Date: 2022-11-14
From: Andre Meister <andre@netzpolitik.org>
To: European Parliament, PEGA Committee

Country hearing: Germany

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.[1]

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[2] 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.

Definition

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.

1 https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/
2 https://www.sophieintveld.eu/nl/pega-draft-report

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.[3] 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[4], 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".

History

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

In 2005, the foreign intelligence agency BND hacked the government of Afghanistan[5], where they exfiltrated emails between an Afghan minister and a German journalist.[6] 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 the wife of another German spy.[7] 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.[8]

Another important state hacker is the military. In 2015, the German military hacked a mobile network operator in Afghanistan.[9] 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.

Use cases

Customs and police in Germany have been hacking since at least 2008. The first three targets that became public were suspects selling anabolic steroids[10], fake Viagra, and contraband cigarettes[11].

3 https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/
4 https://netzpolitik.org/2019/staatstrojaner-zitis-will-autos-hacken/
5 https://www.spiegel.de/international/germany/bnd-scandal-how-german-spies-eavesdropped-on-an-afghan-ministry-a-550212.html
6 https://www.spiegel.de/international/germany/german-spy-chief-under-pressure-agency-admits-spying-on-afghan-politician-and-spiegel-journalist-a-549488.html
7 https://www.spiegel.de/politik/digitale-spionage-a-4d084fc3-0002-0001-0000-000064497190
8 https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html
9 https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html
10 https://www.spiegel.de/netzwelt/netzpolitik/ueberwachungssoftware-der-staatstrojaner-kommt-aus-bayern-a-790960.html
11 https://www.tagesspiegel.de/potsdam/brandenburg/schnuffelsoftware-nicht-im-masseneinsatz-7446136.html

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.[12] 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".[13] 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[14], German police were granted to hack 64 times and actually did 15 times.[15] More than a third of cases were extortion, another third were drugs. There were zero cases of terror and zero cases of murder.[16]

In 2020[17], the must current numbers we have, German police were granted to hack 48 times and actually did 22 times.[18] Again, more than a third of cases were drugs, another third were extortion. Again, there were zero cases of murder.[19]

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

Civil society

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

12 https://netzpolitik.org/2018/bka-dokument-polizeibehoerden-wollen-staatstrojaner-vor-allem-gegen-drogen-einsetzen/
13 https://dipbt.bundestag.de/dip21/btp/18/18240.pdf#page=128
14 https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2020/20200122.html?nn=74788
15 https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/
16 https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Online_Durchsuchung_2019.pdf?__blob=publicationFile; https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2019.pdf?__blob=publicationFile
17 https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2022/20220808.html
18 https://netzpolitik.org/2022/justizstatistik-2020-polizei-setzt-staatstrojaner-alle-zwei-wochen-ein/
19 https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistik/Uebersicht_Online_Durchsuchung_2020.pdf?__blob=publicationFile; https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistik/Uebersicht_TKUE_2020.pdf?__blob=publicationFile

than treason for doing our job[20]: reporting truthful information in the public interest on the internet surveillance capabilities of his agency.[21] 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[22] and climate activists[23]. 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.[24]

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.

Law

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.[25] 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.[26] 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.[27]

Last year, a new law officially legalized state hacking for all 19 German intelligence agencies[28], 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

20 https://netzpolitik.org/2015/verdacht-des-landesverrats-generalbundesanwalt-ermittelt-doch-auch-gegen-uns-nicht-nur-unsere-quellen/
21 https://netzpolitik.org/2015/classified-department-we-unveil-the-new-unit-of-the-german-domestic-secret-service-to-extend-internet-surveillance/
22 https://www.verfassungsschutz.bayern.de/mam/anlagen/vsb-2020_210414.pdf#page=258
23 https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2022-06-07-verfassungsschutzbericht-2021-startseitenmodul.pdf?__blob=publicationFile#page=143
24 https://www.polizei.bayern.de/aktuelles/pressemitteilungen/038276/index.html
25 https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/__20k.html
26 https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/
27 https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528
28 https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408

customers.[29] The communication providers vehemently criticized this, citing risks for the integrity of their infrastructure, a loss of trust, and an attack on IT security.

Fundamental rights

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".[30]

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."[31]

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

Legal trick

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.[32] 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".[33]

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".[34]

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.[35]

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.[36] 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.[37] Once you hack a device, you have

29 https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/
30 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
31 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
32 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html
33 https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0604
34 https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528
35 https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-g10-vb
36 https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/
37 https://cdn.netzpolitik.org/wp-upload/Rehak-Angezapft.pdf

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.[38] 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.[39] It took FinFisher five years and three versions, until the tool was in line with the legal requirements.[40]

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.[41] Since then, they have used it at least “half a dozen” times.[42]

Products used

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[43] 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.[44] 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.[45]

Official investigations verified the CCC revelations.[46] DigiTask was found to be illegal, and law enforcement abandoned the product. The company has since repeatedly been sold[47], most recently to German electronics giant Rohde & Schwarz[48], which is also a sponsor of the Wiretappers Ball ISS World.[49]

After this disaster, German police developed their own hacking tool called “Remote Communication Interception Software” or RCIS.[50] In four years, 29 police officers programmed a

38 https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma/
39 https://netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisher-finspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal/
40 https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/
41 https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-103.html
42 https://www.zeit.de/politik/ausland/2022-07/nso-pegasus-ueberwachung-klage-untersuchungsausschuss/komplettansicht
43 https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-107.html
44 https://www.ccc.de/en/updates/2011/staatstrojaner
45 https://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner
46 https://www.datenschutz-bayern.de/0/bericht-qtkue.pdf; https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_11_12.pdf?__blob=publicationFile#page=97
47 https://www.handelsregisterbekanntmachungen.de/skripte/hrb.php?rb_id=251567&land_abk=sn
48 https://www.rohde-schwarz.com/ch/news-und-presse/pressebereich/pressemitteilungen-detailseiten/rohde-schwarz-uebernimmt-ipoque-gmbh-pressemitteilungen-detailseite_229356-63128.html
49 https://www.issworldtraining.com/ISS_EUROPE/sponsors.html
50 https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/

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.[51] 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[52], the Italian company RCS Labs and its product Hermit[53], and the Israeli companies Quadream[54] and Candiru[55]. However, the government refuses to provide a comprehensive list of companies ZITIS met, let alone products it bought for police and intelligence to use.[56]

Secrecy

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.”[57] 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.[58] 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.[59]

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.[60]

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.[61] Unfortunately, they didn’t. Now they are part of the government.

---

51 https://www.zitis.bund.de/
52 https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12
53 https://dserver.bundestag.de/btd/20/038/2003840.pdf
54 https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29
55 https://dserver.bundestag.de/btd/20/003/2000327.pdf
56 https://dserver.bundestag.de/btd/20/041/2004141.pdf#page=39
57 https://www.sophieintveld.eu/nl/pega-draft-report
58 https://fragdenstaat.de/anfrage/vertrag-ueber-nso-pegasus/#nachricht-727800
59 https://netzpolitik.org/2022/untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/
60 https://netzpolitik.org/2022/staatstrojaner-bundesregierung-verweigert-antwort-zu-nso-pegasus/
61 https://www.sueddeutsche.de/digital/it-sicherheit-bka-verpasst-staatstrojaner-testern-maulkorb-1.3942712

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[62], we requested the contract.[63] The police denied meaningful information, so we sued them[64] – and won.[65] Later, we filed another request for updates to this contract.[66] The police again denied meaningful information. So again, we sued them[67] – and again, we won.[68]

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.[69] The police again denies to provide any information. The dispute is ongoing, but it looks like we will have to sue the police again.[70]

But even when we win, mostly we get what's already public or of little relevance. This is the contract with FinFisher the police gave us after we won in court.[71] 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 is what they gave us.[72] It will remain redacted and classified like this until the year 2080.[73] 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".[74] This is super relevant. But the document is classified and locked away.[75] Two: The Police has analysed NSO Pegasus.[76] But this report is beyond classified and locked away.[77] Three: The Police commissioned

62 https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma/
63 https://cdn.netzpolitik.org/wp-upload/2013-04_Vertrag-BKA-Elaman-FinFisher-Klage.pdf
64 https://netzpolitik.org/2015/wir-verklagen-das-bundeskriminalamt-wir-wollen-einblick-in-den-den-vertrag-ueber-den-staatstrojaner-finfisher/
65 https://netzpolitik.org/2015/urteil-gegen-das-bka-teilerfolg-beim-staatstrojaner-vertrag/
66 https://fragdenstaat.de/anfrage/anderungen-zum-vertrag-mit-elamangamma-uber-staatstrojaner/
67 https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/
68 https://netzpolitik.org/2022/finfisher-vertrag-wir-haben-das-bka-verklagt-und-gewonnen/
69 https://fragdenstaat.de/anfrage/vertrag-ueber-nso-pegasus/
70 https://fragdenstaat.de/anfrage/vertrag-ueber-nso-pegasus/#nachricht-727800
71 https://netzpolitik.org/wp-upload/2022/11/2015_BKA_Elaman_FinFisher_Ergaenzungsvertrag_Seite-5.png
72 https://netzpolitik.org/wp-upload/2022/02/2020-06-25_BfDI_Quellen-TKUe-beim-BKA_Seite-3.png
73 https://netzpolitik.org/2022/die-software-ist-%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88-%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88-%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88%E2%96%88/
74 https://netzpolitik.org/2014/projekt-tgatt-innenministerium-laesst-grundrechtsschonende-alternativen-zur-quellen-tkue-erforschen/
75 https://fragdenstaat.de/anfrage/studie-grundrechtsschonende-alternativen-zur-quellen-tkue-tgatt/
76 https://web.archive.org/web/20211027032730/https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-103.html
77 https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/#nachricht-638677

an external report on its other hacking tools.[78] But this document is also classified and locked away.[79]

Security dilemma

Revealingly, part of the reason to deny this report is - and I quote the police - “the providers of commercial hardware and software [could] close the attack vectors used by the surveillance software (like vulnerabilities) and prevent the use of the spyware”.[80]

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.[81] 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.[82] This argument was theoretical for a long time, but now we have an example in the EU: The Spanish state hacked Catalans[83], and with the exact same vulnerability Morocco hacked the Spanish prime minister and defence minister.[84]

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

The tech industry understands this.[85] ENISA understands this.[86] 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.”[87]

This is a much needed first step. Unfortunately, the German government still didn’t implement their promise.[88] 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.

Conclusion

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

78 https://dserver.bundestag.de/btd/19/014/1901434.pdf#page=5
79 https://fragdenstaat.de/anfrage/uberprufung-von-produkten-der-itu/
80 https://netzpolitik.org/2018/it-sicherheit-das-bka-verhindert-dass-sicherheitsluecken-geschlossen-werden/
81 https://netzpolitik.org/2020/der-staat-sollte-alle-it-sicherheitsluecken-schliessen-manche-laesst-er-lieber-offen/
82 https://citizenlab.ca/2022/07/john-scott-railton-delivers-testimony-to-house-permanent-select-committee-on-intelligence/
83 https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
84 https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
85 https://cornelia-ernst.eu/2022/06/big-tech-and-spyware-14-june-2022/
86 https://cornelia-ernst.eu/2022/10/big-tech-and-spyware-ii-26-october/
87 https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1#page=110
88 https://netzpolitik.org/2022/gegen-koalitionsvertrag-innenministerin-faeser-will-sicherheitsluecken-offenlassen/

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."[89]

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[90] – a danger to European security. Let's fight this danger.

Having stressed my time already, this concludes 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.

89 https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
90 https://netzpolitik.org/2022/staatstrojaner-untersuchungsausschuss-die-eu-kommission-verschweigt-wie-oft-sie-gehackt-wurde/