Deutscher Bundestag **Drucksache 18/4007**

18. Wahlperiode 11.02.2015

Kleine Anfrage

der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, Annette Groth, Ulla Jelpke, Dr. Alexander S. Neu, Frank Tempel, Halina Wawzyniak, Jörn Wunderlich und der Fraktion DIE LINKE.

Aufrüstung der IT-Analysefähigkeiten bei der EU-Polizeiagentur Europol

In seinem kürzlich veröffentlichten Arbeitsprogramm für das Jahr 2015 kündigt die Polizeiagentur Europol die Einführung eines ganzen Arsenals neuer Analysesoftware an (Ratsdokument 5250/15). Die Rede ist von „fortgeschrittenen Werkzeugen für Datenverarbeitung, aufklärungsbasierte Analyse, darunter auch strategische Analyse und Analyse offener Quellen“. Schon vor zwei Jahren hatte Europol von Anwendungen zu „Data Fusion“ geschrieben (www.europol.europa.eu/ec3/services). Gemeint ist Data Mining, also die Möglichkeit, die existierenden Datenbestände in Beziehung zu setzen und grafisch anzuzeigen. Die Tageszeitung „THE WALL STREET JOURNAL“ (14. Januar 2013) berichtete darüber hinaus, dass Europol an der Entwicklung neuer digitaler Analysewerkzeuge zur Mustererkennung arbeitet.

Im neuen Arbeitsprogramm werden die Anwendungen als „future-forecasting and scenario techniques“ beschrieben. Es ist aber unklar, inwiefern ihr Einsatz überhaupt rechtlich einwandfrei ist. Data Mining wird von Polizeibehörden in Deutschland beispielsweise nicht vorgenommen (Bundestagsdrucksache 18/707). Auch die neue „Ma³tch“-Technologie zur Echtzeit-Analyse von Finanzdaten, auf deren Einführung Europol drängt, darf vom deutschen Bundeskriminalamt (BKA) nicht angewandt werden (Bundestagsdrucksache 18/2888). Würden aus Deutschland angelieferte Daten bei Europol mit automatisierten Verfahren verarbeitet, könnte es sich nach Ansicht der Fragesteller um einen Verstoß gegen Datenschutzbedingungen handeln. Deutschland ist laut eigenen Angaben „zweitstärkster Nutzer“ von Europols Informationssystemen (Bundestagsdrucksache 18/3766).

Laut dem Arbeitsprogramm sollen Verfahren zur Auswertung und zum Vergleich biometrischer Daten eingeführt werden. Europol beabsichtigt, auf das neue EU-System zur Speicherung von Fingerabdrücken im Schengener Informationssystem zuzugreifen. Auch die Beschaffung von Software zur Erkennung von Personen und Sachen in Bild- und Videodaten steht auf der Europol-Wunschliste. Bald sollen die Arbeiten an einem „European Tracking System“ abgeschlossen sein, mit dem europäische Polizeibehörden ihre GPS-Peilsender (GPS – Global Positioning System), etwa an Fahrzeugen Verdächtiger, auch grenzüberschreitend betreiben können. Europol richtet hierzu einen zentralen Server ein, der außer durch die Mitgliedstaaten auch von „Third Parties“ genutzt werden kann. Die Ausgabeformate der Peilsender werden hierfür standardisiert. Das seit zwei Jahren bei Europol angesiedelte „European CyberCrime Center“ (EC3) soll einen eigenen „Malware Scanner“ erhalten. Das könnte bedeuten, dass Europol selbst das Internet absucht. Geplant ist auch die Verbesserung des

Austauschs in Echtzeit. Nun soll ein übergreifendes „Europol Analysis System“ (EAS) aufgebaut werden. Vor zwei Jahren wurden ähnliche Pläne bekannt, wonach Europol eine „Plattform für den Informationsaustausch von Strafverfolgungsbehörden“ einrichtet (Bundestagsdrucksache 17/13441).

Die Europäische Kommission hat für die Europol-Pläne zusätzliche Mittel von 12,5 Mio. Euro bereitgestellt. Als Begründung der IT-Aufrüstung dient die neue Europol-Verordnung, wonach die Agentur in einem „erweiterten Mandat“ ihre Analysefähigkeiten verbessern und ausweiten soll. Geplant ist etwa, dass Europol zukünftig selbst Daten von europäischen Polizeibehörden einsammeln darf und nicht mehr auf entsprechende Lieferungen warten muss.

Wir fragen die Bundesregierung:

1. Inwiefern kann die Bundesregierung ihre Angaben, wonach Deutschland „zweitstärkster Nutzer“ von Europols Informationssystemen ist, nach Zulieferungen und Abfragen aufschlüsseln?
2. Inwiefern hält es die Bundesregierung für notwendig, dass die Polizeiagentur Europol „fortgeschrittene Werkzeuge für Datenverarbeitung, aufklärungsbasierte Analyse, darunter auch strategische Analyse und Analyse offener Quellen“ beschafft, und aus welchem Grund kann dies nicht mit vorhandener IT-Ausrüstung bewerkstelligt werden?
3. Was ist der Bundesregierung darüber bekannt, welche Anwendungen zur Vorhersage und Szenario-Modellierung („future-forecasting and scenario techniques“) beschafft werden sollen, welche Defizite damit behoben werden sollen und im Rahmen welcher Ermittlungen diese eingesetzt würden?
4. Was ist der Bundesregierung darüber bekannt, in welchem Maße und in welchen Fällen die aus Deutschland angelieferten Daten bei Europol mit Verfahren zum Data Mining, zur Mustererkennung, zur Prognose oder zu „Predictive Analytics“ verarbeitet werden?
5. Inwiefern kann die Bundesregierung um die Bearbeitung der von ihr angelieferten Daten mit solchen Analyseverfahren bitten oder sie ausschließen?
6. Was ist der Bundesregierung darüber bekannt, in welchem Maße und in welchen Fällen aus Deutschland angelieferte Finanzdaten bei Europol mit der „Ma³tch“-Technologie zur Echtzeit-Analyse analysiert werden, bzw. inwiefern ist ein solches Verfahren geplant?
7. Inwiefern bzw. auf welcher rechtlichen Grundlage hält die Bundesregierung ein solches Verfahren für denkbar, obwohl dies dem deutschen BKA untersagt ist?
8. Welche Verfahren zur Auswertung und zum Vergleich biometrischer Daten sollen nach Kenntnis der Bundesregierung bei Europol eingeführt werden?
9. Inwiefern beabsichtigt Europol nach Kenntnis der Bundesregierung, auf das neue EU-System zur Speicherung von Fingerabdrücken im Schengener Informationssystem zuzugreifen?
10. Was ist der Bundesregierung über Pläne Europols zur Beschaffung von Software zur Erkennung von Personen und Sachen in Bild- und Videodaten bekannt, wofür würden diese genutzt, und inwiefern würden auch aus Deutschland gelieferte Daten damit durchsucht?
11. Was ist der Bundesregierung über den Stand von Arbeiten an einem „European Tracking System“ bekannt, welche Behörden von Mitgliedstaaten der Europäischen Union oder sonstigen Partner sind daran beteiligt, und inwiefern würde das System auch von deutschen Behörden genutzt?

12. Inwiefern werden im Zuge der Errichtung eines „European Tracking Systems“ auch deutsche Ausgabeformate von Peilsendern standardisiert?

13. Was ist der Bundesregierung darüber bekannt, wofür das bei Europol angesiedelte „European CyberCrime Center“ einen eigenen „Malware Scanner“ erhalten soll?

14. Was ist der Bundesregierung darüber bekannt, in welchem Rahmen und auf welcher rechtlichen Grundlage Europol selbst das Internet absucht, etwa zur Auswertung offener Quellen in Sozialen Medien, wie Facebook oder Twitter?

15. Inwiefern sind die Inhalte bzw. der Umfang der Plattform für den Informationsaustausch bei Strafverfolgungsbehörden (IXP) bei Europol mittlerweile abschließend festgelegt (Bundestagsdrucksache 17/13441)?

16. Welche Informationen zu Behörden, Institutionen, Expertennetzwerken, Strafverfolgungsinstrumenten, Übersetzungswerkzeugen, Kommunikationskanälen sowie Fahndungsdaten soll das IXP nach Kenntnis der Bundesregierung enthalten, und wo wird es angesiedelt?

17. Welche Endnutzer des IXP sind der Bundesregierung bekannt?

18. Was ist nach Kenntnis der Bundesregierung unter dem „Europol Analysis System“ zu verstehen, und welche Fähigkeiten bzw. Anwendungen werden hierunter zusammengefasst?

19. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit, derartige Analysetätigkeiten in der neuen Europol-Verordnung zu verankern?

20. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit, die neue Europol-Verordnung so zu gestalten, dass Europol selbst Daten einsammeln kann und nicht mehr auf Zulieferungen der Mitgliedstaaten warten muss?

21. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit direkter Kontakte zwischen Europol und nationalen Behörden unter Umgehung des bislang vorgeschriebenen Weges über die jeweilige nationale Kontaktstelle?

22. Mit welchen „als relevant eingeschätzten Bedrohungslagen und Sachverhalten aus dem Bereich der Cybercrime“ hat sich die „Joint Cybercrime Action Taskforce“ (J-CAT) nach Kenntnis der Bundesregierung „bedarfs- und anlassbezogen“ befasst (Bundestagsdrucksache 18/2674)?

23. Welche Rolle kam dabei jeweils Europol zu?

24. Auf welche Weise haben sich „Cybercrimedienststellen aus den USA, Kanada, Australien und Kolumbien“ in die Arbeit des J-CAT eingebracht?

25. Mit welchen Aufgaben war der vom BKA für die sechsmonatige Pilotphase von J-CAT entsandte Mitarbeiter bislang befasst?

26. Inwiefern wurden bereits „auf Grundlage von Auswertungen koordinierte Maßnahmen gegen Hauptakteure und Erscheinungsformen aus dem Phänomenbereich Cybercrime“ betrieben, indem Ermittlungsverfahren auf nationaler Ebene eingeleitet wurden?

27. Inwiefern wurde bei den Ermittlungen außer auf die Focal Points „Cyborg“, „Terminal“ und „Twins“ auf weitere „bei Europol vorliegende[n] Informations- und Auswertemöglichkeiten“ zurückgegriffen?

28. Was ist der Bundesregierung über Ziele und Beteiligte einer „European Expert Group on Cybercrime“ bekannt?

    a) Wer führt die Gruppe an, und welche Rolle übernehmen die „Leader“ und „Co-Leader“ (bitte für eine etwaige deutsche Beteiligung ausführlich darstellen)?

    b) Wann und auf wessen Veranlassung wurde die Gruppe gegründet?

    c) Auf welche Art und Weise und mit welcher Zielsetzung werden in der „European Expert Group on Cybercrime“ auch Anonymisierungsverfahren und Verschlüsselungen behandelt?

    d) Welchen ähnlichen EU-Arbeitsgruppen gegen „Cyberkriminalität“ gehören deutsche Behörden als „Leader“, „Co-Leader“ oder Unterstützer an?

29. Auf welche Weise wurde nach Kenntnis der Bundesregierung das Projekt „Interpol project on interoperability – A practical development for enhanced police cooperation within EU Member States“ inzwischen weiterbetrieben oder umgesetzt (Ratsdokument 10094/14)?

    a) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus den in dem Dokument genannten Defiziten sowie den dort gemachten Vorschlägen für den Ausbau der polizeilichen Zusammenarbeit?

    b) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung zu der in dem Dokument vorgeschlagenen „One Stop Shopping Strategy“ hinsichtlich deutscher datenschutzrechtlicher Vorgaben?

30. Was ist der Bundesregierung über die derzeitigen Beteiligten der bei Interpol angesiedelten Projekte VENLIG und HAMAH bekannt, in denen Informationen des US-Verteidigungsministeriums über „ausländische Terroristen“ ausgewertet werden (Bundestagsdrucksache 17/4407)?

    a) Was ist der Bundesregierung darüber bekannt, in welchem Umfang VENLIG und HAMAH bzw. ähnliche Projekte für andere Länder überhaupt genutzt werden bzw. inwiefern eine Nutzung seit dem Jahr 2011 zu- oder abnimmt?

    b) Was ist der Bundesregierung darüber bekannt, ob Europol die dort erlangten Daten nicht nur in die Analysearbeitsdatei „Hydra“ einstellt, sondern auch in anderen Dateien speichert?

    c) Inwiefern lässt sich rekonstruieren, ob auch deutsche Behörden die aus Beständen des US-Verteidigungsministeriums stammenden Daten abrufen dürfen, bzw. inwiefern ist das Ministerium als Besitzer der Daten erkennbar?

31. Welche Haltung wird die Bundesregierung in den zuständigen Ratsarbeitsgruppen zur Frage vertreten, ob bzw. mit welchen Einschränkungen Europol, wie im Arbeitsprogramm für das Jahr 2015 skizziert, ein Zusammenarbeitsabkommen mit Israel verhandelt oder abschließt?

32. Inwiefern wäre ein solches Abkommen einer EU-Agentur aus Sicht der Bundesregierung überhaupt möglich, wenn dabei mit einer Polizei zusammengearbeitet würde, die über ein Hauptquartier in den von Israel besetzten Gebieten verfügt?

    a) Welchen Stand haben nach Kenntnis der Bundesregierung Verhandlungen eines Kooperationsabkommens zwischen Europol und Israel (Bundestagsdrucksache 17/3143)?

    b) Welche Informationen sollen im Rahmen des Abkommens getauscht werden?

c) Auf welche Daten hätten israelische Behörden demnach Zugriff?

d) Wie lange würden die Daten in Israel gespeichert?

e) Dürfte Israel die Daten an Drittstaaten weitergeben?

33. Was ist der Bundesregierung darüber bekannt, inwiefern die Errichtung und der Betrieb einer gesicherten privaten Kommunikationsinfrastruktur und eine Breitbandverbindung im „sTESTA“-Netzwerk zwischen Estland, Frankreich und Österreich mittlerweile nicht mehr durch ein Konsortium aus OBS (Orange Business Services) und HP (Hewlett-Packard) bereitgestellt wird, sondern auf ein System der Firma T-Systems migriert ist (Bundestagsdrucksache 18/1832)?

34. Welche Gründe sind der Bundesregierung für eine Neuausschreibung des „sTESTA“-Netzwerks bekannt?

35. Was ist der Bundesregierung darüber bekannt, welche technischen Anlagen des SIS I (SIS – Schengener Informationssystem) nach Umstieg auf das SIS II veraltet sind und nicht mehr genutzt werden, wer für dessen Abbau bzw. Entsorgung zuständig ist und welche Kosten hierfür anfallen?

36. Inwiefern hat die Bundesregierung mittlerweile weiter geprüft, auf welche Weise ein Europäischer Kriminalaktennachweis (European Police Records Index – EPRIS) etwaige Defizite des grenzüberschreitenden polizeilichen Informationsaustauschs schließen kann (Bundestagsdrucksache 18/1832)?

37. Welche weiteren Schlussfolgerungen zieht die Bundesregierung aus einer hierzu erstellten Studie?

38. Inwiefern und mit welchem (vorläufigen) Ergebnis wurde nach Kenntnis der Bundesregierung in den zuständigen Ratsarbeitsgruppen erörtert, wie etwaige Lücken in den bestehenden polizeilichen Systemen geschlossen werden könnten?

Berlin, den 6. Februar 2015

Dr. Gregor Gysi und Fraktion

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