Deutscher Bundestag **Drucksache 18/542**

18. Wahlperiode 12.02.2014

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, Heike Hänsel, Martina Renner, Dr. Petra Sitte, Frank Tempel und der Fraktion DIE LINKE.

Polizeiliche Aktivitäten zur Überwachung und Manipulation vernetzter Fahrzeuge

Die britische Bürgerrechtsorganisation Statewatch hat das Arbeitsprogramm des „European Network of Law Enforcement Technology Services (ENLETS)“ veröffentlicht (Statewatch, 23. Januar 2014). ENLETS wurde erst im September 2008 unter französischer Präsidentschaft gegründet. Zur zunächst damals noch informellen Struktur gehörten Belgien, Griechenland, Zypern, die Niederlande, Polen, Finnland und Großbritannien. Als deutsche „Nationale Kontaktstelle“ fungiert die Deutsche Hochschule der Polizei in Münster (Bundestagsdrucksache 17/14474). Ab dem Jahr 2010 wurde die engere Einbeziehung der Europäischen Kommission begonnen, kurze Zeit später nahmen auch die EU-Agenturen Europol und FRONTEX teil. Mittlerweile sind 19 EU-Mitgliedstaaten bei den ENLETS-Treffen zugegen. Im Sommer 2013 hatte der Rat Schlussfolgerungen verabschiedet, um Polizeien mit der „sicherheitsbezogenen Forschung und Industriepolitik“ besser zu verzahnen (Ratsdokument 12103/13). Für ENLETS bedeutete dies eine signifikante Aufwertung: Das Netzwerk betreibt nun eine „Technologie-Beobachtungsstelle“. Zu ihrem Auftrag gehört unter anderem die „Unterstützung proaktiver Kontakte“ zwischen Industrie und Anwendern. Laut dem Arbeitsprogramm setzt sich ENLETS dafür ein, dass zukünftig ein ferngesteuertes Anhalten (Remote Stopping Vehicles) serienmäßig in alle in der Europäischen Union (EU) zugelassenen Fahrzeuge eingebaut werden soll. Das Polizeinetzwerk ist aber selbst nicht mit entsprechenden Forschungen befasst. Stattdessen fungiert ENLETS als Schnittstelle, um Bedürfnisse und entsprechende Lösungen aus den Mitgliedstaaten zu koordinieren.

In einem weiteren Vorhaben unterstützt die EU Forschungen zu Möglichkeiten des Anhaltens von „nicht kooperativen Fahrzeugen“. Das Projekt trägt den Titel „Safe control of non cooperative vehicles through electromagnetic means“ (SAVELEC) und will bis zum Jahr 2015 Anwendungen entwickeln, um mit künstlich erzeugten elektromagnetischen Impulsen (EMP) oder Mikrowellen (HPM) die in der Nähe befindliche Elektronik von Fahrzeugen oder Schiffen zu blockieren oder sogar zu zerstören (www.savelec-project.eu). Ziel ist es, die bislang nur militärisch genutzte Technologie für polizeiliche Zwecke nutzbar zu machen. Jedoch seien die marktverfügbaren Systeme noch zu groß für den polizeilichen Einsatz. Die Forschungen sollen sich deshalb auf brauchbare Antennen, Verstärker und Stromquellen konzentrieren. Das Endprodukt soll tragbar sein, um es in Polizeifahrzeugen mitführen zu können. Das Finanzvolumen von SAVELEC beträgt 4,2 Mio. Euro, von denen rund 3,3 Mio. Euro durch die Europäische Kommission übernommen werden. Das gesamte Vorhaben besteht aus acht „Work Packages“, deren Fokus entweder auf den späteren Anwendungen, technischen Erfordernissen, der konkreten Umsetzung oder Experimenten liegt. Eine der Arbeitsgruppen soll die Entwicklung eines Prototypen sicherstel-

len. Angeführt wird das Projekt von der Polytechnischen Universität im spanischen Valencia. Auch das Landeskriminalamt (LKA) Sachsen-Anhalt beteiligt sich an den Forschungen. Weitere deutsche Partner sind die Otto-von-Guericke-Universität Magdeburg, das Deutsche Zentrum für Luft- und Raumfahrt e. V. (DLR) und die Firma IMST GmbH aus Kamp-Lintfort. Mit von der Partie ist auch eine slowakische Militärakademie und der Raketenhersteller MBDA, der wie deutsche Rüstungsfirmen unter anderem an neuen Laserwaffen forscht. Die Technik gilt offiziell als „nicht-tödliche Waffe“. Die Definition ist allerdings umstritten: Statewatch macht darauf aufmerksam, dass die Technologie genauso als Weiterentwicklung tödlicher Waffen verstanden werden kann: Denn wenn die elektrischen Anlagen von Krankenhäusern oder auch Herzschrittmachern attackiert werden, dürfte dies für die Betroffenen lebensgefährlich sein (Statewatch, 18. April 2013). Zudem ist unklar, inwiefern Fahrzeuglenker nach einer elektromagnetischen Attacke die Kontrolle über das Fahrzeug verlieren und einen Unfall verursachen könnten. Zu klären ist aber auch, ob der polizeiliche Einsatz der Mikrowellenwaffen überhaupt mit der Gesetzgebung in den EU-Mitgliedstaaten vereinbar ist. Auch hier will SAVELEC abhelfen. Als Ergebnis sollen gesetzliche Rahmenbedingungen erarbeitet werden, die auch die Sicherheit von Anwendern und Adressaten der Waffen berücksichtigen.

Mit einem ähnlichen Finanzvolumen forschen mehrere Firmen und Polizeibehörden unter dem Akronym AEROCEPTOR zu Drohnen, die ebenfalls gegen „nicht kooperative Fahrzeuge“ oder Schiffe eingesetzt werden könnten (www.aeroceptor.eu). Dabei geht es nach Ansicht der Fragesteller um Fahrzeuge, in denen unerwünschte Migranten oder Drogen transportiert werden. Laut der Projektbeschreibung seien derartige Maßnahmen immer mehr erforderlich. Getestet wird eine Helikopterdrohne (Vertical Takeoff and Landing – VTOL) der Firma Yamaha. Die Flugroboter sollen mit Netzen ausgerüstet werden, in denen sich Räder oder Propeller verwickeln. Die Rede ist auch von einem „Spezial-Polymerschaumstoff“, der auf der Windschutzscheibe verhärtet und Fahrzeuglenkerinnen und Fahrzeuglenker zum Halten zwingt. Sofern dies nicht weiterhilft, könnten die Fahrzeuge mit „Durchstechen der Reifen“ angehalten werden. Auch eine Störung der Bordelektronik, wie bei SAVELEC, sei denkbar. Das Projekt ist brisant, denn erstmals geht es bei der polizeilichen Nutzung von Drohnen nicht mehr nur um Überwachung.

Auch in Deutschland befassen sich Polizeien mit dem ferngesteuerten Zugriff auf Kraftfahrzeuge. Ziel ist die Überwachung der Fahrenden. Im November 2011 hatte der Arbeitskreis Vorratsdatenspeicherung einen „Leitfaden zum Datenzugriff“ der Generalstaatsanwaltschaft München veröffentlicht (www.cryptome.org/isp-spy/munich-spy-all.pdf). Daraus geht hervor, dass das Landeskriminalamt Bayern die Technik zur Strafverfolgung nutzen möchte: „Ist in einem Kfz ein SIM-Modul (z. B. BMW-Assist/ConnectedDrive […]) eingebaut, so ist dessen Ortung möglich (sowie darüber hinaus alle Varianten des TKÜ-Instrumentariums wie Inhaltsdatenüberwachung od. Verkehrsdatenerhebung)“. Zur gesetzlichen Grundlage heißt es weiter, „seit 12/2009 ist BMW selbst Netzprovider; ist die FIN (Fahrzeugidentifikationsnummer) bekannt, erfolgt eine Bestandsdatenabfrage bei BMW nach § 113 TKG; mittels dieser Daten kann eine TKÜ Maßnahme nach § 100a StPO veranlasst werden“. Sofern keine Katalogtat vorliegt, erklärt das Papier: „liegen Einverständniserklärungen des Herstellers (z. B. BMW) u. des Eigentümers vor, handelt es sich bei der Ortung des SIM-Moduls um keinen Rechtseingriff i. S. des Art. 10 G (Fernmeldegeheimnis)“. Die Staatsanwaltschaft vermerkt, dass dies „rechtl. streitig“ ist und empfiehlt weiter: „Folgende Vorgehensweise: auf privatrechtlicher Schiene wird ein GSM-Tracking über einen LocationBasedService-Dienst (z. B. Fa. Ubinam) realisiert. Der LBS-Diensteanbieter erhält die aktuellen Standortdaten über privatrechtliche Verträge zur Funkzellenortung mit den Netzbetreibern“.

Britische Autoversicherer bieten ihren Kundinnen und Kunden laut einem Bericht der „FAZ“ (1. Februar 2014) günstigere Tarife an, wenn sie in ihrem Auto eine Blackbox installieren, die den Versicherer mit Daten über das Fahrverhalten versorgt. Seit Januar 2014 würde dem Artikel zufolge ein solches Tarifsystem auch in Deutschland erprobt. Hinzukommen neue Kooperationen von Autokonzernen, wie Audi, und IT-Konzernen, wie Facebook oder Google, um anfallende Bewegungsdaten zu vermarkten.

In der Regel ist es für die Besitzerinnen und Besitzer der Fahrzeuge nicht möglich, die vernetzten Funktionen abzustellen oder gar die benötigte Hardware auszubauen. Das Gleiche gilt für die ab dem Jahr 2015 obligatorische Ausstattung mit einer „E-Call-Funktion“.

Wir fragen die Bundesregierung:

1. Auf welche Weise sind deutsche Stellen in das Netzwerk ENLETS eingebunden, und inwiefern arbeiten diese dort mit Europol und FRONTEX zusammen?

   Welche Konsequenzen haben die im Jahr 2013 verabschiedeten Ratsschlussfolgerungen für die Rolle der Deutschen Hochschule der Polizei in Münster sowie des Bundeskriminalamtes (BKA) in ENLETS?

2. Welchen Mehrwert verspricht sich die Bundesregierung von der Einrichtung einer „Technologie-Beobachtungsstelle“ bei ENLETS?

   a) Wie wäre die dort als Ziel niedergelegte „Unterstützung proaktiver Kontakte“ zwischen Industrie und Anwendern aus Sicht der Bundesregierung hinsichtlich der im „Arbeitsprogramm“ von ENLETS festgelegten Schwerpunkte „ANPR, Open Source Intelligence, Signal Intelligence, Surveillance, Front Line Policing, Vehicle Stopping“ umzusetzen?

   b) Welche Maßnahmen hat ENLETS hierzu bereits ergriffen?

3. Inwiefern haben sich Bundesbehörden bereits mit dem im ENLETS-Arbeitsprogramm als „Open Source Intelligence“ beschriebenen Monitoring offener Quellen des Internets für die Nutzung des „front line policing“ befasst, wonach diese vor allem für die Handhabung von Menschenmassen (crowd control) geeignet sei?

   a) Inwiefern haben sich Bundesbehörden bereits mit der im ENLETS-Arbeitsprogramm als „Signal Intelligence“ beschriebenen Nutzung „einer ganzen Reihe von Sensoren“ befasst, die an IT-Systemen der Strafverfolgungsbehörden angeschlossen seien, und inwiefern teilt die Bundesregierung die Einschätzung, dass hierbei öfter Probleme aufträten?

   b) Wie würde die Bundesregierung die von ENLETS aufgeworfenen Fragen nach der meist effektiven Aufklärung elektronischer Signalquellen bei bestmöglicher Integration von Sensoren sowie nach dem benötigten Konzept zur Verarbeitung von immer mehr Daten („What kind of signal intelligence is the most operationally effective and open for integrating the sensors in the EU?“ und „What kind of concept will be needed as ever more data is forwarded for processing and more information needs to be analysed?“) beantworten?

4. Welche Haltung vertritt die Bundesregierung zum Vorschlag von ENLETS, wonach ein ferngesteuertes Anhalten von Fahrzeugen (Remote Stopping Vehicles) serienmäßig in allen, in der EU zugelassenen Fahrzeugen eingebaut werden könnte?

   a) Wie könnte dies aus Sicht der Bundesregierung technisch umgesetzt werden?

b) Inwiefern wären hierfür neue, rechtliche Bestimmungen nötig?

c) Sofern sich die Bundesregierung mit dem ENLETS-Vorschlag noch nicht befasst hat, wann gedenken sich welche Stellen des Bundesministeriums des Innern hierzu zu positionieren?

5. Inwiefern hält die Bundesregierung es überhaupt für nötig, technische Anwendungen zum Anhalten von „nicht kooperativen Fahrzeugen“ zu entwickeln?

6. Inwieweit waren Bundesbehörden bereits selbst mit entsprechenden Überlegungen zur Umsetzung eines ferngesteuerten Anhaltens von Fahrzeugen befasst?

a) Welche „Lösungen“ wurden hierfür in Betracht gezogen?

b) Inwiefern hat es hierzu bereits Kontakte mit privaten Firmen, Automobilkonzernen oder Instituten gegeben?

c) Inwiefern haben sich hieraus kontinuierliche Zusammenarbeitsformen ergeben?

7. Inwiefern haben sich Bundesbehörden des Innern oder der Verteidigung bereits mit dem Anhalten von „nicht kooperativen Fahrzeugen“ durch elektromagnetische Impulse (EMP) oder Mikrowellen (HPM) befasst?

a) Welche „Lösungen“ wurden hierfür in Betracht gezogen?

b) Inwiefern hat es hierzu bereits Kontakte mit privaten Firmen, Automobilkonzernen oder Instituten gegeben?

c) Inwiefern haben sich hieraus kontinuierliche Zusammenarbeitsformen ergeben?

8. Inwiefern haben sich Bundesbehörden bereits mit Länderpolizeien über Möglichkeiten zum Anhalten von „nicht kooperativen Fahrzeugen“ ausgetauscht?

a) Welche „Lösungen“ wurden hierfür in Betracht gezogen?

b) Inwiefern hat es hierzu bereits Kontakte mit privaten Firmen, Automobilkonzernen oder Instituten gegeben?

c) Inwiefern haben sich hieraus kontinuierliche Zusammenarbeitsformen ergeben?

9. Über welche eigenen Erkenntnisse verfügt die Bundesregierung zum EU-Projekt SAVELEC?

a) Inwiefern hält die Bundesregierung die Ausgaben für die Forschung für erforderlich, die bis zum Jahr 2015 Anwendungen entwickeln will, um mit künstlich erzeugten EMP oder HPM die in der Nähe befindliche Elektronik von Fahrzeugen oder Schiffen zu blockieren oder sogar zu zerstören?

b) Inwiefern haben sich Bundesbehörden hierzu mit dem LKA Sachsen-Anhalt ausgetauscht?

10. Worin besteht der Beitrag des Deutschen Zentrums für Luft- und Raumfahrt e. V. (DLR) bei SAVELEC?

a) Was ist der Bundesregierung (beispielsweise über die Mitarbeit des DLR im Projekt) zu den Beiträgen der Otto-von-Guericke-Universität Magdeburg oder der Firma IMST GmbH aus Kamp-Lintfort bei SAVELEC bekannt?

b) Worin bestehen die Beiträge der slowakischen Militärakademie und des Raketenherstellers MBDA?

c) Inwiefern werden nach Kenntnis der Bundesregierung auch Laserwaffen von MBDA bei SAVELEC beforscht?

11. Inwiefern wäre der polizeiliche Einsatz von Mikrowellenwaffen nach Kenntnis der Bundesregierung mit der deutschen Gesetzgebung vereinbar, bzw. welche Änderungen würden nötig?

12. Inwiefern hält die Bundesregierung EU-Ausgaben für das Projekt AEROCEPTOR zu Drohnen, die ebenfalls gegen „nicht kooperative Fahrzeuge“ oder Schiffe eingesetzt werden könnten, für erforderlich?

    Auch wenn die Bundesregierung an AEROCEPTOR nicht selbst beteiligt ist (Bundestagsdrucksache 17/13646), inwiefern teilt sie die Einschätzung der Fragesteller, wonach das Projekt brisant ist, da bei der polizeilichen Nutzung von Drohnen erstmals nicht mehr die Überwachung im Vordergrund steht?

13. Inwiefern hat sich nach Kenntnis der Bundesregierung auch die „Cross-Border Surveillance Working Group“ mit Möglichkeiten zum Anhalten „nicht kooperativer Fahrzeuge“ beschäftigt (Bundestagsdrucksache 17/5677)?

    Sofern es hierzu einen „Erfahrungsaustausch“ oder „Fachvorträge“ gegeben hat, wer hat diese vorbereitet, und welchen Inhalt hatten diese?

14. Worum handelt es sich nach Kenntnis der Bundesregierung bei der „European Tracking Solution“ (ETS, Ratsdokument 10182/13)?

    a) Welche Treffen haben hierzu stattgefunden, und wie haben sich Bundesbehörden bzw. nach Kenntnis der Bundesregierung auch Landesbehörden hierzu eingebracht?

    b) Wer verantwortet das Projekt, und inwiefern ist auch die „Cross-Border Surveillance Working Group“ beteiligt?

    c) Welche Firmen oder Institute sind mit welchen Produkten und Beiträgen an der Entwicklung der ETS beteiligt?

    d) Worin besteht die Neuerung einer ETS gegenüber bereits bestehenden Systemen?

15. Inwiefern und in welchem Umfang haben sich Bundesbehörden möglicherweise bereits über das Verarbeitungs- und Verwertungsverbot von Mautdaten hinweggesetzt, und von der Betreibergesellschaft Toll Collect GmbH erhobene Daten, beispielsweise des GPS oder der On Board Unit, verarbeitet?

16. Inwiefern haben sich Bundesbehörden bereits mit der Möglichkeit der polizeilichen Nutzung des „Elektronischen-Ticket-Systems (eTicketing)“ der Deutschen Bahn AG oder im öffentlichen Personennahverkehr befasst?

    a) Welche Überwachungsmöglichkeiten ergeben sich daraus?

    b) Aufgrund welcher Verordnung könnten Verkehrsdaten herausverlangt werden?

17. Inwiefern trifft es nach Kenntnis der Bundesregierung zu, dass die Bayerische Motoren Werke Aktiengesellschaft (BMW AG) Daten aus den Diensten „BMW ConnectedDrive“, „BMW Assist“ oder „BMW Online“ an Strafverfolgungsbehörden weitergibt?

    a) Wenn ja, welche deutschen oder ausländischen Behörden wurden hierfür von der BMW AG Deutschland bereits in welchem Umfang beliefert, und welche richterlichen Anordnungen müssen dafür vorgelegt werden?

    b) Inwieweit werden Betroffene nach Kenntnis der Bundesregierung durch die BMW AG von einer Auskunft an Behörden benachrichtigt?

c) Bei welcher Stelle innerhalb des Konzerns können Betroffene nach Kenntnis der Bundesregierung Auskunftsersuchen über gespeicherte Daten stellen, und inwiefern werden an Strafverfolgungsbehörden weitergegebene Daten von dort beauskunftet?

18. Inwiefern trifft es nach Kenntnis der Bundesregierung, wie von der Generalstaatsanwaltschaft München beschrieben, zu, dass deutsche Fahrzeughersteller selbst Netzprovider geworden sind, und um welche handelt es sich dabei?

19. Inwiefern haben sich Bundesbehörden bereits mit der Möglichkeit befasst, auf in Fahrzeugen verbaute SIM-Module oder GPS-Module zuzugreifen?

a) Inwiefern und in welchem Umfang wurden bzw. werden diese Möglichkeiten bereits genutzt?

b) Inwiefern wäre die Ortung, Inhaltsdatenüberwachung oder Verkehrsdatenerhebung über einen Zugriff auf die SIM-Module bzw. GPS nach Ansicht der Bundesregierung von der Strafprozessordnung gedeckt?

c) Inwiefern handelt es sich nach Kenntnis der Bundesregierung bei der Ortung des SIM-Moduls oder GPS-Moduls um einen Rechtseingriff im Sinne des Fernmeldegeheimnisses?

20. Inwiefern kann nach Kenntnis der Bundesregierung auf diese Weise über die Fahrzeugidentifikationsnummer eine Bestandsdatenabfrage bei der BMW AG bzw. einem anderen Hersteller/Provider erfolgen?

a) Was ist der Bundesregierung darüber bekannt, ob ein Tracking der Fahrzeuge auch über LocationBasedService-Dienste erfolgt, und um welche Dienste handelt es sich dabei?

b) Inwiefern werden nach Ansicht der Bundesregierung hiermit die rechtlichen Beschränkungen des Fernmeldegeheimnisses umgangen, da der Diensteanbieter die Funkzellenortung über privatrechtliche Verträge betreibt?

21. Inwiefern und mit welchem Ergebnis hat sich das Bundesamt für Sicherheit in der Informationstechnik bereits mit der Möglichkeit befasst, dass Fahrzeughersteller oder auch Dritte auf in Fahrzeugen verbaute SIM-Module oder GPS-Module zugreifen?

22. Was ist der Bundesregierung über die Erprobung eines neuen Tarifsystems von Autoversicherern bekannt, die ihren Kundinnen und Kunden günstigere Tarife anbieten, wenn sie in ihrem Auto eine Blackbox installieren, die den Versicherer mit Daten über das Fahrverhalten versorgt?

a) Was ist der Bundesregierung über die Kooperationen von Autokonzernen, wie die Audi AG, und IT-Konzernen, wie Facebook oder Google, bekannt, um anfallende Bewegungsdaten zu vermarkten?

b) Inwieweit handelt es sich hierbei nach Ansicht der Bundesregierung um eine Verletzung von Bestimmungen des Datenschutzes, zumal diese Systeme von den Fahrzeughalterinnen und -haltern oder -fahrerinnen und -fahrern nicht abzustellen sind?

23. Welche Haltung vertritt die Bundesregierung zur Frage, ob die Besitzerinnen und Besitzer der Fahrzeuge die ab dem Jahr 2015 obligatorische Ausstattung mit einer „E-Call-Funktion“ ausbauen oder abschalten dürfen?

24. Inwieweit hält es die Bundesregierung für wichtig, dass sämtliche GPS-, GSM- oder UMTS-basierten Dienste in Fahrzeugen, in denen diese verbaut sind, derart deaktiviert werden können, dass diese keine Signale mehr senden und empfangen können?

25. Inwiefern unterstützt die Bundesregierung den Vorschlag, ein „No-Spy“-Zertifikat für Neuwagen oder „No-Spy“-Regeln in das Wiener Übereinkommen über den Straßenverkehr aufzunehmen?

    Wenn nein, wie kann sonst verhindert werden, dass Bewegungsprofile oder Halterinformationen der Fahrzeuge ungehindert gespeichert und verarbeitet werden?

Berlin, den 11. 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