4088/J XXV. GP

Eingelangt am 06.03.2015

Anfrage

der Abgeordneten Albert Steinhauser, Freundinnen und Freunde an den Bundesminister für Landesverteidigung und Sport

betreffend Überwachung von Telekommunikation und Versammlungen

BEGRÜNDUNG

Die NGO für BürgerInnenrechte Arbeitskreis Vorratsdatenspeicherung (kurz AK Vorrat) plant anhand eines Handlungskataloges zur Evaluierung von Anti-Terror-Gesetzen (HEAT) unterschiedlichste Formen von staatlicher Überwachung zu beleuchten. Im Rahmen dieses Projekts sind einige Fragen aufgetreten.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Hat Ihre Ministerium, insbesondere Abwehramt und Heeresnachrichtenamt Hinweise darauf, dass die NSA allen Verkehr, der über den Vienna Internet Exchange (VIX) läuft, kopiert und auswertet?
2) Gibt es im BMLVS Bestrebungen, Zugriffsermächtigungen für die Dienste des Bundesheers auf die Glasfaser-Backbones von österreichischen Kommunikationsnetzen zu erhalten beziehungsweise auszuweiten?
3) War das BMLVS oder eine seiner Dienststellen bereits Opfer eines Cyberangriffes?
4) Falls ja, welcher Natur war dieser Angriff und welcher Schaden wurde verursacht, insbesondere welche Daten waren betroffen?
5) Welche Software kommt bei Abwehramt und Heeresnachrichtenamt für den Zweck Open Source Intelligence (OSINT) zum Einsatz?
6) Welche Software kommt bei Abwehramt und Heeresnachrichtenamt für den Zweck von Profiling zum Einsatz?

7) Welche Software wird bei Abwehramt und Heeresnachrichtenamt zur Beobachtung von Nutzern und/oder nutzergenerierten Inhalten im Internet eingesetzt?
8) Welche Software wird bei Abwehramt und Heeresnachrichtenamt zur Identifikation speziell von Gefahrenpotentialen in social-media Plattformen eingesetzt?
9) Welche Software kommt bei Abwehramt und Heeresnachrichtenamt zur Beobachtung von online Foren und sozialen Medien zum Einsatz?
10) Mit welchen social-media-, PR- oder Beratungsagenturen bestehen bei Abwehramt und Heeresnachrichtenamt Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
11) Mit welchen Sicherheitsfirmen, Beratungsagenturen und Dienstleistern im Bereich Netzwerk- und Kommunikationsüberwachung bestehen Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
12) Inwiefern werden die DIANA/DIANGO[1] Systeme in ihrem Vollzugsbereich eingesetzt?
13) Wenn ja, mit welchen Mitteln in welcher Höhe wurden die Projekte DIANA/DIANGO bereits gefördert und welche weiteren Ausgaben sind geplant?
14) An welchen Übungen und Trainings der NATO zum Thema Cyberwar haben Angehörige des Bundesheers bisher teilgenommen?
15) Welche Beziehungen unterhält das Bundesheer zum neuen "Cyber Training Center" der NATO in Estland?
16) Wie viele MitarbeiterInnen des Bundesheeres waren in den vergangenen 5 Jahren auf offiziellen Schulungen bei der deutschen Bundeswehr, um über elektronische Kampfführung unterrichtet zu werden bzw. selbst zu unterrichten?
17) Wie viele MitarbeiterInnen des Bundesheeres waren in den vergangenen 5 Jahren auf offiziellen Schulungen beim US-amerikanischen Militär, um über elektronische Kampfführung unterrichtet zu werden bzw. selbst zu unterrichten?
18) Wie viele MitarbeiterInnen des Bundesheeres waren in den vergangenen 5 Jahren auf offiziellen Schulungen bei militärischen Einrichtungen anderer Staaten, um über elektronische Kampfführung unterrichtet zu werden bzw. selbst zu unterrichten? (bitte auch um Angabe des jeweiligen Staates)
19) Hat das Bundesheer Zugriff auf sogenannte Exploits, die das Eindringen in Computernetze über Sicherheitslücken ermöglichen, etwa von spezialisierten Firmen oder von Individuen erworben?
20) Wenn ja, wie viele solcher Exploits, welchen Typs, zu welchen Preisen und von welchen Firmen und auf welcher Rechtsgrundlage?
21) Unterhält das Bundesheer geschäftliche Beziehungen zu folgenden Firmen, die Exploits und Überwachungssoftware für Behörden anbieten: Vupen

[1] http://derstandard.at/2000004325700/Projekt-Diana-Bundesheer-testet-Internet-Beobachtungssystem

(Frankreich), Digitask (Deutschland), Hacking Team (Italien) oder einem der Unternehmen, die zur deutschen-britischen Gamma Group gehören?

22) Gab es zu einer dieser Firmen in der Vergangenheit geschäftliche Beziehungen?
23) Gab oder gibt es solche Geschäftsbeziehungen des Bundesheers zu Firmen mit einer vergleichbaren Produktpalette?
24) Welche Angriffszenarien auf Computernetze im Bereich "Net Centric Warfare" werden von Angehörigen des Bundesheeres trainiert?
25) Sind auch Angriffsszenarien auf zivile Netze Teil des Trainings?
26) Welche Sicherheitsvorkehrungen bestehen im Bereich MilCert und CNO des Bundesheeres?
27) Dürfen MitarbeiterInnen im Bereich MilCert und CNO des Bundesheeres nebenberuflich selbstständig oder für andere Firmen tätig sein?
28) Werden für diese Tätigkeiten im Bereich MilCert und CNO des Bundesheeres externe Dienstleister eingesetzt?
29) Auf wie vielen Demonstrationen bzw. Zusammenkünften (§22 Abs 7 MBG) in Österreich wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufnahmen durch das Abwehramt erstellt?
30) Auf wie vielen Demonstrationen bzw. Zusammenkünften (§22 Abs 7 MBG) im Ausland wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufnahmen durch das Heeresnachrichtenamt oder das Abwehramt erstellt?
31) Zu welchem Zweck wurden diese Videoaufnahmen verwendet?
32) Nach welcher Zeit werden die Videoaufzeichnungen gelöscht?
33) Auf welcher Rechtsgrundlage wurden die Videos erstellt?
34) Auf wie vielen Demonstrationen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufnahmen von privaten Unternehmen oder Personen für Ermittlungszwecke angefordert?
35) Im Rahmen welcher Demonstrationen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufzeichnungen erstellt oder angefordert?
36) Hinsichtlich wie vieler Personen kam es aufgrund der Auswertung von Videoaufzeichnungen im Rahmen von Demonstrationen jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zur Feststellung der Identität und der Verarbeitung personenbezogener Daten?
37) Findet ein Abgleich von bei Demonstrationen angefertigten Videodaten mit Video-, oder sonstigen Daten vorangehender Demonstrationen statt?
38) An welchen Standorten kommt es zu einem automatisierten Bildabgleich von Überwachungsvideos?
39) Welche Systeme werden für automatisierten Bildabgleich von Überwachungsvideos verwendet?
40) Sofern automatisierte Gefahrenerkennung Teil des Funktionsumfangs solcher Systeme ist, nach welchen Kriterien wird eine angenommene Gefahr bestimmt?

41) An welchen Standorten und Veranstaltungen wurde bzw. wird das System „SECRET – Search of Critical Events in Videoarchives“ [2], „SECRET Search for Critical Events in Videoarchives – interactive”[3] oder ein darauf aufbauendes System eingesetzt oder getestet?
42) An welchen Standorten und Veranstaltungen wurde bzw. wird das System „iObserve“[4], „iObserve NG”[5] oder ein darauf aufbauendes System eingesetzt oder getestet?
43) Wie viele IMSI Catcher[6] welchen Gerätetyps und Modells wurden im Verantwortungsbereich des Ministeriums angeschafft?
44) Wie viele IMSI Catcher im Verantwortungsbereich des Ministeriums besitzen ausschließlich Funktionalität zur Identifikation von Teilnehmern und wie viele sind darüber hinaus auch im Stande Inhalte zu überwachen? [7]
45) Für welche Behörde und welche Abteilung dieser wurde jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 IMSI-Catcher-Ausrüstung angeschafft?
46) Was hat diese gekostet?
47) Welche Datenarten bzw. Kategorien von Daten werden bei einem Einsatz eines IMSI-Catchers erhoben?
48) Von wie vielen Personen wurden Daten im Rahmen des Einsatzes von IMSI Catchern jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 erhoben?
49) Von wie vielen dieser Einsätze von IMSI Catchern jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 wurde lediglich die Funktionalität zur Identifizierung einzelner TeilnehmerInnen genutzt und in wie vielen Fällen wurden darüber hinaus auch Kommunikationsinhalte überwacht?
50) Worin besteht die jeweilige Einsatznotwendigkeit dieser Ausrüstung für die jeweilige Abteilung der jeweiligen Behörde?
51) In wie vielen Fällen kam diese Ausrüstung jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zur Anwendung und in welche Aufgabe nach dem MBG lassen sich diese Fälle einordnen?
52) Aufgrund welcher Rechtsgrundlage werden IMSI-Catcher zum Einsatz gebracht?
53) Welche Vorkehrungen werden getroffen, um die Daten von unbeteiligten Dritten im Einsatzgebiet eines IMSI-Catchers zu schützen?
54) Wurden in der Vergangenheit oder werden aktuell IMSI-Catcher im Rahmen von Demonstrationen eingesetzt?

---

[2] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=24&cHash=c8063d3ebb3a80263621fabe0ded58e0
[3] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=97&cHash=47ffca09ba67f5c0fdf9a26add5b83be
[4] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=18&cHash=1b9806fd280d8f1b648047f8884714e2
[5] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=37&cHash=f44685bc6dd8cbd27f9d664cf5ce64da
[6] http://de.wikipedia.org/wiki/IMSI-Catcher#cite_note-heise_IMSI_catcher-2
[7] siehe Dabrowski et.al. 2014 https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf

55) Falls ja, bei wie vielen Demonstrationen wurden IMSI Catcher jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zum Einsatz gebracht?
56) Wurden in der Vergangenheit oder werden aktuell IMSI-Catcher im Rahmen von Großveranstaltungen eingesetzt?
57) Falls ja, in wie vielen Großveranstaltungen wurden IMSI-Catcher jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zum Einsatz gebracht?
58) Werden die Betroffenen vom Einsatz eines IMSI-Catchers informiert?
59) Wenn nein, warum nicht?