Deutscher Bundestag **Drucksache 20/683**

20. Wahlperiode 15.02.2022

Antrag

der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Anke Domscheit-Berg, Dr. André Hahn, Jan Korte, Ina Latendorf, Petra Pau, Sören Pellmann, Dr. Petra Sitte und der Fraktion DIE LINKE.

Kein Kauf und Einsatz von Spähsoftware durch Bundesbehörden

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die Geschichte des Kaufs von Überwachungssoftware, mit der heimlich verschlüsselte Kommunikation ausgeleitet oder auf Datenträger zugegriffen werden kann, ist von zahlreichen Skandalen überschattet. Die vom Bundeskriminalamt und anderen Bundesbehörden beschaffte Software wie beispielsweise „FinFisher“ oder „Pegasus“, auch „Staatstrojaner“ genannt, konnte entweder mehr, als vom Gesetzgeber zugelassen war, oder leitete abgefangene Daten über Server der Softwarehersteller im Ausland an die zuständigen Behörden. Diese Hersteller kooperieren regelmäßig auch mit autoritären und diktatorischen Regimes. Zudem sind diese Spähprogramme darauf angewiesen, Schwachstellen in der IT-Sicherheit zu nutzen, die auch durch andere Akteure – Geheimdienste oder kriminelle Unternehmen – genutzt werden können.

Wo „Staatstrojaner“ zum Einsatz kommen, um vermutete Gefahren zu erforschen oder verfassungsfeindliche Bestrebungen zu durchleuchten, stellt ihr Einsatz einen unverhältnismäßigen Eingriff in das IT-Grundrecht der Betroffenen dar. Schon nach dem Strafprozessrecht können solche Eingriffe im Vorfeld von konkreten Straftaten gegen Leib und Leben oder die Freiheit der Person vorgenommen werden. Eine noch weiter gehende Verlagerung eines so tiefen Eingriffs in die Privatsphäre in das Vorfeld des Vorfeldes einer möglichen Gefahr steht in keinem angemessenen Verhältnis zum möglicherweise erreichbaren Ziel.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. den Kauf von Spähsoftware von kommerziellen Anbietern umgehend einzustellen, und den Einsatz von bereits erworbener Spähsoftware bei den Nachrichtendiensten und im Bereich der polizeilichen Gefahrenabwehr bei Behörden des Bundes umgehend zu untersagen;
2. einen Gesetzentwurf vorzulegen, mit dem die Befugnisse der Nachrichtendienste und der Polizeibehörden des Bundes in der Gefahrenabwehr zum Einsatz von Spähsoftware aufgehoben werden.

Berlin, den 15. Februar 2022

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Begründung

Im Jahr 2014 wurde bekannt, dass die deutsch-britische Firma Gamma eine Überwachungssoftware namens FinFisher nach Bahrain geliefert hatte, wo sie zur Ausspähung von Oppositionellen eingesetzt wurde, darunter auch solche mit Wohnsitz in Deutschland. Das Bundeskriminalamt hatte die Software FinFisher 2012 ebenfalls erworben, allerdings nicht eingesetzt, weil sie deutlich mehr konnte, als nach deutscher Rechtslage zulässig war (vgl. BT-Drs. 18/4008). Dies konnte allerdings erst nach Tests der Software festgestellt werden, weil der Quellcode nicht offengelegt wurde und deshalb den hoheitlichen Stellen unbekannt war. Im Jahr 2021 wurde bekannt, dass das Bundeskriminalamt eine Software zur Durchführung von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung namens „Pegasus“ von der israelischen Firma „NSO Group“ gekauft hatte, die ebenfalls zunächst an die deutsche Rechtslage angepasst werden musste (tagesschau.de vom 7.9.2021, „BKA kaufte Spionagesoftware bei NSO“). Die „NSO Group“ stand im Verdacht, die Spähsoftware „Pegasus“ auch an staatliche Akteure verkauft zu haben, die sie zur Ausspähung von Oppositionellen, Journalist*innen und Mitgliedern von Regierungen und Auslandsvertretungen einsetzten (vgl. BT-Drs. 19/32246). Laut Medienberichten wurden die vom BKA überwachten Telefonnummern der NSO-Group nicht bekannt gemacht, sondern mit hash-Werten versehen; es ist also davon auszugehen, dass die abgehörten Telefonate bzw. ausgespähten Daten nicht unmittelbar an das BKA, sondern zunächst an die NSO Group ausgeleitet und von dort an das BKA weitergegeben wurden (tagesschau.de vom 7.9.2021, „BKA soll Seehofer nicht informiert haben“). In diesem Fall hätte das BKA nicht einmal Maßnahmen ergreifen können, um die Weiterleitung der Daten an Dritte wirksam zu unterbinden. Im Ergebnis bedeutet das: der Einsatz von Trojanern gefährdet durch die Nutzung noch ungeschlossener Sicherheitslücken in digitalen Endgeräten und Anwendungen nicht nur allgemein die IT-Sicherheit. Es werden sogar weitere Sicherheitsrisiken geschaffen. Erst recht gilt dies hinsichtlich des Geschäftsmodells der Softwareschmieden in diesem Sektor: ihr Hauptgeschäft machen sie nicht mit demokratischen Rechtsstaaten, sondern mit Diktatoren und autoritären Staatsführungen. Wer ihre Produkte kauft und ihrer Erzählung vom Kampf gegen Terrorismus und Organisierte Kriminalität, zu deren Bekämpfung ihre Produkte eingesetzt würden, so Legitimität verschafft, macht sich die Hände mit schmutzig. Ein Verzicht auf den Ankauf solcher Produkte sollte dabei in eine Strategie eingebunden sein, solchen Firmen auch international das Handwerk zu legen. Es darf keine Kommerzialisierung von Überwachung geben.

Das Bundesverfassungsgericht hat in mehreren Entscheidungen die Leitplanken einer grundrechtlichen Einhegung der staatlichen Zugriffsmöglichkeiten auf digitale Geräte skizziert. Der Gesetzgeber hat in den vergangenen Legislaturperioden die Linie verfolgt, immer genau an diesen Leitplanken entlang zu rasen. Ratsamer wäre jedoch, einen Sicherheitsabstand einzuhalten. Mit der Ausweitung des Terrorismusstrafrechts weit in das Vorfeld konkreter Anschlagshandlungen und Schutzgutverletzungen wurde das Recht der polizeilichen Gefahrenabwehr noch weiter in das Vorfeld des Vorfelds vorverlagert; Geheimdienste sollen sogar noch davor aktiv werden. Gefahrenabwehr- und Geheimdienstbefugnisse richten sich so gegen Gefahren, die sich noch sehr im Ungefähren bewegen bzw. noch gar nicht oder nur mutmaßlich bestehen. Die Überwachung von Smartphones und PCs stehen als tiefe Eingriffe in das Recht auf Sicherheit, Integrität und Verfügbarkeit von Geräten und Daten (IT-Grundrecht) in keinem Verhältnis zu diesen lediglich nur ungefähr sich abzeichnenden Gefahren. Erst recht gilt das für Maßnahmen insbesondere des Bundesamtes für Verfassungsschutz bei der Beobachtung von (vermeintlich) verfassungsfeindlichen Bestrebungen. Das Bundesverfassungsgericht hat mit der Konstruktion, eine Gefahr sei auch schon dann hinreichend konkretisiert, „wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt“, jedenfalls „sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr (…) hinweisen“, für die Auseinandersetzung keinen hilfreichen Beitrag geleistet. Leider hat auch der Gesetzgeber wenig Mühe aufgewendet, diese Konstruktion des Gerichts in die gängigen Rechtsbegriffe des polizeilichen Gefahrenabwehrrechts zu übersetzen. So klagen auch die Behörden selbst über das

Problem, die Befugnisse rechtssicher anzuwenden. Es ist ohnehin eine umfassende Revision der Sicherheitsgesetzgebung der vergangenen Jahre angezeigt. Diese kann der von den Koalitionsparteien verabredeten Evaluation der Sicherheitsgesetze und einer „Überwachungsgesamtrechnung“ vorbehalten bleiben; hier ist die Unverhältnismäßigkeit der Befugnis aber so evident, dass sie bereits jetzt gestrichen werden muss.