

Kleine Anfrage

der Abgeordneten Jan Korte, Christine Buchholz, Annette Groth, Heike Hänsel, Andrej Hunko, Ulla Jelpke, Petra Pau, Harald Petzold (Havelland), Martina Renner, Dr. Petra Sitte, Frank Tempel und der Fraktion DIE LINKE.

Ermittlungen gegen eine deutsch-britische Software-Firma wegen illegaler Überwachung von Oppositionellen in Bahrain und Deutschland

Das European Center for Constitutional and Human Rights (ECCHR) und die britische Organisation Privacy International haben Anhaltspunkte, wonach bahrainische Behörden unter anderem auch in Deutschland lebende Oppositionelle mithilfe des Gamma-Trojaners FinFisher unrechtmäßig ausgespäht haben. Am 16. Oktober 2014 haben die Organisationen deshalb bei der Staatsanwaltschaft München Strafanzeige gegen Mitarbeiter des deutsch-britischen Konzerns Gamma eingereicht. Den Organisationen liegen Datensätze vor, die den Verdacht begründen, dass Gamma die Überwachungssoftware FinFisher nach Bahrain lieferte sowie technische Hilfe von Deutschland aus leistete. Dadurch konnten laut ECCHR bahrainische Behörden den Trojaner nutzen, um Computer in Deutschland auszuspähen. Die Staatsanwaltschaft hat eine entsprechende Ermittlungsaufnahme indes abgelehnt, obwohl aus Wikileaks-Dokumenten (www.wikileaks.org/spyfiles4/database.html) entsprechende Hinweise und Informationen hervorgehen. Weitere Hinweise, insbesondere zur Situation in Bahrain und zum Einsatz des Gamma-Trojaners FinFisher, lassen sich in etlichen Dokumenten auf der Homepage der Nichtregierungsorganisation Bahrain Watch finden (vgl. www.bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/). Laut Dr. Miriam Saage-Maaß, der stellvertretenden Legal Director des ECCHR, werden in Bahrain Menschenrechtsaktivisten, Journalisten und Oppositionelle systematisch überwacht, verfolgt, inhaftiert und immer wieder auch gefoltert. „Angesichts der Überwachungsrealität in Bahrain ist es absurd, zu sagen, staatliche Behörden könnten gar nicht ‚hacken‘ und gegen § 202a StGB [StGB – Strafgesetzbuch] – dem Verbot der Ausspähung von Daten – verstoßen“ (Pressemitteilung des ECCHR vom 12. Dezember 2014). Die Staatsanwaltschaft München erklärte in ihrem Schreiben an das ECCHR vom 28. November 2014 unter Punkt 2aa), dass das Vorbereiten des Ausspähens von Daten gemäß § 202c StGB generell nicht die Herstellung und den Vertrieb von Software zur Datenerhebung durch staatliche Stellen erfasst, unabhängig davon, ob die Datenerhebung durch den Staat mithilfe der Software rechtmäßig erfolgt.

Nach Informationen des ECCHR geht aus Daten von 77 Computern hervor, dass bahrainische Behörden mit dem Trojaner neben Geräten in Großbritannien auch je einen Computer in Belgien und Deutschland ausgespäht haben. In Großbritannien waren davon unter anderem prominente bahrainische Menschenrechtsaktivisten betroffen. Die Identität der in Deutschland ausspionierten Person ist bisher nicht bekannt.

Auch in Großbritannien und Belgien liegen derzeit Strafanzeigen gegen die Firma Gamma International, die FinFisher entwickelt und produziert hat, vor.

Werbematerial der Firma zeigt, dass die Software den umfassenden Zugriff auf infizierte Geräte und alle enthaltenen Daten ermöglicht. Dazu gehört auch, dass Kameras und Mikrofone an Computern angezapft werden können. Laut Privacy International wird FinFisher-Software in 35 Ländern, darunter Äthiopien, Turkmenistan, Bahrain und Malaysia, eingesetzt.

Da selbst das Bundeskriminalamt mindestens bis zum Jahr 2012 auf den Einsatz einer Version des Gamma-Trojaners verzichtete, weil die Software gegen die „standardisierende Leistungsbeschreibung“ der Bundesregierung (www.netzpolitik.org vom 21. August 2014 „Geheimes Dokument: Bundeskriminalamt darf FinFisher/FinSpy nicht einsetzen, versucht einfach neue Version nochmal“) und damit gegen verfassungsrechtliche Mindeststandards verstieß, wirft das ECCHR der Staatsanwaltschaft München außerdem vor, durch die Entscheidung keine Ermittlungen gegen Gamma International einzuleiten, die Rechtslage in Deutschland zu ignorieren.

Wir fragen die Bundesregierung:

1. Haben die Bundesregierung und deutsche Sicherheitsbehörden Kenntnis über die Ausspähung in der Bundesrepublik Deutschland lebender Oppositioneller mithilfe des Gamma-Trojaners FinFisher, und wenn ja, durch wen erfolgt die Überwachung und wer ist davon betroffen?
2. Ist der Bundesregierung bekannt, ob auch Rechner und Informationssysteme von an Asylverfahren beteiligten Einrichtungen, vor allem des Bundes, Ziel der Ausspähung durch Geheimdienste von Staaten sind, die Oppositionelle verfolgen?
 - a) Sind der Bundesregierung derartige Angriffe bekannt, und wenn ja, auf welche Einrichtungen sind diese wann, von wem und mit welchem Ziel jeweils erfolgt, und welche Konsequenzen seitens der Sicherheitsbehörden, des Bundesamts für Sicherheit in der Informationstechnik oder des Bundesamtes für Verfassungsschutz hatte dies jeweils?
 - b) Sind der Bundesregierung grundsätzlich Angriffe auf die Kommunikationsinfrastruktur des Bundes bekannt, die mit Produkten der Gamma-Firmengruppe verübt wurden?
3. Wie beabsichtigt die Bundesregierung ihrer Schutzpflicht gegenüber ihren Bürgerinnen und Bürgern aber auch gegenüber Asylsuchenden in Deutschland nachzukommen, sie vor Zugriffen ausländischer Geheimdienste zu schützen?
4. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus den auf der Wikileaks-Plattform veröffentlichten Dokumenten zur Gamma-Firmengruppe im Hinblick auf ihre Beweiskraft?

Befürwortet die Bundesregierung, dass gegen das Unternehmen Ermittlungen erfolgen?
5. Welche Maßnahmen wird die Bundesregierung in Bezug auf den Inhaber der IP-Adresse 217.86.164.76 ergreifen, der laut im August 2014 veröffentlichter Dokumente möglicherweise seit 2011 in Deutschland vom bahrainischen Geheimdienst ausgespäht wird?
6. Stimmt die Bundesregierung der Auffassung der Staatsanwaltschaft München zu, wonach das Vorbereiten des Ausspähens von Daten gemäß § 202c StGB generell nicht die Herstellung und den Vertrieb von Software zur Datenerhebung durch staatliche Stellen erfasst, unabhängig davon, ob die Datenerhebung durch den Staat mithilfe der Software rechtmäßig erfolgt?

7. Ist die Bundesregierung Hinweisen darauf, dass Gamma International bzw. FinFisher Labs GmbH kontinuierlich Updates an Bahrain liefert bzw. die Technologie wartet, nachgegangen (www.netzpolitik.org vom 2. August 2014 „Gamma FinFisher: Überwachungstechnologie „made in Germany“ gegen Arabischen Frühling in Bahrain eingesetzt (Update)“ und www.spiegel.de vom 8. August 2014 „FinFisher-Software: Kundendienst half bei Überwachung in Bahrain“)?
 - a) Würden solche Wartungen im Zusammenhang mit Bahrain nach Ansicht der Bundesregierung einen Einzeleingriff gemäß § 6 des Außenwirtschaftsgesetzes (AWG) rechtfertigen bzw. gegen die geänderte Europäische Verordnung (EG) Nr. 428/ 2009 (EG-Dual-Use-Verordnung) verstoßen?
 - b) Liegen der Bundesregierung entsprechende Anträge der Gamma- bzw. FinFisher-Firmengruppe oder des Unternehmens Elaman vor?
8. Wie viele Lieferungen von Überwachungstechnologie und Zensursoftware an Drittstaaten wurden im Zuge der vom Bundesminister für Wirtschaft und Energie, Sigmar Gabriel, am 19. Mai 2014 angekündigten strengeren Kontrolle des Exports von Überwachungstechnologie und Zensursoftware durch den Zoll auf Grundlage des Instruments des Einzeleingriffs gemäß § 6 AWG untersagt (bitte mit Exportgut und Empfängerland konkret angeben)?
9. Wie viele Lieferungen von Überwachungstechnologie und Zensursoftware an Drittstaaten sind seit der Ankündigung des Bundesministers für Wirtschaft und Energie, Sigmar Gabriel, vom 19. Mai 2014 nach Kenntnis der Bundesregierung erfolgt (bitte mit Exportgut und Empfängerland konkret angeben)?
10. Wie bewertet die Bundesregierung den Einsatz des FinFisher-Trojaners in Deutschland in rechtlicher Hinsicht?
11. Inwieweit treffen Berichte zu (www.sueddeutsche.de vom 15. April 2014 „Allianz gegen die Feinde des Internets“ und www.ndr.de vom 7. Dezember 2011 „Exporthilfe für Überwachungstechnologie“), dass es außer den zwei zugestandenen Hermesbürgschaften für Überwachungstechnologie in den Jahren 2005 und 2006 weitere Hermesbürgschaften für solche Software gegeben hat?
12. Wie erklärt die Bundesregierung ihre widersprüchlichen Angaben gegenüber den Bundestagsabgeordneten und der Presse zum Export von Überwachungssoftware (vgl. Süddeutsche Online vom 28. November 2014)?
13. Wann genau hat das Bundeskriminalamt von der Gamma- bzw. FinFisher-Firmengruppe den Staatstrojaner FinSpy 4.20 gekauft, wie hoch waren die Kosten, und wie oft wurde dieser mittlerweile eingesetzt?
14. Sofern der Staatstrojaner FinSpy 4.20 nicht eingesetzt wurde, worin bestanden bzw. bestehen die Gründe?
15. Welche andere Version des FinSpy-Trojaners wurde bzw. wird im Bundeskriminalamt eingesetzt (bitte nach Version und Anzahl der eingesetzten Fälle aufschlüsseln)?
16. Inwiefern und mit welcher Begründung trifft es zu, dass die Firma CSC Deutschland Solutions GmbH letztes Jahr festgestellt hatte, dass die Software in der Version 4.20 gegen deutsches Recht verstößt bzw. verstieß (www.netzpolitik.org vom 8. Januar 2015 „Informationsfreiheits-Ablehnung des Tages: Informationsfreiheits-Bbeauftragte lehnt Anfrage zu illegalem Trojaner ab“)?

17. Wird von der CSC ein Vorschlag gemacht, wie der Einsatz der Version 4.20 technisch und rechtlich ermöglicht werden könnte, und wenn ja, wie sieht dieser aus?
18. Aus welchen Gründen ist der CSC-Prüfbericht als geheim eingestuft, und wann wurde er wie dem Deutschen Bundestag zugänglich gemacht?

Berlin, den 23. Januar 2015

Dr. Gregor Gysi und Fraktion