufklärungssystem (MoGeFA)“ der Firma Plath GmbH verfügt (www. bundeswehr-journal.de/2014/mobile-fernmeldeaufklaerung-in-krisengebieten)?

    a) Wer hat die montierten Systeme jeweils hergestellt, und welche Kosten fielen hierfür an?

b) Was ist mit der beworbenen Funktionalität der „Ermittlung vollständiger Funk-Lagebilder in einsatzrelevanten Frequenzbereichen“ gemeint?

c) Inwiefern trifft es zu, dass „in wichtigen Frequenzbereichen alle elektromagnetischen Aussendungen entdeckt und geortet werden“, und um welche handelt es sich dabei?

d) Auf welche Weise wurden bei der Beschaffung des Systems Datenschutzbeauftragte des Bundes oder der Bundeswehr eingebunden, und was war das Ergebnis eines Datenschutzkonzeptes (sofern dies überhaupt erstellt wurde)?

e) Auf welchen bzw. wie vielen weiteren schwimmenden, fahrenden oder fliegenden Plattformen nutzt die Bundeswehr ähnliche Überwachungstechnik?

25. Welche weiteren Angaben kann die Bundesregierung zu den Inhalten der „Working group on modern technology“ innerhalb der European Police Chiefs Taskforce mitteilen, die von Europol mit Blick auf die dritte „European Police Chiefs Convention“ eingerichtet wurde (Bundestagsdrucksache 17/14833)?

a) Welche Instrumente zur „Früherkennung von Neuen Technologien“ wurden behandelt?

b) Was ist damit gemeint, wenn die Bundesregierung von einer „strategisch-technologischen Früherkennung ohne Fokussierung auf bestimmte Technologien“ spricht?

c) Inwiefern wurde das Ziel erfüllt, „ein gemeinsames methodisches Vorgehen im Erkennen und Bewerten von Neuen Technologien hinsichtlich einer potentiellen polizeilichen Relevanz im Allgemeinen zu beraten“?

d) Welche seiner „methodischen Erfahrungen im Bereich der strategischen Früherkennung und Folgenabschätzung von Neuen Technologien“ hatte das BKA eingebracht?

Berlin, den 12. Februar 2014

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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