Rede im Europaparlament

Staatstrojaner gefährden nationale und europäische Sicherheit

Staatliches Hacken schafft keine Sicherheit, sondern Unsicherheit. Die Europäische Union muss handeln und den Verkauf und Einsatz von Staatstrojanern verbieten. Das habe ich dem Pegasus-Untersuchungsausschuss im Europaparlament gesagt. Wir veröffentlichen das Video und mein Eingangsstatement. Update: Und ein Transkript.

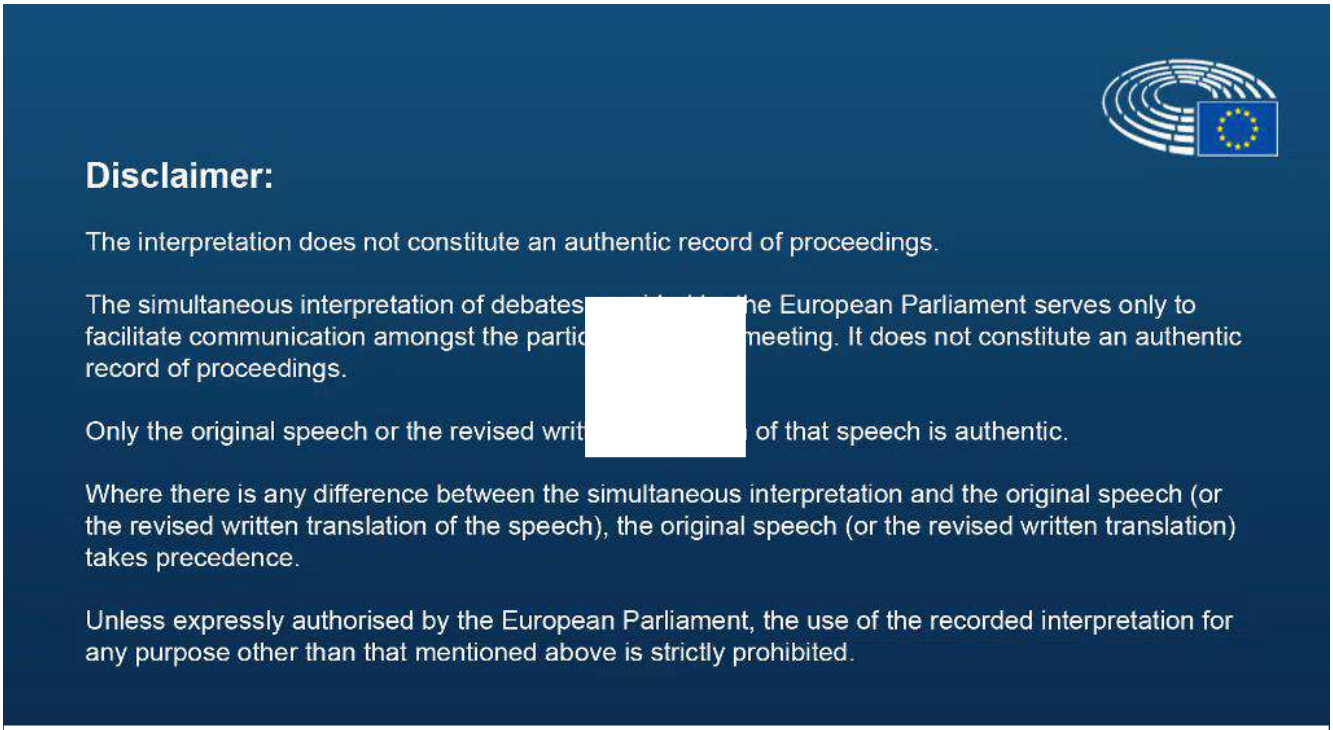
15.11.2022 um 12:27 Uhr - Andre Meister - in Überwachung - 3 Ergänzungen

Andre Meister und der Ausschuss-Vorsitzende.
– Alle Rechte vorbehalten Pegasus-Untersuchungsausschuss

Seit April tagt im Europaparlament ein Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware. Am Montag, den 14. November, veranstaltete der Ausschuss eine Anhörung zum Thema des Ausschusses in Deutschland. Ich durfte dort als Sachverständiger sprechen.

Von der Anhörung gibt es eine Video-Aufzeichnung. Hier veröffentlichen wir die übersetzte Version meines Eingangsstatements.

Update: Wir veröffentlichen auch ein inoffizielles Transkript der Sitzung. (Danke, Julien.)



Eingangsstatement

Sehr geehrte Abgeordnete

Vielen Dank für die Einladung, über staatliches Hacken und sogenannte Spyware in Deutschland zu sprechen.

Ich bin investigativer Journalist und arbeite für das Medium netzpolitik.org in Berlin. Wir recherchieren und berichten seit über einem Jahrzehnt über staatliches Hacken. In meiner Freizeit bin ich auch Mitglied im Chaos Computer Club und Beobachter bei European Digital Rights, aber heute spreche ich nicht in deren Namen.

Ich bin überrascht, dass ich der einzige Experte in der heutigen Anhörung bin. Ich verstehe, dass meine Kolleg:innen aus der Zivilgesellschaft einfach nicht genug Ressourcen hatten. Die Staatsanwaltschaft München war zwar interessiert, darf aber aus rechtlichen Gründen nicht öffentlich über die laufenden Ermittlungen gegen FinFisher sprechen.

Aber dass die Bundesregierung und das Bundeskriminalamt die Einladung dieses Ausschusses abgelehnt haben, ist beschämend. Mit der Weigerung, hier auszusagen, reiht sich Deutschland in die lange Liste der Länder ein, die nicht bereit sind, bei Ihren wichtigen Untersuchungen mitzuarbeiten.

Ich werde zeigen, dass dieses Verhalten symptomatisch ist und dass Deutschland viele der Probleme in den anderen Ländern, die Sie untersuchen, teilt.

Da das heutige Thema sehr umfangreich ist und ich der einzige Experte bin, der erschienen ist, hat mir der Vorsitzende freundlicherweise erlaubt, etwas länger zu sprechen.

In meinem Beitrag werde ich mich auf den Einsatz von Staatstrojanern in Deutschland konzentrieren, da das Kapitel dazu im Entwurf ihres Berichts noch kurz und oberflächlich ist. Ich bin auch gerne bereit, Informationen über deutsche Firmen wie FinFisher und andere zu geben. Aber mit Rücksicht auf die Zeit werde ich das für die Fragen und Antworten aufheben.

Ich werde zunächst die Geschichte des staatlichen Hackens in Deutschland skizzieren und die Fälle, in denen es eingesetzt wird. Dann werde ich den rechtlichen Rahmen und ein spezielles neues Grundrecht in Deutschland erklären. Drittens werde ich die Produkte nennen, die Deutschland gekauft und entwickelt hat. Dann werde ich die Geheimhaltung und mangelnde Rechenschaftspflicht des staatlichen Hackens in Deutschland verdeutlichen. Abschließend werde ich eine lobenswerte Initiative der deutschen Regierung vorstellen, einen wichtigen Aspekt dieses Problems zu regulieren.

Definition: Staatstrojaner statt Spähsoftware

Lassen Sie mich mit einer Bemerkung zur Definition beginnen. Im öffentlichen Diskurs in Deutschland sprechen wir nicht von „Spyware“. Dieser Begriff ist unpräzise und überspezifisch.

Stattdessen sprechen wir von „Staatstrojanern“ oder „staatlichem Hacken“. Das trifft besser, worum es geht: in IT-Systeme einzudringen, heimlich, ohne Wissen des Besitzers,

indem man sie hackt, ihre Integrität und Vertraulichkeit bricht und die Kontrolle über sie übernimmt.

Natürlich ist das Hauptziel Überwachung, aber staatliches Hacken wird auch eingesetzt, um IT-Systeme zu sabotieren und zu stören oder um belastende Beweise zu platzieren, wie wir es bei der Polizei in Indien gesehen haben. Der Unterschied besteht, wenn überhaupt, nur in einer Handvoll Zeilen Code.

Außerdem geht es nicht nur um Smartphones, auch wenn diese die meiste Aufmerksamkeit auf sich ziehen. Jedes erdenkliche digitale Gerät kann und wird gehackt werden. Das reicht von Laptops und Armbanduhren über Fernseher und Hausautomatisierung bis hin zu Servern und Routern und natürlich dem Internet der Dinge. Es umfasst sogar Autos und Flugzeuge, die jetzt Computer sind, in die wir unseren Körper stecken, und medizinische Implantate, also Computer, die wir in unseren Körper stecken.

Um all dies zu berücksichtigen, verwende ich den Begriff „Staatliches Hacken".

Geschichte: 20 Jahre staatliches Hacken

Deutsche staatliche Stellen hacken schon seit mindestens 20 Jahren.

Im Jahr 2005 hackte der Auslandsgeheimdienst BND die afghanische Regierung und las E-Mails zwischen einem afghanischen Minister und einer deutschen Journalistin mit – was illegal ist. Im Jahr 2006 hackte der BND ein Hotel in der Demokratischen Republik Kongo. Dabei las ein deutscher Spion die E-Mails eines deutschen Soldaten, der mit der Ehefrau eines anderen deutschen Agenten flirtete – was ebenfalls illegal ist.

Der Auslandsgeheimdienst hackt nicht, um Verbrechen aufzuklären. Es ist auch nicht seine Aufgabe, Terrorismus zu bekämpfen – das ist Aufgabe der Polizei. Spione hacken meist für klassische Spionage. Die Geheimdienste führen wahrscheinlich die Liste der staatlichen Hacks an. Im Jahr 2009 hatte der BND bereits über 2.500 Geräte gehackt.

Ein weiterer wichtiger staatlicher Hacker ist das Militär. Im Jahr 2015 hackte die Bundeswehr einen afghanischen Mobilfunkbetreiber. Dies beweist, dass es beim Hacken nicht nur um einzelne Ziele geht, sondern auch um ganze Infrastrukturen und Netzwerke.

Leider gibt es nur sehr wenige Informationen über Hacks von Geheimdiensten und Militärs, obwohl diese den Großteil des staatlichen Hackens ausmachen. Die wenigen

Fälle, von denen wir wissen, wurden nur dank investigativem Journalismus bekannt, weil es sich in diesen Fällen um illegale Aktivitäten handelte, die zu Aufsichtsmaßnahmen führten.

Fälle: Drogen und Betrug statt Terror und Mord

Der Zoll und die Polizei in Deutschland hacken seit mindestens 2008. Die ersten Ziele, die bekannt wurden, waren Verdächtige, die Anabolika, gefälschtes Viagra und geschmuggelte Zigaretten verkauften. Der letztgenannte Fall war erfolglos, weil der Staatstrojaner unbeabsichtigt die Festplatte des Zielcomputers beschädigte.

Wie Sie sehen, handelt es sich hier nicht um den Terror oder die Schwerstverbrechen, die Befürworter:innen als Rechtfertigung für staatliches Hacken anführen. Und es funktioniert auch nicht problemlos.

Aber das sind bis heute typische Fälle. Im Jahr 2013 wurde die Polizei beauftragt, ihre Forderung nach staatlichem Hacken zu begründen. Sie sammelten eine Liste von fast 300 Ermittlungsverfahren mit schweren Straftaten, bei denen die Polizei behauptete, sie müsse Verdächtige hacken.

Diese Stichprobe ist wissenschaftlich nicht zuverlässig. Die Daten belegen auch weder die Notwendigkeit noch die Verhältnismäßigkeit, da sie nicht berücksichtigen, ob die Ermittlungen auch ohne staatliches Hacken erfolgreich waren oder ob die Verdächtigen unschuldig waren.

Aus der Statistik ging jedoch hervor, wofür die Polizei die Staatstrojaner wirklich einsetzen wollte. Bei über der Hälfte der Fälle handelte es sich um Drogendelikte. Fast ein Viertel waren Eigentumsdelikte, Betrug, Raub und Erpressung.

Im Parlament wurden die Staatstrojaner-Gesetze mit „Bildung einer kriminellen Vereinigung, Straftaten gegen die sexuelle Selbstbestimmung, Kinderpornografie, Mord und Totschlag“ begründet. Die eigenen Daten der Polizei zeigten jedoch null Fälle von Bildung einer kriminellen Vereinigung, null Fälle von Straftaten gegen die sexuelle Selbstbestimmung, null Fälle von Kinderpornografie und null Fälle von Mord und Totschlag.

Diese Zahlen sind vergleichbar mit dem klassischen Abhören von Telefon- oder Internetverbindungen. Und jedes Jahr bestätigen die offiziellen Statistiken, dass sie auch in der Praxis zutreffen.

Im Jahr 2019 durfte die deutsche Polizei 64 Mal hacken und tat dies auch 15 Mal. In mehr als einem Drittel der Fälle ging es um Erpressung, in einem weiteren Drittel um Drogen. Es gab null Fälle von Terror und null Fälle von Mord.

Im Jahr 2020, dem Jahr, für das uns die aktuellsten Zahlen vorliegen, wurden der deutschen Polizei 48 Staatstrojaner-Einsätze bewilligt, von denen 22 tatsächlich durchgeführt wurden. Wiederum waren mehr als ein Drittel der Fälle Drogen, ein weiteres Drittel waren Erpressungen, es gab null Fälle von Mord.

Das zeigt, dass staatliches Hacken von Anfang an öffentlich mit Terror und Mord begründet wird, aber fast nie wegen Terror und Mord eingesetzt wird.

Zivilgesellschaft: Landesverrat und Klima-Proteste

Erlauben Sie mir eine persönliche Geschichte. Im Jahr 2015 hat der Präsident des Bundesverfassungsschutzes persönlich Strafanzeige gegen mich und meine Kollegen erstattet und uns nichts Geringeres als Landesverrat vorgeworfen, weil wir unseren Job gemacht haben: wahrheitsgemäße Informationen im öffentlichen Interesse zu berichten über die Internet-Überwachung seiner Behörde.

Die strafrechtlichen Ermittlungen wurden später eingestellt, aber die extremen Anschuldigungen gaben der Polizei das gesamte Arsenal an Überwachungsmöglichkeiten – zu denen zwei Jahre später auch staatliches Hacken gehören sollte.

Das vorliegende Thema ist für mich also mehr als nur theoretisch. Deshalb möchte ich diese Gelegenheit nutzen und meine Solidarität mit allen Journalist:innen und Menschenrechtsverteidiger:innen auf der ganzen Welt zum Ausdruck bringen, die von staatlichem Hacken ins Visier genommen wurden, um sie einzuschüchtern, zu unterdrücken und zum Schweigen zu bringen. Kämpft weiter.

Die Fälle, die wir kennen, liegen alle in der Vergangenheit, aber wir müssen an die Zukunft denken.

In Deutschland spioniert der Verfassungsschutz antifaschistische Menschenrechtsverteidiger und Klimaaktivist:innen aus. In diesem Moment sitzen in Deutschland zwölf Klimaaktivist:innen im Gefängnis, ohne dass sie wegen eines Verbrechens verurteilt oder auch nur angeklagt wurden. Die Polizei hat sie einen ganzen Monat lang in so genannten „Präventivgewahrsam“ genommen, um sie davon abzuhalten, auf der Straße zu protestieren.

In diesem politischen Klima braucht man nicht viel Fantasie, um sich vorzustellen, dass auch in Deutschland Journalist:innen, Menschenrechtsverteidiger:innen und Aktivist:innen früher oder später zur Zielscheibe staatlicher Hackerangriffe werden.

Es ist Ihre Aufgabe, zu handeln und dies zu verhindern.

Gesetz: Immer wieder Ausweitung

Werfen wir einen Blick auf den rechtlichen Rahmen in Deutschland. Das erste Bundesgesetz, das der Polizei ausdrücklich Staatstrojaner erlaubt, war das Bundeskriminalamtgesetz 2008. Es beschränkte das staatliche Hacken auf das Bundeskriminalamt, auf den internationalen Terrorismus und die Verhinderung von Terroranschlägen.

Seitdem haben Landes- und Bundesgesetze den Anwendungsbereich und die Nutzung von staatlichem Hacken kontinuierlich erweitert. Seit 2017 erlaubt die Strafprozessordnung staatliches Hacken für alle Strafverfolgungsbehörden und für eine lange Liste von 42 Straftaten, darunter Steuerhinterziehung, die Verleitung zur missbräuchlichen Asylantragstellung – und natürlich Drogendelikte.

Letztes Jahr hat ein neues Gesetz das staatliche Hacken für alle 19 deutschen Geheimdienste offiziell legalisiert, obwohl mindestens die Geheimdienste des Bundes dies bereits ohne ein spezielles Gesetz getan haben.

Dieses Gesetz verpflichtet auch Kommunikationsanbieter, den Staat beim Hacken zu unterstützen, indem sie staatliche Hardware in ihren Netzen installieren, um Machine-in-the-Middle-Angriffe gegen ihre Kund:innen zu ermöglichen. Die Kommunikationsanbieter kritisierten dies vehement und beklagen Risiken für die Integrität ihrer Infrastruktur, einen Vertrauensverlust und einen Angriff auf die IT-Sicherheit.

Grundrecht auf Vertraulichkeit und Integrität

Die deutschen Staatstrojaner-Gesetze werden regelmäßig vor Gericht angefochten. Als Reaktion darauf hat das Bundesverfassungsgericht 2008 ein neues Grundrecht geschaffen: das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen“.

Das höchste deutsche Gericht sagt, dass staatliches Hacken nur dann legal sein kann, „wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder

solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt."

Das ist der Terrorismus und die schwerste Kriminalität, von der wir immer hören. Das ist jedoch nicht, was tatsächlich passiert.

Juristischer Trick: Zwei Arten des Hackens

Um dieses wegweisende Urteil und das neue Grundrecht zu umgehen, hat sich die deutsche Polizei einen juristischen Trick einfallen lassen. Sie erfand zwei verschiedene Arten des Hackens. Bei der einen hacken sie ein Gerät und haben Zugriff auf alle Daten auf diesem Gerät. Sie nennen dies „Online-Durchsuchung".

Bei der anderen hacken sie ein Gerät, und obwohl sie technisch gesehen Zugang zu allen Daten auf diesem Gerät haben, beschränken sie sich auf das Abhören und Aufzeichnen von laufender Kommunikation. Sie nennen dies „Quellen-Telekommunikationsüberwachung". Sie wurde sogar in denselben Paragraf der Strafprozessordnung aufgenommen, in dem die klassische „Telekommunikationsüberwachung" beschrieben wird.

Diese absichtliche Umdeutung des aktiven staatlichen Hackens zu wenig mehr als passives Abhören von Telefonen ist eine Verhöhnung des vom Verfassungsgericht verkündeten neuen Grundrechts. Es bleibt abzuwarten, ob es vor Gericht Bestand haben wird, da verschiedene Verfassungsbeschwerden noch anhängig sind.

Die Neuregelung hat auch in der Praxis zu Fehlern und Irrtümern geführt. Die Staatsanwaltschaften haben bei ihren Ermittlungen immer wieder die klassische Telefonüberwachung mit dem aktiven staatlichen Hacken verwechselt. Dabei sind sie Strafrechts-Experten.

Aus technischer Sicht ist die Unterscheidung zwischen zwei Arten von Hacken, die darauf beruht, welche Art von Daten man nach dem Hacken ausleitet, künstlich und willkürlich. Sobald man ein Gerät gehackt hat, hat man Zugriff auf das gesamte Gerät, einschließlich aller Daten und Sensoren. Um sich auf die Kommunikation in bestimmten Apps zu beschränken, braucht man neuen, zusätzlichen Quellcode und neue Funktionalitäten.

Deshalb gibt es in Deutschland besondere Anforderungen beim Kauf von kommerziellen Staatstrojanern. Im Jahr 2013 kaufte das Bundeskriminalamt FinSpy von FinFisher. Standardmäßig war FinSpy jedoch nur in der Lage, alle Daten auf dem

Zielgerät auszuleiten. Daher forderte die Polizei FinFisher auf, zusätzlichen Quellcode zu entwickeln, um die Leistung des Produkts zu begrenzen. FinFisher brauchte fünf Jahre und drei Versionen, bis das Produkt den gesetzlichen Anforderungen entsprach.

Das ist auch der Grund, warum die deutsche Polizei Pegasus nicht sofort gekauft hat. BKA und NSO trafen sich zum ersten Mal im Jahr 2017. Aber auch hier dauerte es Jahre der Verhandlungen und der zusätzlichen Arbeit von NSO, um eine modifizierte Version zu entwickeln. Die deutsche Polizei kaufte Pegasus schließlich Ende 2020. Seitdem haben sie Pegasus mindestens ein halbes Dutzend mal eingesetzt.

Produkte: DigiTask, RCIS, FinFisher, Pegasus

Das bringt mich zu den in Deutschland verwendeten Produkten. Leider haben wir so gut wie keine Informationen über das Militär und die Geheimdienste, abgesehen davon, dass der BND auch NSO Pegasus verwendet, wahrscheinlich neben vielen anderen Produkten. Die Regierung verweigert jede Information darüber, auch gegenüber dem Parlament.

Der erste Staatstrojaner in Deutschland wurde 2011 entdeckt. Experten des Chaos Computer Clubs bekamen die kommerzielle Schadsoftware eines ehemaligen deutschen Unternehmens namens DigiTask. Sie analysierten die Software und deckten eine Reihe von Problemen auf: Es beschränkte sich nicht ausreichend auf laufende Kommunikation, erlaubte die Übernahme des infizierten Geräts durch andere Akteure und hatte verschiedene IT-Sicherheitsprobleme.

Offizielle Untersuchungen bestätigten die CCC-Enthüllungen. DigiTask wurde als illegal eingestuft, und die Strafverfolgungsbehörden kündigten das Produkt. Die Firma wurde inzwischen an den deutschen Elektronikriesen Rohde & Schwarz verkauft – ein Sponsor der „Abhör-Ball“ genannten Messe ISS World.

Nach diesem Desaster entwickelte die deutsche Polizei ihren eigenen Staatstrojaner namens „Remote Communication Interception Software“ oder RCIS. In vier Jahren programmierten 29 Polizeibeamte eine erste Version, RCIS Desktop, die Windows hacken und Skype-Kommunikation abhören kann. Ein Update für eine zweite Version, RCIS Mobile, wurde 2017 fertiggestellt und wird verwendet, um Smartphones und Tablets zu hacken.

Wie ich bereits erwähnt habe, hat die deutsche Polizei auch die Staatstrojaner FinSpy von FinFisher und Pegasus von NSO gekauft. Aber es ist unwahrscheinlich, dass dies die einzigen Werkzeuge sind, die der deutschen Polizei zur Verfügung stehen.

Im Jahr 2017 errichtete der Bundesinnenminister eine neue Agentur mit der Bezeichnung „Zentralstelle für IT im Sicherheitsbereich“ (ZITiS). Diese Agentur ermöglicht sowohl die Forschung und Entwicklung von Staatstrojanern durch den Staat selbst als auch den Kauf von Staatstrojanern von kommerziellen Unternehmen.

Die Regierung gab zu, dass ZITiS folgende Unternehmen getroffen und bewertet hat: das österreichische Unternehmen DSIRF mit seinem Produkt Subzero, das italienische Unternehmen RCS und sein Produkt Hermit sowie die israelischen Unternehmen Quadream und Candiru. Die Regierung weigert sich jedoch, eine umfassende Liste der Unternehmen vorzulegen, die ZITiS getroffen hat, geschweige denn Produkte, die es für den Einsatz bei Polizei und Geheimdiensten gekauft hat.

Geheimhaltung: Regierung verhindert Kontrolle

Damit komme ich zu einem übergreifenden Problem: dem Mangel an Kontrolle. Im Entwurf des Berichts dieses Ausschusses heißt es: „Ein Haupthindernis bei der Aufdeckung und Untersuchung des unrechtmäßigen Einsatzes von Spähsoftware ist die Geheimhaltung.“ Und „‚Nationale Sicherheit‘ wird häufig als Vorwand für die Beseitigung von Transparenz und Rechenschaftspflicht angeführt.“ Diese beiden Sätze treffen definitiv auf Deutschland zu.

Regierung und Polizei verweigern unter dem Vorwand der „nationalen Sicherheit“ jede aussagekräftige Information über Staatstrojaner. Bis zum heutigen Tag weigert sich das BKA, öffentlich zuzugeben, NSO Pegasus gekauft zu haben. Es behauptet, sein Vertrag mit NSO erlaube dies nicht. NSO hat jedoch vor diesem Ausschuss erklärt, dass seine Kunden diese Informationen sehr wohl sagen öffentlich dürfen, sie müssen nur wollen.

Die deutsche Regierung verweigert diese Informationen sogar dem Deutschen Bundestag. Abgeordnete haben immer wieder wichtige Fragen gestellt, aber die Regierung verweigert die Antwort.

Um notwendige Geheimnisse zu schützen, könnte die Regierung einige wichtige Informationen schwärzen oder Dokumente als vertraulich oder geheim oder sogar streng geheim einstufen und nur Abgeordneten mit entsprechender Sicherheitsfreigabe zeigen. Aber selbst das verweigert sie.

Vor zwei Jahren kündigten Abgeordnete zweier Parteien an, die Regierung wegen dieser Informationen zu verklagen. Leider haben sie das nicht getan. Inzwischen sind sie Teil der Regierungskoalition.

Es bleibt also, wie überall, an der Zivilgesellschaft, an Aktivist:innen und Journalist:innen, für Aufklärung zu sorgen.

Als Journalist:innen nutzen wir Instrumente wie Pressegesetze und Informationsfreiheitsgesetze. Dies hat einen gewissen, aber begrenzten Erfolg.

Als wir aufgedeckt haben, dass das BKA 2013 FinFisher gekauft hat, haben wir den Vertrag angefordert. Das BKA verweigerte aussagekräftige Informationen, also verklagten wir sie – und haben gewonnen. Später stellten wir einen weiteren Antrag zur Aktualisierung dieses Vertrags. Wieder verweigerte das BKA aussagekräftige Informationen, also verklagten wir sie erneut – und wieder haben wir gewonnen.

Ja, wir müssen die Polizei verklagen, damit sie sich an das Gesetz hält.

Vor vier Monaten haben wir den Vertrag mit NSO für Pegasus beantragt. Das BKA verweigert erneut jegliche Auskunft. Der Streit dauert an, aber es sieht so aus, als müssten wir die Polizei erneut verklagen.

Aber selbst wenn wir gewinnen, bekommen wir meist nur das, was bereits öffentlich ist oder von geringer Relevanz. Diese Seite ist der Vertrag mit FinFisher, den uns die Polizei nach unserem Sieg vor Gericht gegeben hat. Wie sie sehen, sehen sie nichts.

Nachdem die Polizei ihren eigenen Staatstrojaner RCIS programmiert hatte, prüfte der deutsche Datenschutzbeauftragte das Produkt. Nach vier Anträgen und fünf Jahren des Wartens hat uns der Datenschutzbeauftragte diese Seite gegeben. Sie wird bis zum Jahr 2080 geschwärzt und geheim bleiben. Wahrscheinlich lebt von uns dann niemand mehr.

Viele andere Dokumente werden uns überhaupt nicht zur Verfügung gestellt. Ein paar Beispiele. Erstens: Die Polizei hat eine Studie über „Grundrechtsschonende Alternativen zur Quellen-TKÜ“ in Auftrag gegeben. Das ist superrelevant, aber das Dokument ist eingestuft und wird uns verweigert. Zweitens: Die Polizei hat NSO Pegasus analysiert. Aber dieser Bericht ist geheimer als geheim und wird allen verweigert. Drittens: Die Polizei hat ihre anderen Staatstrojaner extern prüfen lassen. Aber auch dieses Dokument ist geheim und wird uns verweigert.

Dilemma: Sicherheit gegen Sicherheit

Aufschlussreich ist, dass einer der Gründe für die Verweigerung dieses Berichts darin besteht – ich zitiere die Polizei -, dass „die Anbieter kommerzieller Hard- und Software in die Lage versetzt [würden], die von der Überwachungssoftware genutzten

Angriffsvektoren (Schwachstellen etc.) zu schließen und den Einsatz der Software unter Umständen zu verhindern“.

Normalerweise versuchen sowohl kommerzielle Anbieter als auch staatliche Akteure, der Frage nach Zero-Day-Schwachstellen auszuweichen. Hier gibt die Polizei offen zu, dass sie von Zero-Day-Schwachstellen in kommerzieller Hard- und Software weiß, und anstatt die Hersteller zu informieren, damit sie diese Schwachstellen für alle schließen, hält sie sie offen und geheim.

Dies ist das grundlegende Sicherheitsdilemma des staatlichen Hackens. Um ein gewisses Maß an öffentlicher oder nationaler Sicherheit zu erlangen – und sei es nur ein Dutzend Drogendelikte – schafft staatliches Hacken immense Unsicherheit in der IT-Sicherheit. Um die iPhones von ein paar Dutzend mutmaßlichen Kriminellen zu hacken, halten Staaten und Unternehmen alle zwei Milliarden iPhones auf diesem Planeten unsicher und anfällig für Hackerangriffe durch jedermann.

Sicherheitslücken sind eine Gefahr für die nationale Sicherheit. Dieses Argument war lange Zeit theoretisch, aber jetzt haben wir ein Beispiel in der EU: Der spanische Staat hat Katalanen gehackt, und mit genau derselben Schwachstelle hat Marokko den spanischen Premierminister und die Verteidigungsministerin gehackt.

IT-Sicherheit ist binär. Niemand ist sicher, bis alle sicher sind.

Die Technologiebranche weiß das. Die EU-Agentur für Cybersicherheit weiß das. Und die deutsche Regierung weiß das auch. In ihrem Koalitionsvertrag hat sie letztes Jahr beschlossen: „Die Ausnutzung von Schwachstellen von IT-Systemen steht in einem hochproblematischen Spannungsverhältnis zur IT-Sicherheit und den Bürgerrechten. Der Staat wird daher keine Sicherheitslücken ankaufen oder offenhalten, sondern sich [...] immer um die schnellstmögliche Schließung bemühen.“

Dies ist ein dringend notwendiger erster Schritt. Leider hat die Bundesregierung ihr Versprechen noch nicht umgesetzt. Aber dieser Ausschuss sollte nicht hinter der Bundesregierung zurückbleiben. Ihr Abschlussbericht sollte sowohl staatliche als auch private Akteure verpflichten, ausnahmslos alle Sicherheitslücken so schnell wie möglich zu schließen.

Fazit: Staatliches Hacken verbieten

Zusammengefasst: Staatliches Hacken hat grundlegende Probleme. Das ist überall so, auch in Deutschland.

Hätte die deutsche Polizei den Mut gehabt, heute hierher zu kommen, hätte sie behauptet, staatliches Hacken sei: notwendig, verhältnismäßig, gut kontrolliert und werde nur gegen Terror und schwerste Verbrechen eingesetzt. Alle diese Behauptungen sind falsch, und ich kann gerne weitere Fakten vorlegen, die das belegen.

Stattdessen stimme ich dem Europäischen Datenschutzbeauftragten zu, der sagt, staatliches Hacken birgt „beispiellose Risiken … nicht nur für die Grundrechte und -freiheiten des Einzelnen, sondern auch für die Demokratie und die Rechtsstaatlichkeit".

Darüber hinaus ist staatliches Hacken auch eine Gefahr für die IT-Sicherheit, eine Gefahr für kritische Infrastrukturen, eine Gefahr für die öffentliche Sicherheit, eine Gefahr für die nationale Sicherheit und – wie das Hacken von EU-Institutionen gezeigt hat – eine Gefahr für die europäische Sicherheit.

Handeln Sie und bekämpfen Sie diese Gefahr.

Mit diesen Worten schließe ich mein Eingangsstatement.

Ich bin gerne bereit, weitere Themen wie deutsche Unternehmen oder mögliche Handlungsfelder in den Fragen und Antworten zu diskutieren.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf Ihre Fragen.

Transcript (inoffiziell)

- **Datum:** 2022-11-14
- **Ort:** Brüssel
- **Institution:** Europäisches Parlament
- **Ausschuss:** PEGA
- **Vorsitz:** Jeroen Lenaers
- **Experte:** Andre Meister, investigativer Journalist netzpolitik.org

Jeroen Lenaers (Chair): Afternoon, colleagues. If everybody would like to take their seats. Then we can start with today's hearing.

First of all, a warm welcome to all the colleagues here today. We have interpretation in the following languages: German, English, French, Italian, Greek, Spanish, Hungarian, Polish, Slovakian, Slovenian, Bulgarian and Romanian.

Two other short announcements. We are still trying to find a suitable date for a coordinators meeting this week where all coordinators can be present. I will inform you if we manage to find such a slot, but it would be important.

Secondly, as already announced during our visit to Greece, the Greek government has informed me today that they will send their draft proposal for legislation on legal surveillance later today. So we can hopefully also already share that with you later this evening.

Then the programme for today is a country hearing on Germany.

Before we get started, I would like to make one comment. We have invited Ms. Martina Link, which was also a request from all the groups, who is the Vice President of the German Federal Police. We invited her three times and each time she was unavailable.

We also invited the Munich prosecutor that investigates the FinFisher case. However, the prosecutor immediately took contact with our secretariat and explained that as they have not shared the content of the investigation with the suspects and therefore they were prevented by law to share it with anyone else before that as well. Now, of course, in that sense, we respect it because any criminal investigation must have its proper run.

But I have to say that the response from the prosecutor was a short, sharp contrast to that of Ms. Link. I'm not sure whether she cannot make it or she is not allowed by her boss. But it's not a very good sense of cooperation we received from the German authorities.

In this sense, however, it means that we have a lot of time. I know that Mr. Meister also has a lot of information to share with us. So I'm very grateful that you are here to share it with us. You have a lot of experience investigating FinFisher, but also the wider context of these kind of technology in Germany. So I would give you the floor for normally ten minutes, but if you want to take longer, be our guest because we have the time and then we start a round of questions and answers with the colleagues. But thank you very much for being here. And you have the floor.

Andre Meister: Thank you. Dear members of the PEGA Committee:

Thank you for inviting me to speak about state hacking and so-called spyware in Germany.

I am an investigative journalist working for the digital rights media outlet netzpolitik.org in Berlin. We have been investigating and reporting on state hacking for over a decade. In my free time, I am also a member of Chaos Computer Club and an observer at European Digital Rights, but today I do not speak on their behalf.

I am surprised that I am the only expert in todays hearing. I understand my colleges from civil society just didn't have enough resources. And the Munich Public Prosecutor was interested, but is legally restricted to talk publicly about ongoing investigations.

But that the German government and police turned down the invitation of this committee is disgraceful. With their refusal to show up and testify today, Germany joins the long list of countries unwilling to cooperate with your important inquiry. I will show that this behaviour is symptomatic and Germany shares many of the problems in the other countries you are investigating.

Because today's topic is broad and I am the only expert that showed up, the chair graciously gave me permission to speak for 20 minutes. Thank you.

In my intervention, I will focus on the use of state hacking tools in Germany, as that is where this committees draft report from last week is still short and shallow. I am also happy to provide information on German companies like FinFisher and others. But with regards to the time, I will keep that for the Q&A.

I will first outline the history of state hacking in Germany and the cases it's used for. Then, I will explain the legal framework and a special new fundamental right in Germany. Third, I will name the products that Germany has bought and developed. I will then illustrate the secrecy and lack of accountability of state hacking in Germany. Finally, I will present a laudable initiative of the German government to regulate an important aspect of this problem.

First, a remark on terminology. In German public discourse, we don't use the term „spyware". This word is imprecise and overspecific.

Instead, we speak of „state malware" or „state hacking". This captures more accurately what these tools are about: intruding into IT-systems, in secret, without the knowledge of the owner, by hacking them, breaking their integrity and confidentiality, and taking control over them.

Of course, the primary goal is surveillance, but state hacking is also used to sabotage and disrupt IT-systems, or to plant incriminating evidence on them, as we have seen

police in India do. The difference, if any, is only a few of lines of code.

Also, it's not just about smartphones, they just have the most publicity. Any digital device imaginable can and will be hacked. This ranges from laptops and watches to televisions and home automation to servers and routers, and of course the Internet of Things. It even includes cars and aeroplanes, which are now computers we put our bodies in, and medical implants, which are computers we put into our bodies.

To reflect all this, I use the term „state hacking".

German state entities have been hacking for at least 20 years.

In 2005, the foreign intelligence agency BND hacked the government of Afghanistan, where they exfiltrated emails between an Afghan minister and a German journalist. This is illegal. In 2006, they hacked a hotel in the Democratic Republic of Congo, where a German spy read the emails of a German soldier flirting with another German spy. This is also illegal.

The foreign intelligence agency doesn't hack to solve crimes, and it's not their job to fight terrorism – that's the job of police. Spies mostly hack for classic espionage. Foreign intelligence likely top the list of state hacks. In 2009, they had already hacked over 2.500 devices.

Another important state hacker is the military. In 2015, the German military hacked a mobile network operator in Afghanistan. This proves that state hacking is not limited to individual targets. They also hack entire communication networks and critical infrastructure.

Unfortunately, there is extremely limited information about the hacking operations of intelligence agencies and military, even though that is the bulk of state hacking. The few cases we do know about only became public thanks to investigative journalism, because the hacking involved illegal activity which led to oversight actions.

Customs and police in Germany have been hacking since at least 2008. The first three targets that became public were suspects selling anabolic steroids, fake Viagra, and contraband cigarettes. The latter case was unsuccessful, because the hacking software unintentionally damaged the target computers hard drive.

As you can see, this is NOT the terror or most serious crime that advocates use to justify state hacking. Nor does it work flawlessly.

But these cases are typical to this day. In 2013, the police was tasked to justify their demands for state hacking. They came up with a list of almost 300 investigations into serious crime where the police claimed they needed to hack suspects. This sample is not scientifically reliable and the data does not show that state hacking was necessary or proportionate, as police didn't say whether they were able to solve the cases without state hacking or if the suspects were innocent.

But the survey did reveal what the police really wanted to use state hacking tools for. Over half of the cases were drug crimes. Almost a quarter were property crimes, fraud, robbery, and extortion. In Parliament, hacking laws were justified with: „forming criminal organizations, crimes against sexual self-determination, child pornographic content, and murder". But the police's own data showed zero cases of forming criminal organizations, zero cases of crimes against sexual self-determination, zero cases of child pornographic content and zero cases of murder.

These numbers are similar to classic taps of telephone or internet connections. And each year, official statistics confirm that they are also true in practice.

In 2019, German police were granted to hack 64 times and actually did 15 times. More than a third of cases were extortion, another third were drugs. There were zero cases of terror and zero cases of murder.

In 2020, the must current numbers we have, German police were granted to hack 48 times and actually did 22 times. Again, more than a third of cases were drugs, another third were extortion. Again, there were zero cases of murder.

This shows that state hacking is always publicly justified with terror and murder, but it is almost never actually used for terror and murder.

Allow me a personal story. In 2015, the president of the German domestic intelligence agency personally filed a criminal complaint against me and my colleagues, accusing us of nothing less than treason for doing our job: reporting truthful information in the public interest on the internet surveillance capabilities of his agency. These criminal investigations were later dropped, but the extreme allegations allowed police the entire arsenal of surveillance capabilities against us. Only two years later, this would include state hacking.

So the issue at hand is more than theoretical for me. Therefore I want to take this opportunity and express my solidarity with all the journalists and human rights

defenders around the world that have been targeted by state hacking to intimidate, repress, and silence them. Keep fighting.

The cases we know about are all in the past, but we must think about the future. In Germany, domestic intelligence agencies spy on anti-fascist human rights defenders and climate activists. In this very moment, twelve climate activists are prison in Germany, without being sentenced or even charged for a crime. The Police put them in so-called „preventive custody", for an entire month, to keep them from protesting on the streets.

In this political climate, it doesn't take much fantasy to imagine that journalists, human rights defenders and activists will be targeted by state hacking in Germany sooner or later.

It is your job to act and stop this from happening.

Let's look at the legal framework in Germany. The first Federal German law explicitly granting state hacking powers to police was passed in 2008. It limited state hacking to the Federal Police, to international terrorism, and to the prevention of terrorist attacks.

Since then, state and federal laws have continuously expanded the scope and use of state hacking. A 2017 law allows state hacking for every law enforcement agency and for a long list of 42 criminal offences – including tax evasion, submitting fraudulent asylum applications and, of course, drug offences.

Last year, a new law officially legalized state hacking for all 19 German intelligence agencies, although at least the Federal agencies had been doing this already without a specific law.

This law also obliges communication providers to assist the state in hacking by installing government hardware in their networks to allow machine-in-the-middle attacks against their customers. The communication providers vehemently criticized this, citing risks for the integrity of their infrastructure, a loss of trust, and an attack on IT security.

The German hacking laws are regularly taken to court. In response, the Federal Constitutional Court created a new constitutional right in 2008: the „fundamental right to protection of the confidentiality and integrity of IT-systems".

The Highest German Court says that state hacking can only be legal, „if there are factual indications of a specific danger to an exceptionally significant legal interest.

Exceptionally significant legal interests are life, limb and liberty of the person or public interests that are of such significance that a threat to them would affect the foundations or existence of the state, or the foundations of human existence."

That's the terrorism and serious crime we often hear about. However, that is not what is happening in reality.

To get around this landmark ruling and this new fundamental right, German police came up with a legal trick. They invented two different kinds of hacking. In one, they hack a device and have access to any and all data on that device. They call this „covert remote search of IT systems".

In the other, they hack a device and even though they technically have access to any and all data on that device, they restrict themselves to intercept and record live communication only. They call this „telecommunications surveillance at the source". It was even amended to the same section of the criminal law specifying classic „telecommunications surveillance".

This intentional re-framing of active state hacking being little more than a passive phone tap makes a mockery of the new fundamental right proclaimed by the Constitutional Court. It remains to be seen if it holds up in court, as various constitutional complaints are still pending.

The re-framing has also resulted in practical mistakes and errors. Public prosecutors have repeatedly mixed-up classic phone surveillance and active state hacking in their investigations. And they are criminal justice experts.

From a technical perspective, the distinction between two types of hacking, based on what kind of data you exfiltrate after the hacking, is artificial and arbitrary. Once you hack a device, you have access to the entire device, including all its data and sensors. To limit yourself to communication in certain Apps only requires new, additional source code and functionality.

This is why Germany has special requirements when purchasing commercial hacking tools. In 2013, the police bought FinSpy from FinFisher. But, by default, it was only able to exfiltrate all data on the target device. So the police made FinFisher develop additional source code to limit the power of its product. It took FinFisher five years and three versions, until the tool was in line with the legal requirements.

This is also the reason why German Police did not immediately buy Pegasus. Police and NSO met for the first time in 2017. But again, it took years of negotiations and additional work by NSO to develop a modified version. German Police only bought Pegasus in late 2020.

That brings me to the products used in Germany. Unfortunately, we have virtually no information about the military and intelligence agencies. Only that the foreign intelligence agency uses NSO Pegasus among probably many others. The government denies any and all information about this, even to Parliament.

The first state hacking tool was discovered in Germany in 2011. Chaos Computer Club experts obtained the commercial malware of a former German company called DigiTask. They analysed the tool and uncovered a list of problems: it did not sufficiently limit itself to communication only, it allowed the takeover of the infected device by anyone else, and it had various other IT security issues.

Official investigations verified the CCC revelations. DigiTask was found to be illegal, and law enforcement abandoned the product. The company has since repeatedly been sold, most recently to German electronics giant Rohde & Schwarz, which is also a sponsor of the Wiretappers Ball ISS World.

After this disaster, German police developed their own hacking tool called „Remote Communication Interception Software“ or RCIS. In four years, 29 police officers programmed a first version, RCIS Desktop, to hack Windows and exfiltrate Skype communication. An update to a second version, RCIS Mobile, was finished in 2017. It is used to hack smartphones and tablets.

As I mentioned previously, German Police have also bought the mercenary hacking tools FinSpy from FinFisher and Pegasus from NSO. But these are not the only tools that German police have at their disposal.

In 2017, the Federal Minister of Interior created a new Agency called „Central Office for IT in the Security Sector“ or ZITIS. This agency facilitates both research and development of hacking tools by the state itself, and the purchase of hacking tools from commercial companies.

The government admitted that ZITIS met and evaluated: the Austrian company DSIRF and its product Subzero, the Italian company RCS Labs and its product Hermit, and the Israeli companies Quadream and Candiru. However, the government refuses to provide

a comprehensive list of companies ZITIS met, let alone products it bought for police and intelligence to use.

This brings me to an overarching problem: the lack of accountability. The draft report of this committee says „A major obstacle in detecting and investigating the illegitimate use of spyware is secrecy." And „'National security' is frequently invoked as a pretext for eliminating transparency and accountability." These two sentences are definitely true for Germany.

Government and police refuse to provide any meaningful information about state hacking tools, with the excuse of „national security". To this day, the police refuses to publicly acknowledge that they have bought NSO Pegasus. They claim their contract with NSO doesn't allow this. But NSO told this very committee that their customers are free to reveal that information, if they want to.

The German government even denies this information to Federal Parliament Bundestag. Members of Parliament have time and again asked important questions. But the government refuses to answer.

To protect necessary secrets, the government could redact some vital information or classify documents as confidential or secret or even top secret, and show them only to MPs with proper security clearance. But they deny even this.

Two years ago, MPs from two parties said that this blanket refusal is illegal and announced that they would sue the government for this information. Unfortunately, they didn't. Now they are part of the government.

So, like everywhere else, it's up to civil society, activists and journalists to provide some insight.

As journalists, we use tools like press laws and Freedom of Information laws. This has some, but limited success.

When we revealed that the police bought FinFisher in 2013, we requested the contract. The police denied meaningful information, so we sued them – and won. Later, we filed another request for updates to this contract. The police again denied meaningful information. So again, we sued them – and again, we won.

Yes, we have to sue the police to make them abide by the law.

Four months ago, we filed another request for their contract with NSO for Pegasus. The police again denies to provide any information. The dispute is ongoing, but it looks like we will have to sue the police again.

But even when we win, mostly we get what's already public or of little relevance. This the contract with FinFisher the police gave us after we won in court. As you can see, you can't see anything.

When the police programmed their own hacking tool RCIS, the German Data Protection Commissioner reviewed the product. After four requests and five years of waiting, this what they gave us. It will remain redacted and classified like this until the year 2080. I don't know if any of us will still be alive then.

Many other documents they don't give us at all. A few examples. One: The Police has commissioned a study „alternatives to state hacking respecting fundamental rights". This is super relevant. But the document is classified and locked away. Two: The Police has analysed NSO Pegasus. But this report is beyond classified and locked away. Three: The Police commissioned an external report on its other hacking tools. But this document is also classified and locked away.

Revealingly, part of the reason to deny this report is – and I quote the police – „the providers of commercial hardware and software attack vectors used by the surveillance software (like vulnerabilities) and prevent the use of the spyware".

Usually, both commercial vendors and state actors dodge the question of zero-day-vulnerabilities. Here, police openly admit that they know about zero-day-vulnerabilities in commercial hard- and software and instead of informing the vendors to close these vulnerabilities for everyone, they keep them open and secret.

This is the fundamental security dilemma of state hacking. In order to gain some level of public security – even if that is just a dozen drug crimes – state hacking creates immense insecurity in our digital environment. To hack the iPhones of a few dozen alleged criminals, states and companies keep all two billion iPhones on this planet insecure and vulnerable to hacking by anyone.

Security vulnerabilities are a danger to national security. This argument was theoretical for a long time, but now we have an example in the EU: The Spanish state hacked Catalans, and with the exact same vulnerability Morocco hacked the Spanish prime minister and defence minister.

IT security is binary. No-one is safe until everyone is safe.

The tech industry understands this. ENISA understands this. And the German government understands this. In their coalition agreement last year they wrote: „Exploiting vulnerabilities in IT systems is highly problematic in terms of IT security and civil rights. The state will therefore not buy or keep open any vulnerabilities, but will always strive to close them as quickly as possible."

This is a much needed first step. Unfortunately, the German government still didn't implement their promise. But this committee should not fall behind the German government. Your final report should mandate both state and private actors to fix all vulnerabilities as quickly as possible, without exception.

To sum up: State hacking has fundamental problems. This is true everywhere, also in Germany.

If the German Police had the courage to come here today, they would have claimed that state hacking is: necessary, proportionate, accountable, and used only against terror and the most serious crimes. All of these claims are false, and I can gladly provide more facts to support that.

Instead, I agree with the EDPS, who said that state hacking „poses unprecedented risks … not only to the fundamental rights and freedoms of the individual, but also to democracy and the rule of law."

Beyond that, state hacking is also a danger to IT security, a danger to critical infrastructure, a danger to public security, a danger to national security, and – as the hacking of EU institutions has shown – a danger to European security. Let's fight this danger.

With this, I want to conclude my intervention.

I am happy to discuss further issues like German companies or possible areas of action in the Q&A.

Thank you for your attention. I look forward to your questions.

Jeroen Lenaers (Chair): Thank you very much, Mr. Meister. And thank you also for giving such an elaborate introduction. And we have the time. So I'm happy you you took it to inform us about all of this. And I'm sure there will be many questions that will also give

you the opportunity to to dive in a little bit deeper in the other subjects that you mentioned.

We start the round with our rapporteur, Sophia in ,t Veld.

Sophia in ,t Veld: Yes, thank you, Chair. And thank you, Mr. Meister, for your very detailed intervention.

As with many speakers, I think many of us would be interested to get your speaking notes through, to have some time to go through it again, and check out in particular all the figures and statistics and years that you mentioned, because it's it was very rich in information.

I think I, personally at least, agree very much with your many of your conclusions on the use of state hacking, state malware, etc. And I think the problem is indeed that citizens get less and less information about what states are doing with their power. And then if you try and ask questions, they say „Oh, but you're asking the wrong questions or you're making the wrong assumptions", but you can only make assumptions if you don't have all the facts on the table. So I entirely agree with you.

A few questions in random order. So you mentioned two kinds of state hacking, and one basically allows what what to do, what we call spyware here, basically extracting everything from from your phone, monitoring your communications, but also accessing your documents, etc., etc. And the other one is more like conventional wiretapping, real time listening into conversations. If I understood correctly what you say, but due to two kinds of state hacking, do they require the same kind of judicial authorisation? Because they're very different types of of spying or hacking, if you want, then, uh. All in order.

Another source of information. If the authorities are stonewalling, you are stonewalling. The Parliament as well are stonewalling this parliament as well.

Then another source would of course, be people who who have the feeling that they have been targeted with spyware. Can you say something about people who've come forward in Germany? Maybe journalists, maybe activists or politicians even who have been targeted?

Then can you say something, because you've mentioned a lot of different brands. One is DSIRF, which is produced in in Austria, and you have published about that fairly extensively. But can you say something about where the German authorities are now in

using that or not using that to say something about the connexions between German personalities and the company ideas?

And if and finally, maybe something about RCIS, if I understood correctly, the police's own hacking tool, because we have been focussing, of course, very much on commercial spyware tools, but there are plenty of authorities all around the world who are developing their own stuff. And do you have more information about the capabilities of that tool, how it's being used? Can it be detected? Are any of the targets already known?

Yeah, those would be my questions for now.

Jeroen Lenaers (Chair): Thank you, Sophie in ,t Veld. Mr. Meister.

Andre Meister: I can gladly provide my speaking notes. And if you want, feel free at any time to drop me a mail. I can also provide sources to every single sentence I have said.

With regards to the two types of hacking in Germany: This is only a legal distinction. Technically, there is not that much of a difference. And there's an academic paper doubting it's possible to develop a restricted hacking tool at all.

In German law the telecommunications surveillance at the source and the remote forensic full search, they have slightly different legal authorisations. I can gladly provide them to you, even in English. I think they are linked already in the draft report of this committee.

But both have a long list of crimes that they are used against. The telecommunications at the source, the classic phone surveillance by hacking, is used for everything that classic phone surveillance is used, for a long list of 42 crimes. The remote forensic search is used for slightly less crimes. Both require, as far as I know, I'm not a lawyer, prior approval. It's used by police in investigations, but they are probably also used by secret services, where the authorisation is, of course, different.

You asked about victims in Germany. Unfortunately, we publicly know very few victims that have come forward. The first victim that came forward in 2011 and allowed Chaos Computer Club to investigate the German tool called DigiTask was some bodybuilder. He was accused of exporting anabolic steroids, which are legal in Germany but not legal in neighbouring countries. His lawyer found in the court documents the police had printed hundreds of pages of screenshots of his, back then, computer and only because the lawyer was smart enough to understand where the only place they could have obtained it is the computer itself. He went to the CCC to analyse this. So it's hard for

people to to know, even in criminal investigations and court proceedings, that these tools are being used. Police don't advertise that, even after criminal investigations and proceedings.

We have been trying to find more victims in Germany. We don't know. We do know it is being actively used. But so far, we don't publicly know of victims. We now know that there are people involved in the so-called Catalan Gates scandal, Catalan activists and politicians and lawyers being targeted by Candiru and Pegasus, while in Germany. This also touches Germany. I think one of them is also a German citizen. But as far as we know, they were not targeted by German entities.

This only shows the transnational aspect of these tools. Anyone from anywhere in the world can use these kinds of tools to hack any device. Borders, national borders, even EU borders, don't matter.

I'm still reaching out to them. There are some legal problems because of ongoing investigations, where I they have a hard time speaking publicly. But of course, we'd be happy to hear the stories of any victims. If you're hearing this, please come forward to me.

The Austrian company DSIRF. We do not know whether it's used in Germany. Police and government just flat out deny any information about this. The only thing we know is that the government agency called ZITiS had talks with them. We don't know whether they bought it. We don't know which agencies they gave it to. We don't know if they've used it. How many times against whom? We don't know. Government knows this, but it is not telling us.

In my reporting on DSIRF. Unfortunately, it had lots of Russians connections, but it was in December 2021 – when those didn't really interest a lot of people. The Russian connections are, I think, the most intriguing and most important.

But yes, there is also a strong link to Germany with the person of Jan Marsalek, the COO of Wirecard Company. Actually, I found the document advertising this product in his mailbox. He was giving it to someone else, advertising to use this product possibly for commercial espionage, not for government espionage. But we don't know.

RCIS, the German police's own product. Again, we only know very few things I have said in my introductory statement. We do not know the exact capabilities. I believe I said that since 2017 it is used to hack smartphones. That is five years ago. That's an eternity in the IT development world. We just do not have any updates. Any time a Member of

Parliament or anyone else asks, they are refused this information. We would like to know, but we just do not know.

Also, we do not know how to detect it because if you don't have a sample, you can also not create tools to find this. We also do not know who was targeted by RCIS or any other specific tool. The only information we have, is that German police hacked such and such many times. I have said the numbers. But they do not say with which tool, whether it's their own tool or one of the many commercial tools that they are able to purchase or have purchased.

German police knows this. They could have shown up here today and told you. But they chose not to. I don't know it.

Jeroen Lenaers (Chair): Thank you. Karolin Braunsberger-Reinhold.

Karolin Braunsberger-Reinhold: Vielen Dank. Ich werde Deutsch sprechen. Ich vermute das ist kein Problem.

Erst mal vielen Dank, dass Sie heute hier sind. Sie haben eine sehr intensive Arbeit, um es mal so zu beschreiben. Ich weiß, dass das absolut nicht einfach ist. Ich finde es auch sehr, sehr schade, dass Sie der Einzige sind, der heute hier ist. Ich finde es nicht schade, dass Sie hier sind, sondern dass die anderen nicht da sind, um das mal klarzustellen. Trotzdem habe ich da ein paar Nachfragen. Sie mögen es mir verzeihen.

Zum Beispiel: Sie haben darauf hingewiesen, dass der Einsatzbereich schwerpunktmäßig im Drogen-Bereich auch stattfindet. Wenn ich Sie richtig verstanden habe, wir haben in Deutschland eine Klassifizierung der Verbrechen und gerade der Drogen-Bereich ist ein Schwerpunkt im Geldwäsche-Bereich. Im Geldwäsche-Bereich, der die Grundlage für die organisierte Kriminalität zum Beispiel auch ist. Das heißt da wirklich die Frage und nehmen Sie es mir nicht übel, ist nicht in dem Fall ein früheres Einschreiten besser als ein späteres Einschreiten? Da habe ich aber dann die Herausforderungen: Schreite ich erst ein, wenn ich wirklich in die Ecke gehe, damit ich es als OK klassifizieren kann? Oder schreite ich vorher schon ein? Dann wird es aber bei uns in Deutschland als Geldwäsche klassifiziert.

Frage: OK?

Karolin Braunsberger-Reinhold: Entschuldigung. Organisierte Kriminalität. OK ist die organisierte Kriminalität. Entschuldigung. Danke für den Hinweis.

Dann der Bereich Klima-Proteste. Ich weiß, dass das in Deutschland bei uns sehr hohe Wellen geschlagen hat. Es gibt mehrere Klima-Protestler, männlich-weiblich-sächlich, die jetzt 30 Tage erst mal in Haft genommen wurden. Vorbeugend. Aber hier möchte ich darauf hinweisen: Es gab vorher Anhörungen dazu und es gab Androhungen weiterer Straftaten und da ist es deutsches Recht. Dafür gibt es Rechtsgrundlagen, dass diese Personen bei Androhung weiterer Straftaten nun mal in Gewahrsam genommen werden, damit diese Straftaten nicht durchgeführt werden können. Kann man halten von was man will. Aber grundsätzlich ist in dem Punkt alles rechtlich sauber abgelaufen.

Moment, jetzt muss ich hier noch mal gucken. Und Sie wiesen darauf hin, das fand ich grundsätzlich sehr interessant, dass in Deutschland kaum Opfer bekannt sind. Da würde mich tatsächlich mehr interessieren, woran das liegt. Wir haben aus anderen Ländern Opfer, die bekannt sind. Wir haben Leute, die wirklich an die Öffentlichkeit gehen, die mit uns reden, die auch hier sind. Wo ist die Herausforderung, speziell bei uns in Deutschland, dass sich Leute bekannt machen, dass es bekannt wird? Woran liegt das Ganze? Vielleicht können Sie da noch weitere Fragen oder uns weitere Informationen geben.

Und grundsätzlich würde ich mich sehr darüber freuen, was Sie auch angeboten hatten, uns weitere Fakten und Informationen zur Verfügung zu stellen, gerne durch Links, Anhänge oder was auch immer Sie da haben, damit wir weiterarbeiten können. Danke schön.

Jeroen Lenaers (Chair): Thank you. Mr. Meister.

Andre Meister: Sie haben recht. In Paragraf 100a Strafprozessordnung stehen Drogendelikte als schwere Straftaten. Aber das sind nicht die schwersten Straftaten, mit denen diese Tools im Parlament begründet wurden, als die Gesetze verabschiedet wurden. Ich habe viele Beispiele genannt, die diverse Abgeordnete im Bundestag gesagt haben, was sie damit verfolgen werden, nämlich internationaler Terrorismus, Verhütung von internationalem Terrorismus, Mord, Totschlag, Straftaten gegen die sexuelle Selbstbestimmung und sogenannte Kinderpornografie.

Wenn Sie es für Drogen einsetzen wollen, sagen Sie das doch im Parlament. Das haben die Abgeordneten im Parlament nicht getan. Und jetzt wird es dafür eingesetzt, weil es so im Gesetz steht. Sie haben recht, es steht im Gesetz. Es ist legal. Aber in meinen Augen passt das nicht ganz zusammen.

Ja, wir sollten jetzt wahrscheinlich nicht in die Untiefen der deutschen Klimaschutz-Proteste-Debatte einsteigen. Straßen blockieren kann eine Straftat sein. Ich erwarte

aber trotzdem, dass früher oder später auch Klima-Proteste, mögen sie strafbar sein oder nicht, mögen sie ziviler Ungehorsam sein, die Grenze ist fließend, mit mindestens Telefonüberwachungen oder auch Tools wie diesen oder der Überwachung durch den Verfassungsschutz zu tun haben. Wenn Sie das politisch wollen, dann sagen Sie das öffentlich, rechtfertigen Sie sich dafür. Es wird aber immer nur gesagt: Terror und Mord, nicht Drogen und Proteste.

Warum keine Opfer bekannt sind, kann ich Ihnen leider nicht sagen. Ich würde mich sehr freuen, wenn Opfer an die Öffentlichkeit gehen und an Journalisten wie mich, an den Chaos Computer Club, um technische Analysen zu machen. An viele andere Sachverständige von NGOs, von juristischen Vereinigungen oder auch Abgeordneten. Das ist mir egal. Sie können das. Warum diese Opfer diese Möglichkeiten nicht nutzen, kann ich Ihnen leider nicht beantworten. Ich würde mich freuen, wenn es so wäre.

Jeroen Lenaers (Chair): For S&D, it's Katarina Barley.

Katarina Barley: Vielen Dank, vor allem für das Lob des Koalitionsvertrages. Ich hatte die Ehre in der Verhandlungsgruppe dabei zu sein und diese diese Formulierung mit zu beschließen. Ich freue mich auch darauf, wenn die umgesetzt wird.

Ich wollte noch mal fragen, vielleicht etwas komprimierter. Die Zeit, der Zeitraum, innerhalb dessen Sie wissen, dass solche Spyware entweder angekauft oder entwickelt worden ist, ob Sie den einmal eingrenzen könnten?

Dann habe ich eine Frage, weil Sie sagten, dass die Regierung keine Auskünfte gibt. Nach meiner Kenntnis hat es eine Anhörung gegeben im Innenausschuss des Deutschen Bundestages am 7. September 2021, die natürlich nicht öffentlich war, logischerweise, aber die stattgefunden hat in dem Gremium, das dafür zuständig war, meine Kenntnis.

Dann die Frage des Rechtsschutzes. Sie haben mehrfach gesagt, dass geklagt wird, dass auch Sie geklagt haben. Haben Sie den Eindruck, dass das funktioniert? Das ist jetzt keine keine rechtlich irgendwie bindende Aussage. Haben Sie den Eindruck, dass Sie das, dass das System, wenn man sich in seinen Rechten verletzt wird, fühlt, dann klagt man auf der Basis der geltenden Gesetze, dass das in Deutschland funktioniert?

Der Hintergrund meiner Frage, Sie werden es sich wahrscheinlich schon denken können, ist, dass wir hier Fälle aus anderen Ländern hören, wo sich ihnen die Nackenhaare aufstellen. In allen möglichen Zusammenhängen. Und ich weiß nicht, inwieweit sie sich mit den Fällen in Griechenland zum Beispiel oder so auseinandergesetzt haben. Und ich glaube, da ist es schon sinnvoll, vielleicht eine gewisse Relation herzustellen, meiner

Meinung nach. Ich bin jetzt auch nicht ganz objektiv, gebe ich zu, aber der Rechtsschutz in Deutschland funktioniert schon sehr gut.

Dass die Opfer so wenig bekannt sind, das wundert mich auch. Ich fand es sehr bemerkenswert, dass sie sagten: Zwei Mal hat Deutschland Spyware oder Malware gekauft, das aber quasi runter programmieren lassen. Und dafür sieben Jahre gewartet. Gibt es so was auch von einem anderen Land, dass das bekannt ist, dass die quasi von den ganzen Möglichkeiten offensichtlich nicht Gebrauch machen wollten?

Und dann kann man doch sagen. Wenn man Sorge hat, kann man doch sein Handy oder bei uns hier zum Beispiel auch im Europäischen Parlament untersuchen lassen. Deswegen verstehe ich auch nicht. Leute, die die Sorge haben, dass sie vielleicht ausspioniert worden sind, können das doch tun, machen das doch auch, oder? Also ich kann mir das auch wirklich sehr, sehr schwer erklären.

Und ich teile viele Sorgen, die sie artikuliert haben, auch aus meiner früheren Tätigkeit. Aber ich muss doch wirklich noch mal klarstellen, weil manchmal in der Übersetzung auch was verloren geht. Bei diesen Protesten gibt es bisher keinerlei Anzeichen dafür, dass da, dass da irgendeine Software eingesetzt worden ist und dass die das vermuten. Dass das irgendwann der Fall sein könnte, ist eine reine Spekulation.

Das wäre mir noch mal sehr wichtig, weil ich, wie gesagt, ich war Mitglied der deutschen Bundesregierung im Justizbereich. Und wenn ich mitkriegen würde, dass wegen solcher Fragen Schadsoftware eingesetzt werden würde, dann würde ich im Kabinett ziemlichen Ärger anfangen. Um es mal so zu formulieren. Also das möchte ich hier nur noch mal, einmal ganz, ganz klar machen, dass das wirklich eine reine Spekulation ist.

Jeroen Lenaers (Chair): That was it Katarina? Yeah. Okay. So you didn't shut the microphone. I wasn't sure whether there were more questions.

Andre Meister: Vielen Dank auch für die Passage im Koalitionsvertrag. Ich habe mich sehr gefreut. Ich bin gespannt, wann die umgesetzt wird. Die letzten Signale aus dem Bundesinnenministerium waren leider nicht so, als ob das demnächst passiert. Ganz im Gegenteil.

Zum Zeitraum der Einsätze in Deutschland, die Ankäufe. Wir wissen von DigiTask, dass das mindestens seit 2008 eingesetzt wurde, bis 2011. Ob es ein paar Jahre eher gekauft wurde, wissen wir nicht. Ich dachte, sie hatten auch nach den Einsätzen und auch nach RCIS gefragt. Ich hatte die Zahlen genannt, seit wann FinFisher seit wann FinFisher gekauft wurde, nämlich 2013. Aber eingesetzt wird es glaube ich erst seit, ich müsste

nachgucken, 2019 oder 2020. Und auch NSO Pegasus wurde seit 2017 verhandelt, wurde erst 2020 gekauft und wird seit Anfang 2021 in Deutschland eingesetzt. Alle anderen kommerziellen Produkte wissen wir einfach nicht. Wir müssen davon ausgehen, dass es mehr gibt.

Ja, nach dem massiven Druck durch die Pegasus-Projekt-Enthüllungen ist das Bundeskriminalamt in den Innenausschuss gekommen und hat zähneknirschend Fragen beantwortet, weil es einfach nicht mehr anders ging. Aber die Sitzung war eingestuft. Und bis heute weigert sich das Bundeskriminalamt öffentlich zuzugeben, dass sie NSO Pegasus gekauft haben.

Außerdem: Ich kann Ihnen eine Reihe an zwölf parlamentarischen Anfragen geben, wo die Bundesregierung sagt „Danke für die Frage, aber nein, wir werden Ihnen nicht antworten." Nicht mal eingestuft, nicht mal geheim, nicht mal streng geheim in der Geheimschutzstelle. Der Bundestag darf von diesen Fakten nicht erfahren. Ich halte das nicht für angemessen.

Sie haben recht, dass wir in Deutschland keine so krassen Fälle haben wie in anderen europäischen und weltweiten Staaten. Das wäre ja noch schlimmer. Das heißt aber nicht, dass der Rechtsstaat perfekt ist. Wir haben zum Beispiel gesehen, es gibt jährlich eine Statistik vom Bundesamt für Justiz über die eingesetzten Maßnahmen von Telekommunikationsüberwachung, die seit zwei Jahren auch die sogenannte Quellen-Telekommunikationsüberwachung, den kleinen Trojaner und die Online-Durchsuchungen, den großen Trojaner, umfassen.

Staatsanwälte und Ermittlungsbehörden haben wiederholt falsche Zahlen geliefert, weil sie verwechselt haben den Unterschied zwischen einer normalen Telekommunikationsüberwachung und einer Quellen-Telekommunikationsüberwachung, zwischen dem Anzapfen einer Telefonleitung und dem Hacken eines Geräts. Sie haben den Fehler 2019 gemacht, und das war sehr peinlich. Und 2020 machen Sie denselben Fehler wieder. Das heißt doch, dass Sie diese Tools auch in der Praxis verwechseln, weil eben das Hacken nur ein Unterpunkt in dem Paragraf zur Telekommunikationsüberwachung ist. Ich glaube nicht, dass das rechtsstaatlich sauber ist.

Die Quellen-TKÜ, der sogenannte kleine Trojaner, scheint mir eine sehr deutsche Erfindung zu sein. Ich kenne kein anderes Land, das eine ähnliche rechtliche Regelung oder ähnliche Anforderungen beim Ankauf solcher Tools hat. Es ist aber auch nur in Deutschland notwendig, weil in Deutschland das Bundesverfassungsgericht gesagt hat:

Das Hacken von Geräten geht nur unter extrem begrenzten Umstanden, nämlich nur für den Bestand des Staates. Also genau der Terror und die wirklich, wirklich schlimmsten Straftaten. Dann hat die Polizei, um das zu umgehen, die Quellen-TKÜ quasi erfunden, damit sie sich nicht daran halten müssen. So erklärt sich, dass es diese Quellen-TKÜ nur im deutschen Recht gibt, aus der Herleitung des Bundesverfassungsgericht-Urteils.

Ja, es gibt in Deutschland und in der ganzen Welt jede Menge Stellen, die Opfern anbieten, Geräte zu untersuchen. Jetzt möchte ich mal ein bisschen freundlich formulieren. Die Quote an wirklich relevanten und interessanten Einsendungen über eine öffentliche Ansage „Du wirst überwacht, kommt zu uns, wir überprüfen." Das ist nicht wirklich sehr hoch. Man braucht ordentliche Filter für so was.

Glücklicherweise gibt es NGOs wie das Amnesty International Security Team, oder Access Now. Reporter ohne Grenzen hat mittlerweile ein eigenes Lab. Die sind in der Lage, in ihren eigenen Netzwerken Leute aufzurufen, bei Verdacht zu ihnen zu kommen und Geräte untersuchen zu lassen und auch diese Art von Filterung vorzunehmen. Aber weltweit ist Deutschland jetzt wahrscheinlich nicht ganz oben in der Anzahl der Einsätze und auch in dem Missbrauch gegenüber Journalistinnen, Aktivistinnen, der Zivilgesellschaft und so fort.

Es gibt in Deutschland jedes Jahr Dutzende Einsätze dieser Tools und diese Opfer kommen nicht zum Chaos Computer Club und sie werden nicht öffentlich. Warum das so ist, kann ich Ihnen nicht sagen. Aber es kann durchaus sein, dass auch nicht jeder Strafverteidiger, jede Strafverteidigerin aus Ermittlungsakten herauslesen kann, dass dort Geräte gehackt werden. Ich bin kein Jurist, erst recht kein Strafverteidiger. Ich weiß nicht, wie das heutzutage in Ermittlungsakten aussieht, ob da steht, die Polizei hat am Tag X Tool Y eingesetzt. Wenn das so ist, dann dürfen diese Strafjuristinnen gerne zum Chaos Computer Club, zu mir oder zu anderen Organisationen kommen.

Aber ich befürchte nicht in allen Strafverfahren ist das so deutlich. Sondern da sind dann einfach ein Ausdruck der WhatsApp-Nachrichten, ein Ausdruck der Telegram-Nachrichten oder was auch immer einfach in der Akte, ohne zu beschreiben, woher die kommen.

Noch mal kurz zu den Klima-Protesten: Ja, derzeit wüsste ich nicht, dass Klima-Aktivistinnen von solchen Tools betroffen wären. Aber es wäre doch schön, wenn sie sagen, das wird auch nicht passieren. Wenn sie sich heute hier hinstellen und versprechen, dass das auch nicht passieren wird. Denn ich habe da so meine Zweifel, ob jedes Landesamt für Verfassungsschutz und jedes Landeskriminalamt, das in den

nächsten drei, fünf, zehn Jahren genauso sehen wird. Meinetwegen können wir nach der Session noch eine Wette abschließen.

Jeroen Lenaers (Chair): Róża Thun had to go and vote in the ITRE-Commitee. So we have Mr. Lebreton.

Gilles Lebreton: Firstly, I would like to thank Mr. Meister for his very interesting contribution. The key subject is the data hacking in Germany in particular. You gave us a picture which is really worrying. You're saying that this country claims that this surveillance is just for serious crimes, for child pornography, for example, for national security purposes. But in fact, you are saying that you've seen majority of cases are abuses. This surveillance is conducted for other reasons in most cases.

So in your view, why is this happening in a country, which is usually seen as a good country in terms of respect for the rule of law? Why is this being used for other purposes? This kind of spying is very worrying. In countries, which are not governed by the rule of law, you may expect this. But it's very worrying in a country like Germany, at least for me.

Secondly, what's the urgent solution? What do you advocate? Do you think the solution would be to ensure that in each states their national legislation has some kind of interlocutor for the police or for those networks practising this kind of spying? Could it be a specialised committee of the National Parliament, for example? Thank you in advance for your answer.

Andre Meister: I am not sure I claim that most of the cases in Germany were abuses of these tools. There are uses of this tools, and they are legal, because the lawmaker parliament has written it into law. They have proclaimed in parliament, it's only used against terrorism and the most serious crimes. But they have written in law that it's legal to use it against a whole list of 42 serious crimes, which includes all kinds of drug crimes, frauds, extortions and similar similar crimes. So I'm not sure I would call them abuses, but it's what German parliament decided to write into law. So that's what they are using it for. They have, in my view, just not been very open before writing it into law, because that's not what they in their speeches in Parliament actually used as examples.

I am not sure I understood the second question. If we are talking about the use of these tools by police, there is, in almost every case, a court order to use this. This is not true for the secret services, which have their own systems of granting these uses. They are not public. They're different in every of the 16 states and again, different for the domestic, the external or the military spy agency on a federal level. But there is some kind of

accountability to either mostly before, but in urgent cases after these cases have been happening, to get approval. So these are these cases that you call abuses. They are not only written into law, but also approved by some government body.

Now, these are the cases we know about. As I said, there is a ton of cases we do not know about, that have no public scrutiny. And every time there's real scrutiny, independent scrutiny, public scrutiny, we find that there are also illegal uses. I have said two examples from the external spy agencies from the early 2000s, which used these tools illegally. Even way before they had a specific law allowing them to use this.

Whether there is sufficient oversight for this by agencies, especially the foreign intelligence agency BND, we cannot know. We cannot say, because we just don't have the data. Only the agencies themselves have this.

Jeroen Lenaers (Chair): Thank you, Ms. Novak.

Ljudmila Novak: Thank you very much. Thank you for the floor. I'd like to thank you for your presentation. I'd like to ask you a question. What is better, in your view: A ban on the use of Pegasus or better regulation when using Pegasus?

And if, on the one hand, we introduced a ban in the EU of this spyware, it's not a given that other countries, third countries, will ban it as well. And this will basically give an advantage to these third countries. So would you say that these programmes need to be banned or regulated? And what needs to be included in the regulation that would make it more likely to be for it to be used lawfully?

Andre Meister: If you ask for my personal opinion, I agree with the EDPS, David Kaye, a former UN special rapporteur, the IT tech companies and various members of this committee like Carles Puigdemont, that a ban on these tools is necessary.

You cannot put the genie back into the bottle. You have to ban this. There are so many fundamental problems, especially the zero-day-problem, which causes a real security dilemma for national security, for European security, for public security. I think a ban is overdue.

You have options to regulate, so that Europe will not in some way fall behind. Of course, regulating things like zero-day-vulnerabilities should be a global effort. And the EU, if it decides to do that, can lead a global effort. I mean, we have seen awesome initiatives of the EU, like the GDPR, which are now a global beacon, and everyone is running to copy that.

The EU and its member states can on UN and various other levels, advocate for a ban on an international ban on the use of zero-day vulnerabilities. Just like there are international bans on other things like weapons.

Now, I have said that I would advocate for a ban of these tools, because I think as long as they exist, they will always be abused. And they have a fundamental security dilemma.

But there are minimum safeguards and conditions that, if you choose not to advocate for a ban, you should do at the very minimum. My friends at Privacy International have, I think already in 2018, published a paper, including ten safeguards for government hacking. And European Digital Rights, just two weeks ago published a paper with eleven conditions for state hacking. I can resend you those papers. And I agree with every single one of those conditions.

The most important, I think, is the security problem. You have the security dilemma. You must not allow any public or private entity to deal, trade or use zero-days. I understand you will have a hearing on this very issue next week.

Also, every member state in the EU should impose a limit on the transnational use of these tools without the consent of the target country. If these tools are only used for terror and the most serious crimes, every target country will agree with these tools being used on their soil. So let's make it illegal to use these tools without the target country's consent.

A technical and slightly underlooked point is impersonation. States and other hackers use impersonation, claiming to be someone else to phish people into installing state hacking tools on their devices. We have seen concrete example in Spain. The Spanish agency sent SMS messages saying „We're the Social Security service of Spain. Here's your Social Security number. You need to click on this link." You cannot do that. That undermines trust in the very institutions of the state.

I understand similar phishing cases impersonating state entities have happened in Poland, although I do not understand the details.

If you're also asking me for my opinion, I think states should not oblige internet service providers or any kind of internet technology companies to assist in installing these tools. Our infrastructure, our networks, they have to be neutral. They can't be attacked by everyone and anyone. We should treat them like the Red Cross and Red Crescent in war

zones. I think states should never hack a telecommunications provider or make them hack their own customers.

Another important aspect is: no bulk hacking. If you have to hack, if you have to decide that a ban is for some reason not an option, please target only individuals, never entire infrastructure, networks or providers.

And also, you have the power to make these rules global. If any company or any customer of any company breaks these provisions, breaks these safeguards, anywhere in the world, you can sanction them. You can stop them from doing business in the EU. The US has sanctioned NSO. You can do the same for Europe.

So I don't see a race with third countries. It's the other way around. The EU can lead in this.

Jeroen Lenaers (Chair): Thank you. Hannes Heide.

Hannes Heide: Danke, Herr Meister. Ich möchte aber schon feststellen, dass ich bedaure, dass wir heute nicht mehrere Auskunftspersonen zur Verfügung haben, um auch andere Zugänge, andere Einschätzungen und Informationen zu bekommen.

Meine erste oder generelle Frage über den Rechtsrahmen in der Bundesrepublik Deutschland, wie weit der ausreichend ist, ist so halbwegs beantwortet, wenn ich das so sagen darf. Um es zusammen zu fassen: Sie kritisieren vor allen Dingen die Informationspolitik, zu wenig Transparenz, die Geheimhaltung in diesen ganzen Fällen.

Aber womit wir zu einer Frage kommen. Sie haben in Ihrem Statement mehrere Anbieter erwähnt und auch dann die Eigenproduktion, wenn ich so bezeichnen darf, is also spezifischer Pegasus. Sie haben auch erwähnt. Was mag der Grund sein, dass mehrere Systeme gleichzeitig im Einsatz sind? Haben sie unterschiedliche Fähigkeiten oder Möglichkeiten? Ist das der Grund oder gibt es andere Gründe?

Eine andere Frage: Sie haben ja die Arbeit dieses Ausschusses sehr genau verfolgt und auch darüber berichterstattet. Mich würde interessieren. Sie haben viele Auskunftspersonen gehört, auch von Unternehmen. Ist Ihnen da irgendetwas aufgefallen, was mit Ihrer Recherche oder Ihren Wissen nicht übereinstimmt? Auskünfte, die uns gegeben wurden, also speziell von Unternehmen.

Und eine weitere Frage betrifft dieses DSIRF. Das erste Mal habe ich gelesen in einem Beitrag von Ihnen. Mich würde interessieren, wie Sie darauf aufmerksam geworden sind

und wie Sie auch zu dieser Präsentation gekommen sind, in der sich das Unternehmen vorstellt. Danke schön.

Andre Meister: Ich bin mir nicht sicher, ob das deutsche Rechtssystem ausreichend ist. Ja, die Transparenz ist ausbaufähig, um es mal so zu formulieren. Es ist notwendig, dass da mehr Transparenz herrscht. Denn jedes Mal, wenn irgendeines dieser Tools unabhängig evaluiert wurde, wurde massiver Missbrauch, Illegalität und anderes bewiesen. Immer, wenn der Chaos Computer Club, Citizen Lab oder Amnesty Tech diese Tools findet, gibt es Missbrauch.

Wir können den staatlichen Institutionen, die dann solche Berichte schreiben, nicht erlauben, sich selbst zu kontrollieren. Zumal es keinen Grund für eine Geheimhaltung gibt. Kriminelle wissen auch heute, dass ihr Telefon abgehört wird oder ihre Wohnung durchsucht werden kann. Sie wissen auch heute, dass Smartphones gehackt werden können. Es gibt keinen Grund für diese Geheimhaltung.

Und wie angemerkt, ich würde mich freuen, wenn der klare Satz im Koalitionsvertrag, den Frau Barley dankenswerterweise da mit reingeschrieben hat, auch umgesetzt wird. Wie gesagt, derzeit sind die Signale aus dem Bundesinnenministerium, dass das Gegenteil der Fall ist und dass sie jetzt doch den Koalitionsvertrag brechen wollen und explizit das Ausnutzen und Geheimhaltung von Sicherheitslücken erlauben wollen.

Warum kaufen Staaten verschiedene Produkte und entwickeln ihre eigenen? Am Anfang, nach dem DiGiTask offensichtlich illegal war und nicht mehr eingesetzt wurde, hat der deutsche Staat begonnen, sein eigenes Produkt zu programmieren. Man hat gesagt, nur so können wir sicherstellen, dass es tatsächlich alle legalen Ansprüche einhält, alle gesetzlichen Vorschriften.

Das hat aber ein Stück gedauert und am Anfang hieß es, wir kaufen FinFisher mal für die Übergangszeit, bis wir unser eigenes Produkt fertig haben. Hat nicht ganz geklappt, denn FinFisher musste so oft überarbeitet werden, dass das überarbeitete FinFisher länger gebraucht hat, als das BKA ihr eigenes Tool programmiert hat. Sie nutzen es weiterhin oder haben es bis vor einiger Zeit weiterhin nutzen wollen. Dann mit der veränderten Begründung: als Backup-Plan, falls unser eigenes Tool nicht funktioniert. Und das ist der eigentliche Grund.

Diese Tools sind alle verschieden. Sie tun nicht dasselbe. Es fängt schon bei Smartphones an, es gibt zwei große Betriebssysteme. Aber wie gesagt, diese Tools zielen nicht nur auf Smartphones. Candiru zielt auf Windows-Rechner. Auch DSIRF hat mit Windows angefangen, wollte macOS später, und dann erst iOS und Android. Andere

dieser Systeme hacken Internet Router. Wir wissen, dass die ZTIiS daran forscht, Autos zu hacken.

Für jedes Zielsystem, für jede Intrusion, um da reinzukommen, brauchen Sie spezielle Sicherheitslücken. Es muss speziell auf das Betriebssystem angepasst werden. Und mit den aktuellen Versionen mitgezogen werden, in dem ewigen Katz-und-Maus-Rennen.

Also aus einer technischen Sicht kann ich verstehen, warum staatliche Behörden mehrere dieser Tools haben. Ich würde mich freuen, wenn auch der Bund der Steuerzahler oder der Bundesrechnungshof mal eine Analyse davon macht, ob das auch angemessene Verwendung von Steuergeldern ist. Aber auch die werden eine schwere Zeit haben, angemessene Informationen bekommen.

Auskünfte von Unternehmen, habe ich mir noch notiert. Können Sie mir ein Stichwort geben?

Hannes Heide: In den Hearings waren verschiedene Unternehmen auch präsent oder oder verschiedene Auskunftspersonen. Und mit ihrem Wissen, ob ihnen da eklatant etwas aufgefallen ist, dass etwas mit Ihren Recherchen nicht übereinstimmt oder andere Kenntnisse.

Andre Meister: Ich muss gestehen, dass ich nicht die Zeit hatte, sämtliche 13 oder 14 Hearings, die es mittlerweile gab, zu gucken. Und da möchte ich diese Gelegenheit auch mal nutzen: Warum produziert dieser Ausschuss keine Transkripte? Niemand hat die Zeit, sich vier Stunden Video anzugucken. Sie nicht, ich nicht, und erst recht die Öffentlichkeit nicht. Warum gibt es keine Text-Transkripte ihrer Anhörungen? Dann hätte ich mir sehr gerne in der Vorbereitung auch die Aussagen der ganzen Firmen hier angeguckt. Das, was ich von den Texten gelesen habe, nichts davon kann ich widersprechen. Aber ich habe nicht die vollständigen Sessions angeguckt.

Hannes Heide: Sie haben nämlich eins transkribiert. Nämlich mit Pegasus, mit NSO. Ist da nichts aufgefallen?

Andre Meister: Von NSO Pegasus gab es ein Transkript. Das haben wir erhalten und veröffentlicht. Es ist mir nichts präsent. Das war das zweite Hearing. Das ist Monate her.

In der Tat sind mir da schon komische Dinge aufgefallen. Aber Edin von Privacy International, der direkt danach gesprochen hat, hat glaube ich die Punkte besser gekontert, als ich das jetzt so viel später tun kann.

Ich dachte, Sie meinen die Big-Tech-Firmen.

DSIRF, das ist eine sehr illustre Firma. Ich bin auf die aufmerksam geworden. Ich war gar nicht der Erste. Vor uns war der Focus, ein deutsches Nachrichtenmagazin, das über einen anderen Teil des Business von DSIRF berichtet hat. Und zwar über biometrische Überwachungssysteme in großen Anlagen bis hin zu Einkaufszentren und Flughäfen und so weiter und so fort. Gesichtserkennung, Verknüpfen mit Kundenkarten und echten Identitäten von Menschen.

Der Focus hat es entdeckt und darüber berichtet und in einem Nebensatz erwähnt: „Und Sie tun auch so, als ob sie Spyware herstellen." Ich habe das gelesen und gedacht „Das ist ja interessant." Und fange an zu recherchieren.

Ich kann und werde jetzt hier meine Quellen nicht offenlegen. Aber ich glaube, ich habe vorhin schon gesagt, wir haben die Präsentation von DSIRF und ihrem Produkt Subzero in einer E-Mail von Jan Marsalek entdeckt. Und ich glaube, ich habe die E-Mail dann auch veröffentlicht. Und die Produktwerbung, die Produktbroschüre sowieso, mit weiteren Hintergrundinformationen zu der Firma.

Mehr als das, was wir damals veröffentlicht haben und was bisher in Österreich und durch andere Berichte raus gekommen ist, kann ich leider auch nicht öffentlich beitragen.

Jeroen Lenaers (Chair): Thank you. Katarina.

Katarina Barley: Ja, es gab zwei Fragen, die noch offen waren von mir. Das eine, ob ihnen bekannt ist, andere Staaten, die solche Programme quasi bestellt haben, abgespeckt haben, damit sie zu ihrem nationalen Regelungsrahmen passen. Und das zweite noch mal zu der Funktionsfähigkeit des Rechtsschutzes.

Andre Meister: Ich dachte, ich hatte beide beantwortet.

Ich kenne kein anderes Land, dass so etwas wie eine Quellen-TKÜ konzeptionell juristisch hat. Deswegen hat auch kein anderes Land das als Anforderungen in ihren Kaufverträgen und auch das mit dem Rechtsschutz.

Wir hatten schon eine politische Debatte. Ich bin kein Jurist. Verzeihen Sie mir, dass ich jetzt nicht detailliert analysieren werde, wo im deutschen Rechtssystem noch nachjustiert werden könnte.

Wie ich auf die anderen Anfragen gesagt habe: Ich glaube nicht, dass wir großartig versuchen sollten, im Nachhinein einzelne Stellschrauben nachzujustieren. Aus unserer Perspektive sind diese Tools so gefährlich und auch nicht notwendig, weil es gibt ja Alternativen, dass wir nicht nachträglich irgendeinen Rechtsschutz einbauen sollten, sondern dafür sorgen sollten, dass die in der EU und in der ganzen Welt nicht mehr genutzt werden.

Jeroen Lenaers (Chair): Thank you. Just a couple of questions from my side.

One thing you said was interesting. When you look at the statistics, you said both for last year and this year, there are a number of issues where the police was granted the permission to use hacking and then a number of cases where it was used. So I think for this year it was 48 times granted, 22 times they actually used it. So what what contributes to this difference between the 48 and the 22? Is those 26 times factors that they feel to do it or they chose not to do it. What what is the reasoning behind that?

Secondly, on victims, we've heard that at least in the majority of EU member states with two, I think, notable exceptions, targets or victims of this kind of spyware have the right constitutionally to be informed. After the spying, when the hacking has ended. So at least when there is no more national security or whatever legal reason to do the spying, they have the right to be informed. And therefore, I'm surprised about the lack of victims known in that sense, because there's no such such mechanism in Germany?

And then thirdly, on the legislation. You mentioned the 42 grounds for hacking that are in the legislation. Are these all at the same level? Are they is there a hierarchy? And is there certain types of spyware or hacking that you can use for terrorism or murder, but not for extortion or drugs? Or is all of these 42 grounds for using state hacking, regardless of what kind of technology can be used to do the hacking?

Andre Meister: Yes. Thank you.

Very sharp to observe the difference between how many times police were granted to use these tools and actually use them in practise. Again, unfortunately, we do not have official answers of this difference in official answers.

It is hard to install state hacking tools. It is hard to hack devices. It is technically complicated. You need to know a lot of information about the target device. If it is up to date, if it is following all the security precautions. Especially with German police's own developed software, it does probably not have a full list of all zero-day vulnerabilities

usable against most currently patched iPhone. It's a technological race, a cat and mouse game between defenders and offenders.

Jeroen Lenaers (Chair): With Pegasus.

Andre Meister: We don't know how many times German police have used NSO Pegasus. They have only cleared it for use last year. The statistics we have were for 2020, so the statistics were Pre-Pegasus.

Pegasus, as I understand it, was or is, we don't really know, exceedingly good. Attacking, fully patched, especially iPhone and Android devices. But maybe the target had a BlackBerry. Maybe they had a feature phone. Maybe they had a hardened Linux system. Maybe they wanted to hack their email service provider. It's not just about two types of smartphones. It's about any digital device people are communicating with. So we don't know what the difference is. And I would be glad if the police were here to tell us.

Yes. In Germany, we also have a system, that people who are surveilled by police and even by secret services, have to be notified of their surveillance after the proceedings ended. That's in the law. However, that is also not the practise. It is not the case that every single victim in every single case is actually concretely notified of how specifically they were targeted. I have yet to see such an information. I would be highly interested in that.

We have an example. There are legal battles in Germany about the duty to inform people after they have been surveilled. We have this thing called „Funkzellenabfrage" or cell tower dumps, which has also been a pet project of mine. I've been working on that for many years. There the police gather thousands and millions of cell tower call data records from areas of crime, creating a de facto data retention for a certain place and time.

By law, they have to notify every single individual whose data they collect with it. But they don't. They claim that these people don't have an interest to be informed about that. And they claim that they don't know who these people are, even though they have their phone number. So this is a legal battle in Germany and a political battle, too.

Maybe we should go back to the law and maybe have some kind of statistics. I don't know of any statistics of how many of those surveillance where has happened were notified. I would be glad if the notification quota is 100%, but I fear that's not the case.

And if people were notified, it is still a question how understandable and detailed they are told what has actually happened. Because they might just be told „We have done telecommunications surveillance on you with this section of the Criminal Code." But it does not differentiate between a classic phone tap and active hacking of their device. That's the legal trick they use. It's the same paragraph in the law. So they might have said, we've done surveillance, communications surveillance on you. And not even lawyers will know for sure that they've been targeted by state hacking.

There's only one difference in German spyware between a small state hacking just exfiltrating communications and big state hacking exfiltrating everything and anything on a device. But beyond that, there is no further distinction. There is one list of 42 serious crimes which allow police to tap a phone and also to hack the device. There is no distinction between the formation of a terrorist organisation, the formation of a criminal organisation, murder or drug crimes or the other not so grave crimes I have mentioned.

Yeah, I think that answers the question.

Jeroen Lenaers (Chair): Yes. Maybe one additional question, because there is no distinction made in the law in the sense is the distinction made when requesting a court order, as we've seen from other countries, for instance, that where court orders were there for the surveillance or the installing of spyware on certain targets, but these targets were only known by a number the technology used to do the hacking was not disclosed through the courts. Is there a need in Germany? If you ask for a court order, the police ask for a court order to to use this legislation to to hack. Do they need to inform the judge whether this is classic wiretapping or using technology to target a device? And if so, which technology used? Or is it something that could be done also without the knowledge of the courts?

Andre Meister: That's a very good question. I am not a lawyer or a judge myself. As far as I know, the investigators only specify the section of the criminal code, saying we want to do surveillance on this, we used to call them, selectors, on this phone number, an email address or whatever identifier of a target. I am pretty sure that most of these applications do not clarify between a difference of we want to do a classic phone tap or active hacking of a device because it's at the exact same legal code. They will say, and we'll do a communications interception according to section 100a of the Criminal Procedure Code. That's it.

Then it is highly unlikely and I would doubt that they ever voluntarily disclose the actual tool they use. They don't even do that for classical surveillance system. We use our classical phone tapping surveillance. I forgot the name. I published the name once. Something similar to Pegasus actually. But they will not disclose. We want to surveil this person and we were going to use RCS or Pegasus or FinFisher. That will not be in a court order and it will especially not be in the possible notifications these people might get later.

On this, allow me a recourse to my introductory statement. The very fact that in the reporting of how many times this has happened, the prosecutors have mixed up a classic phone tap and active hacking of devices in their statistics, shows that in practise that difference is interesting to us and integral to this committee, but not to the day -to-day work of criminal justice courts. I don't know if you've been. Most would claim they read every word of every application they get on their desk. But I hear that with the workload they have, that might not always be the case.

Jeroen Lenaers (Chair): A comment from Katarina Barley.

Katarina Barley: Yes, I couldn't answer that question. The times when I was a judge, are way past this technique. But I would just be grateful to indicate when it's a presumption that you're making and not a knowledge. It was pretty clear, but it then got kind of confusing. So I couldn't answer that question myself. I have been I have ordered this kind of but very conventional surveillance at the time. And yes, you do have a workload as a judge but you know that this is the most serious operation that you can allow. So I would presume that judges are acting responsibly with that. But I'm also in the field of presumption here, so I think we should make that clear.

Jeroen Lenaers (Chair): Thank you for the comment. And to be honest, I think it was very clear that Mr. Meister spoke of presumptions when he indicated that. Also, because he was very clear that he was not a lawyer or a judge and that he's here as an expert, as a journalist.

And I'm very, very happy that you also provide your opinion on these on this matter, also, because we keep, including myself, keep asking him questions that maybe fall in the domain of lawyers or judges. So and we I expect him to to answer our questions. So thank you. Thank you very much.

Another Member has arrived. I'm not sure if you... we are at the end of our Q&A. So if you have any more questions. No, then thank you very much.

Thank you very much, Mr. Meister, for being here. I have noted your your offer also to to send us some some additional information. Also with regards to the papers that are already distribution about the ten point plan, etc. I very much appreciated that you took the time to spend this Monday afternoon with us.

I share your your disappointment, which was also shared by many of the members, that you were the only guests here and that the German police authorities, even though they were invited, did choose not to participate in our hearing.

It's not a unique case in in Germany. We have this with other member states as well. But it is disappointing.

But this is a little bit the fate of our committee. We will have to do a work against the resistance of some official authorities. But that shall only encourage us, just like it encourages you to keep on doing your job, your very important job that you do in investigating these issues in Germany. So thank you. Thank you very much.

Thank you for the colleagues. We meet again on, I believe, next week, Thursday, the 24th, if I'm not mistaken. Yes, I get the confirmation from Mr. Meister, that we meet again on Thursday 24th of November from 9 to 12.

Thank you all very much and have a nice evening.

Über die Autor:in

andre

Andre ist seit 2008 bei netzpolitik.org, seit 2012 festangestellt. Er beschäftigt sich vor allem mit investigativer Recherche. Andre hat Sozialwissenschaften an der Humboldt-Universität zu Berlin studiert und Abschlüsse in Bachelor und Master zu netzpolitischen Themen gemacht. Er ist Gründungsmitglied der Vereine Digitale Gesellschaft, Gesellschaft für Freiheitsrechte und netzpolitik.org, Mitglied im Chaos Computer Club sowie Beobachter bei European Digital Rights. Nebenbei arbeitet er als System-Administrator.

Veröffentlicht
15.11.2022 um 12:27

Kategorie
Überwachung

Schlagworte
BKA, BMI, BND, Bundeswehr, Candiru, DSIRF, Europaparlament, FinFisher, FinSpy, Geheimdienste, Hacken, Hermit, IT-Grundrecht, Online-Durchsuchung, PEGA Transkript, Pegasus, Pegasus-Ausschuss, Präventivgewahrsam, Quadream, Quellen-TKÜ, RCIS, RCS, Spähsoftware, Spyware, Staatliches Hacken, Staatstrojaner, Subzero, Untersuchungsausschuss, ZITiS

3 Ergänzungen

Mit Menschen rechnen. sagt:
16. November 2022 um 13:21 Uhr

Sollte ein Verbot nicht funktionieren, wäre das wohl das Ende der „responsible disclosure“. Man kann ja nicht warten, während der Hersteller an die Behörden durchsteckt, in der Hoffnung, dass da nicht irgendwo einer ungemeldete Nebenverdienste hat.

Da kommt dann bestimmt ein Sicherheitsgesetz zu, dass das dann wiederum kriminalisiert. Dann haben wir einen Agendaindikator.

Smeagol sagt:
16. November 2022 um 19:50 Uhr

Gute Rede, toll zusammengefasst worum es geht.

Stephan sagt:
17. November 2022 um 11:45 Uhr

Schade, dass nur so wenig Leute diese Rede gehört haben.
Die Reihen sahen ziemlich ausgedünnt aus.

Da darf man sich nicht wundern, dass das digitale Verständnis im Parlament auf der Strecke bleibt.