

Public Prosecutor's Office Munich I
Linprunstr. 25
D-80097 Munich

Gesellschaft für Freiheitsrechte e.V.
Hessische Str. 10
D-10115 Berlin
represented by Chair Dr. Ulf Buermeyer,
ulf.buermeyer@freiheitsrechte.org

Reporters Without Borders Germany
Potsdamer Str. 144
D-10783 Berlin
represented by Executive Director Christian Mihr,
christian.mihir@reporter-ohne-grenzen.de

the European Center for Constitutional and Human Rights e.V.
Zossener Str. 55 – 58,
D-10961 Berlin
represented by Dr. Miriam Saage-Maaß, Vice Legal Director,
saage-maasz@ecchr.eu

Netzpolitik.org
Schönhauser Allee 6/7
D-10119 Berlin
represented by Andre Meister,
andre@netzpolitik.org

herewith file a

criminal complaint

for violation of section 18 para. 2 no. 1 and section 18 para. 5 no. 1 of the
Foreign Trade and Payments Act

against

1. Mr Markus Meiler, CEO of Elaman GmbH,
business address: Baierbrunnerstr. 15, D-81379 Munich,
2. Mr Holger Rumscheidt, CEO of Elaman GmbH,
business address: Baierbrunnerstr. 15, D-81379 Munich,
3. Mr Carlos Gandini, CEO of FinFisher GmbH,
business address: Baierbrunnerstr. 15, D-81379 Munich,
4. Mr Lucian Hanga, CEO of Finfisher Labs GmbH,
business address: Baierbrunnerstr. 15, D-81379 Munich,
5. Mr Holger Tesche, CEO of FinFisher Labs GmbH,
business address: Baierbrunnerstr. 15, D-81379 Munich,
6. additional staff members whose names are unknown of Elaman GmbH,
Finfisher GmbH, and Finfisher Labs GmbH,
business address Baierbrunnerstr. 15, D-81379 Munich.

The suspects indicate the following address as the postal address of the companies FinFisher GmbH and FinFisher Labs GmbH:
Sapporobogen 6-8, c/o Kanzlei hph, D-80637 Munich.

Table of Contents

- A. INTRODUCTION AND SUMMARY 4
- B. ABOUT THE SUSPECTS..... 6
- C. ABOUT ELAMAN GMBH, FINFISHER LABS GMBH, FINFISHER GMBH 6
- D. ABOUT FINSPY 7
- E. THE FACTS AND CIRCUMSTANCES..... 8
 - I. FINSPY ON THE FAKE ADALET WEBSITE..... 8
 - II. ATTRIBUTION TO FINFISHER..... 11
 - 1. FORENSIC ANALYSIS OF THE MALWARE 11
 - 2. FURTHER EVIDENCE 12
 - III. TIME OF EXPORT OF THE SOFTWARE..... 13
 - IV. LACK OF EXPORT LICENCE 14
- F. LEGAL ASSESSMENT 15
 - I. LICENSING REQUIREMENT FOR EXPORTING FINSPY 15
 - 1. LICENSING REQUIREMENT IN ACCORDANCE WITH SECTION 8 PARA. 1 NO. 2 AWV 15
 - 2. LICENSING REQUIREMENT IN ACCORDANCE WITH THE DUAL-USE REGULATION 16
 - II. EXPORT WITHOUT THE REQUIRED LICENCE 17
 - III. THE SUSPECTS' CRIMINAL RESPONSIBILITY..... 18
 - IV. ABOUT THE STATUTE OF LIMITATIONS 19
- G. POTENTIAL INVESTIGATIVE MEASURES..... 19
- H. ANNEXES 21

A. INTRODUCTION AND SUMMARY

Factual evidence exists for the fact that the suspects, who at the point in time relevant for the criminal complaint were CEOs or staff members of Elaman GmbH, FinFisher GmbH, or FinFisher Labs GmbH, have made themselves liable to prosecution because of deliberate violations against the obligation to obtain licences for dual-use software in accordance with section 18 para. 2 no. 1 and section 18 para. 5 no. 1 Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG) by exporting the surveillance software FinSpy to Turkey during the period between October 2016 and July 2017 without having previously obtained the required licence from the [German] federal government.

In summary, the criminal complaint is based on the following facts and circumstances:

On 29 June 2017, an extract of a surveillance software application was found on a website directed to an exclusively Turkish-language audience whose source code essentially corresponds to the source code of the surveillance software application FinSpy. The website was designed so that users could easily consider it to be the website used by the Turkish opposition movement for organising – the so-called Adalet website.

In terms of its functionality, the fake Adalet website serves the sole purpose of convincing visitors to the site to install a surveillance software application disguised as an Android application that can be used for networking on their telecommunications devices. After being downloaded to a mobile device, this Android application, which is malware, enabled the attacker to access telephone and VoIP calls, data systems, screenshots and other photos, GPS data, microphones, and connection data as well as various applications, including WhatsApp, Line, Viber, Telegram, Skype, Facebook Messenger, Kakao, and WeChat.

As software analyses by independent experts confirmed, the partially readable source code of the malware found on the website is practically identical to the malware FinSpy manufactured by the companies FinFisher GmbH and FinFisher Labs GmbH (hereinafter simply: FinFisher). A Microsoft report from the year 2016 also mentions that FinSpy was found in Turkey.

FinSpy is manufactured by FinFisher and distributed together with Elaman GmbH. Apart from individual samples, which form the basis of this criminal complaint and represent only parts of the FinSpy code, no data leak of the FinSpy code has been reported. Since these parts are not sufficient for producing a complete malware application corresponding to FinSpy, it must be assumed that nobody except the companies named have access to the entire source code of FinSpy.

Because of its comprehensive surveillance functions, export of FinSpy must be licensed in advance by the federal government, section 8 para. 1 no. 2 Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung, AWV) in

conjunction with Part I Chapter B, Code 5D902 a) in conjunction with 5A902 of the Export List as well as Art. 3 para. 1 of the Dual-Use Regulation (2018/1922) in conjunction with Annex I Code 4A005.

In response to parliamentary questions, most recently on 19 June 2019, the federal government confirmed that it has not issued any such licences since January 2015.

It must be assumed that the suspects, as CEOs of the companies manufacturing and distributing FinSpy, as well as additional staff members whose names are unknown, have at least been involved in or arranged for the unlicensed exports. In so doing, they have made themselves liable to prosecution under section 18 para. 2 no. 1 and section 18 para. 5 no. 1 AWG.

We encourage the initiation of investigative proceedings because of the suspects' criminal conduct.

B. ABOUT THE SUSPECTS

Suspects 1 and 2 have been CEOs of Elaman GmbH since 23 October 2013; suspect 3 has been CEO of FinFisher GmbH since 12 August 2016; suspects 4 and 5 have been CEOs of FinFisher Labs GmbH since 12 February 2014,

Elaman GmbH - HRB [Commercial Register] 153662; FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475, cf. also Annex 3.

C. ABOUT ELAMAN GMBH, FINFISHER LABS GMBH, FINFISHER GMBH

Elaman GmbH, FinFisher Labs GmbH, and FinFisher GmbH are headquartered at the same business address in Munich and are, as far as can be established, also closely interconnected functionally and in terms of personnel. According to their registered business purpose, they jointly produce and distribute security products and systems for government agencies and government-related organisations,

Elaman GmbH - HRB 153662; FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475.

According to the excerpt from the Commercial Register, Elaman GmbH is responsible for national and international distribution and marketing. By entry into the Commercial Register on 26 September 2013, FinFisher Labs GmbH replaced Gamma International GmbH and is responsible for development, production, trade and distribution, research, as well as training in the area of software and telecommunications. The wording of the description of the activities of FinFisher GmbH, which replaced Gamma International Sales GmbH by entry into the Commercial Register on 13 October 2013, is almost identical and includes trade and distribution of software and telecommunications systems, research, and training,

FinFisher Labs GmbH - HRB 176385; FinFisher GmbH - HRB 205475; FinFisher Holding GmbH - HRB 205476.

Not only the activities of the various companies are related to one another, but their offices also coincide. Baierbrunnerstr. 15, D-81379 Munich is the official seat of Elaman GmbH; the offices of FinFisher GmbH and FinFisher Labs GmbH are in fact located there as well. The official address of FinFisher GmbH and FinFisher Labs GmbH at Sapporobogen 6-8, c/o Kanzlei hph, D-80637 Munich, is only a letterbox at a solicitor's office.

This network of companies presumably has sold surveillance software to various authoritarian regimes in recent years. The Citizen Lab of the University of Toronto reports FinSpy findings in Angola, Egypt, Gabon, Lebanon, Morocco, Oman, Saudi Arabia, Turkey and Venezuela,

<https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#1>; last accessed 2 July 2019.

The first reports about deliveries by FinFisher to authoritarian states referred to governments in the Middle East during the 'Arab Spring'. FinFisher's products were repeatedly used there to oppress and divide the political opposition in a targeted fashion. From 2010 to 2012, for example, the government of Bahrain used FinFisher to attack solicitor's offices, journalists, activists, and political leaders of the opposition movement. At first, the then CEO of FinFisher's predecessor Gamma International Sales GmbH, Martin Münch, denied exports to Bahrain,

<https://web.archive.org/web/20120731005707/http://www.bloomber.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html>; last accessed 3 July 2019,

but archival and licensing documents of in-house customer support published by a non-governmental organisation in August 2014 evidenced that Gamma International Sales GmbH had maintained business relations with the government of Bahrain since 2010,

<https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/>; last accessed 2 July 2019.

The communications technology used by Ethiopian dissidents was also infected with FinSpy software in the past,

<https://www.eff.org/cases/kidane-v-ethiopia>; last accessed 3 July 2019.

D. **ABOUT FINSPY**

FinSpy is highly developed spyware which, according to the company's own description on its website, is sold exclusively to governments for the purposes of strategic intelligence and criminal prosecution,

Corporate profile on finfisher.com; last accessed 2 July 2019.

The malware is manufactured and distributed by the FinFisher company group; Elaman GmbH is also involved in distribution. FinSpy is operated in connection with servers to which the data gathered are sent. Normally, these servers cannot be configured and operated without the involvement of the manufacturer. Once FinSpy malware has been installed on an affected person's mobile end-user device, FinSpy enables the customer to covertly access telephone and VoIP calls, data infrastructures, screenshots and other photos, GPS data, microphones, connection data, as well as various applications, including WhatsApp, Line, Viber, Telegram, Skype, Facebook Messenger, Kakao, and WeChat,

Report 'Alert: FinFisher changes tactics to hook critics', 14 May 2018, Gustaf Björkstén and Lucie Krahulcova for Access Now (hereinafter: 'AN Report'), pp. 8 ff., <https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf>; <https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/>, last accessed 4 July 2019.

FinSpy is particularly effective as it remains practically invisible to the untrained eye: after it is activated for the first time, FinSpy deletes the symbol from the smartphone's main menu. The previously known versions of FinSpy were activated when the system was started without the user noticing,

AN Report, p. 8.

E. THE FACTS AND CIRCUMSTANCES

I. FINSPY ON THE FAKE ADALET WEBSITE

Turkey has become the country in the world with the most incarcerated journalists in relation to the population. At present, at least 34 journalists are political prisoners. Hundreds of newspapers and other media outlets have been closed down. Following the failed coup attempt of 15 July 2016, more than 50,000 people were arrested; more than 140,000 people were removed from their jobs,

<https://www.tagesschau.de/ausland/putsch-tuerkei-143.html>,
<https://www.reporter-ohne-grenzen.de/tuerkei/>, last accessed
27 June 2019.

In June and July 2017, the members of the Turkish opposition who were not yet incarcerated or in exile took to the streets over a period of three weeks in a 'March for Justice' to protest against the authoritarian reaction of the government following the failed coup attempt of July 2016. Social media have globally, and also in Turkey, developed to become an important means of communication for activists, human rights defenders, and political dissidents because of their openness, their reach, and the opportunity for protected communication. Accordingly, intruding into social networks and electronic communications is attractive for authoritarian governments. The malware which is the subject of the present proceedings was offered for download under false pretences on a website whose contents addressed the participants of the 'March for Justice' (the so-called Adalet March). This website was a fake campaign website of the Adalet March. Messages from multiple fake Twitter accounts that mostly communicated with the Twitter profiles of the opposition Republican People's Party (Cumhuriyet Halk Partisi, CHP) made the target group of the attack aware of the fake Adalet website.

The fake Adalet website with the domain adaleticiniryuru.com was registered on 29 June 2017. The next day, the malware which is the subject of this criminal complaint (hereinafter: A-Malware), was uploaded to this website. The fake Adalet website had the IP address 178.32.124.175. This IP address was operated by a shared hosting service which sells storage space to customers. Since exclusively Turkish websites were accessible through this IP address, it is logical that the shared hosting service makes services available to customers in Turkey. For this reason, it is logical that the website was not launched from another country, but from within Turkey itself,

AN Report, p. 5.



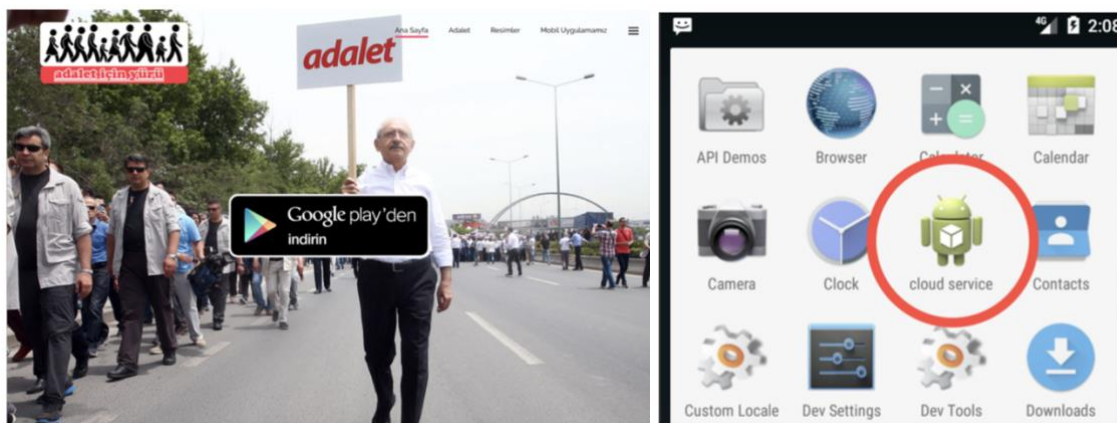
Screenshot of the Twitter profiles recommending the fake Adalet website.

The fake Adalet website did not provide an actual service to website visitors, but only advertised installing an Android application on their mobile devices. As is also common in the case of legitimate applications, this Android application was offered for download via what was apparently a centrally placed Google Play link. The Tweets and the website themselves implied that the software with the file name 'KatilBizeV1.0.apk' (translated from the Turkish: 'Join us!') made a cloud and calendar service available for networking purposes among the Turkish opposition.

Following installation, the application which is the subject of the present proceedings appeared on the users' home screens and was shown as a 'cloud service', paired with an Android symbol inspiring trust. However, instead of offering the Turkish opposition cloud services for organisation, the application was a disguised malware agent. According to documented experiences with FinSpy operations in other countries, this corresponds to the typical behaviour and the standard configuration of FinSpy.

Once the user attempted to open the application, or when the device was restarted for the first time after the download, the alleged Android Cloud symbol removed itself from the home screen. The malware became invisible to the user,

AN Report, p. 5.



Left: Screenshot of the fake Adalet website. The FinSpy malware was downloaded via the Google Play Link located in the middle of the image, which looks deceptively real. Right: This is how the FinSpy malware was displayed in the affected people's smartphone menus. The malware was displayed as a 'cloud service'.

The fake Adalet website was taken offline a short time after the publication of the AN Report. The website is archived online and can be accessed in its complete version of that time; the malware file which is the subject of this criminal complaint can be downloaded there to this day,

archive.org using the search term 'adaleticinyuru.com'; last accessed 29 June 2019.

Once the malware was installed on the mobile end-user device, it could take up its surveillance functions.

They include access to address book information, calendar and telephone call logs, file systems, screenshots and other photos, geolocation, covert eavesdropping of the spoken word through activation of the device's internal microphone, so-called 'spycalls' (concealed calls to enable microphone surveillance), collection of communication and media files as well as data from messengers such as Line, WhatsApp, Viber, Telegram, Skype, Facebook Messenger, Kakao, and WeChat,

AN Report, p. 13.

II. ATTRIBUTION TO FINFISHER

1. FORENSIC ANALYSIS OF THE MALWARE

On the basis of extensive forensic analyses of the A-Malware and comparisons with older known versions of FinSpy, computer scientists of the non-governmental organisation 'Access Now' have established that, with a probability bordering on certainty, this must be FinSpy because of striking similarities of the source code and the metadata. The available source code samples were compared. FinSpy's complete source code cannot be taken from the software; to this day, it is known only to its manufacturer. The FinSpy source code sample that was used for comparison originated from a data leak in the year 2014,

cf. <https://www.pnfsoftware.com/blog/finfisher-finspy-mobile-app-for-android-decompiled/>; <https://netzpolitik.org/2014/gamma-finisher-hacked-40-gb-of-internal-documents-and-source-code-of-government-malware-published/>, last accessed 3 July 2019.

The following findings of the forensic malware analysis clearly indicate that the A-Malware available for download from the fake Adalet website is identical to FinSpy. An extensive technical analysis can be taken from the Technical Appendix,

cf. Technical Appendix, Annex 1.

- **Identical source codes:** The configuration options of the two pieces of malware – that is, those parts of the source code that determine exactly how the file operates, which pieces of information are concealed to the user of the end-user device affected, etc. – are extremely similar to one another. In parts, their source codes are even completely identical. Individual functions, for example the programme code for the surveillance of telephone calls, are identical word for word (see Technical Appendix, Part 1).
- **Linguistic clues in the source code:** Linguistic clues in the source code of the A-Malware are also remarkable. For example, German words such as 'einstellung.html' ('preference.html') are to be found multiple times in the source code, a phenomenon which is rather unusual in the internationalised programmers' scene. What is even more unambiguous, are references to FinFisher by name. For example, unambiguous text fragments such as 'FIN_GIFT' are to be found in certain comments (see Technical Appendix, Part 2).
- **Further development in accordance with strategic goals:** Those differences that exist between the source codes of the A-Malware and older versions of FinSpy correspond to the strategy of improving secrecy and obfuscation pursued by FinFisher since the first leaks. The change serves specifically to remedy those problems that could have led to the leak at the time,

AN Report, p. 9, the findings of the computer scientists of ‘Access Now’ were technically verified by an independent expert team from ‘Cure53’, a German IT security company, cf. Annex V. More precise forensic analyses can be taken from the Technical Appendix in Annex 1 and, if required, can be reviewed by experts using the software samples in Annex 2.

2. FURTHER EVIDENCE

In addition, further evidence indicates that FinSpy was exported to Turkey:

- **FinSpy found by Microsoft:** In its Security Intelligence Report for January through June 2016 (Vol. 21), Microsoft reported that many Microsoft users were affected by malware through a systematic vulnerability in the operating system. Microsoft unequivocally identified the malware as FinSpy. 84 % of the affected users came from Turkey (see Technical Appendix, Part 3),

Microsoft Security Intelligence Report, Volume 21, January through June 2016, pp. 22-29.

- **Additional FinSpy malware in Turkey:** Access Now also found additional FinSpy activity in Turkey besides the A-Malware. The 2018 Access Now Report on which this criminal complaint is based found another malware copy on VirusTotal, an online virus scanner tool operated by Google, which VirusTotal identified as FinSpy (hereinafter: B-Malware). This B-Malware is distinguished by clear similarities to the A-Malware (see Technical Appendix, Part 4).
- **Additional FinSpy malware in Libya:** Malware was also uploaded to VirusTotal from Libya; this malware was clearly identified as FinSpy by VirusTotal. This malware is also very similar to the A-Malware, the B-Malware, and FinSpy. Since non-commercial actors are generally not able to distribute absolutely uniform malware to the most varied places on Earth, this circumstance also indicates that a professional manufacturer is behind the malware found (see Technical Appendix, Part 5).

These indications paint a clear picture: in Turkey as well as other places outside the European Union, uniform malware appeared during a limited period of time whose source code most closely corresponds to the previous finds of FinSpy malware. This can only be an exported version of FinSpy. For it is not only highly unlikely that a non-commercial actor would have the resources and expertise to produce malware of a quality like that of FinSpy – the complete source code of FinSpy has never been passed on or stolen (‘leaked’) outside the manufacturing firm – and to then successfully distribute it worldwide. Such a course of action would also be pointless. It would be significantly more efficient for any criminal actor aiming to produce effective spyware to simply design it from the beginning instead of reproducing a highly complex industrial product step by step.

III. TIME OF EXPORT OF THE SOFTWARE

In the forensic analysis, various characteristics of the A-Malware provide evidence for the fact that it was created between September and October 2016, that is, after the introduction of the licensing requirements into the Dual-Use Regulation effective 1 January 2015 and the AWV effective 18 July 2015.

The first indication is in the file 'build-data.properties', which can be reviewed by simply extracting the original file. This file contains metadata for compiling the Android application, in particular a library it uses called 'GMScore'. It can be taken from there that the system component 'GMScore' from the A-Malware cannot have been created before 23 September 2016.

```
build.time=Fri Sep 23 14\:39\:54 2016 (1474666794)
```

Although it is possible to change key metadata of the basic components of the malware with enormous technical effort, this would not provide any operative advantage to the developer. Instead, it would cause considerable confusion for the further development of the software if these components could no longer be assigned to specific times.

In addition, in the file component 'META-INF/MANIFEST.MF', there is a reference to a piece of Android development software called 'Gradle', version 2.2.1, with which Android programmes can be created.

```
Manifest-Version: 1.0  
Built-By: Generated-by-ADT  
Created-By: Android Gradle 2.2.1
```

However, version 2.2.1 was published only in September 2016, so that the FinFisher Trojan cannot have been developed before then,

<https://developer.android.com/studio/releases/gradle-plugin>; last
accessed 4 July 2019.

In addition, the digital signature of the A-Malware was created only on 10 October 2016, according to the information it contains:

```
Owner: CN=RMS
Issuer: CN=RMS
Serial number: 36891ece
Valid from: Mon Oct 10 05:17:01 CEST 2016 until: Fri Oct 04 05:17:01 CEST
2041
Certificate fingerprints:
    SHA1: 98:5D:08:CD:5F:1B:B3:30:28:CA:C6:20:AE:D1:93:2D:DD:26:91:E1
    SHA256:
1E:62:1A:88:3B:CD:9D:1B:D6:D5:61:11:C4:88:EE:10:D4:67:1D:2C:A6:64:F7:27:FE:
72:59:47:8A:68:79:67
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Thus the A-Malware cannot have been exported for the first time before October 2016,

cf. Technical Appendix, Part 6.

The B-Malware described under II. 2. also indicates that FinSpy was delivered to the Turkish government well beyond October 2016. The VirusTotal analysis shows that the B-Malware was created on 18 July 2017 and uploaded to the VirusTotal website on 21 July 2017. This means that FinSpy versions were exported to Turkey at least until July 2017,

cf. Technical Appendix, Part 4.

IV. LACK OF EXPORT LICENCE

Neither FinFisher GmbH nor Elaman GmbH nor FinFisher Labs GmbH received a licence to export the software to Turkey or any other country outside Europe. The federal government responded to a parliamentary question as well as multiple written questions regarding the facts and circumstances described above that it had not issued, to any companies, any export licences for intrusion software such as FinSpy since introduction of the licensing requirement for the export of software in the year 2015. Concerning criminal investigations, the government referred to the public prosecutor's offices responsible both in terms of the subject matter and in terms of location,

Bundestag document 19/3334, pp. 5ff.; Bundestag document 19/2419, p. 34; confirmed in Bundestag document 19/2610, p. 38; confirmed in Bundestag document 19/3384, p. 56.

The federal government confirmed most recently on 19 June 2019 that although it had issued export licences in 13 cases for telecommunications surveillance

technology and in 15 cases for surveillance centre equipment, it explicitly pointed out that it had never issued an export licence for 'intrusion software' (within the meaning of 4D004, List of Dual-Use Items, Dual-Use Regulation),

Response of Claudia Dörr-Voß, State Secretary in the Federal Ministry for Economic Affairs and Energy, of 19 June 2019 to the written questions from FDP parliamentarian Gyde Jensen, p. 1.

FinSpy is intrusion software in this sense.

F. LEGAL ASSESSMENT

Hence, the suspicion exists that the suspects made themselves liable to prosecution under section 18 para. 2 no. 1 and section 18 para. 5 no. 1 Foreign Trade and Payments Act (AWG) by exporting FinSpy to Turkey between October 2016 and June 2017 without the required licence.

At the time of export, exporting FinSpy required a licence (see I). The suspects exported FinSpy without having the required licence (see II). As far as can be established, this is an intentionally committed crime (see III), the crime is not time-barred (see IV).

I. LICENSING REQUIREMENT FOR EXPORTING FINSPY

At the time of export, exporting FinSpy required a licence. The licensing requirement results both from section 8 para. 1 no. 2 Foreign Trade and Payments Ordinance (AWV) in conjunction with Part I Chapter B, Code 5D902 a) in conjunction with 5A902 of the Export List (1.) and from Art. 3 para. 1 in conjunction with Annex I Code 4A005 of the Dual-Use Regulation (2.).

1. LICENSING REQUIREMENT IN ACCORDANCE WITH SECTION 8 PARA. 1 NO. 2 AWV

In accordance with section 8 para. 1 no. 2 AWV in conjunction with Part I Chapter B, Code 5D902 a) in conjunction with 5A902 of the Export List, the export of software that serves to establish surveillance systems for communication and information technology requires a licence. FinSpy is software that serves to establish surveillance systems for communication and information technology. FinSpy enables covert access to telephone and VoIP calls, data systems, screenshots and other photos, location data, the microphones and connection data of the mobile phones of the persons affected, as well as to various applications. In this way, many and diverse confidential telecommunications data of the persons affected can be intercepted by the infiltration software,

cf. Section E. I.

FinSpy is not included in the derogations formulated in the General Software Note (GSN) preceding the Export List as it is neither freely available nor generally accessible within the meaning of the legal definitions of the definitions of terms. Should the A-Malware be considered merely maintenance or an update of an earlier version of FinSpy, this too would be subject to the licensing requirement, since in accordance with Part I Chapter B, Code 5D902 of the Export List, the delivery of software for purposes of ‘use’ of surveillance facilities within the meaning of 5D902 also includes maintenance services. In the definition of terms of the Export List, ‘use’ is defined as ‘operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.’

The licensing requirement has existed since 18 July 2015, and therefore also existed at the presumed time of export between October 2016 and June 2017,

4th Regulation amending the AWV of 13 July 2015, Federal Gazette AT
17 July 2015 V1.

There are no transitional provisions. Even potentially existing contractual obligations entered into before 18 July 2015 and potentially including future updates or maintenance would not preclude the licensing requirement. Section 1 para. 1 AWV differentiates between legal transactions requiring a licence and actions requiring a licence. In section 2 para. 3 AWG, export is legally defined exclusively as an actual action.

2. LICENSING REQUIREMENT IN ACCORDANCE WITH THE DUAL-USE REGULATION

The licensing requirement on the basis of the Dual-Use Regulation results from Art. 3 para. 1 in conjunction with Annex I Code 4A005. On the basis of the above-mentioned comprehensive surveillance functions, FinSpy is ‘intrusion software’ which, within the meaning of the legal definition, was ‘specially designed or modified to avoid detection by “monitoring tools”, or to defeat “protective countermeasures”, of a computer or network-capable device and performing ... [t]he extraction of data or information, from a computer or network-capable device, or the modification of system or user data’.

The licensing requirement for intrusion software in the Dual-Use Regulation already existed at the presumed time of export between October 2016 and June 2017, for it was introduced into the Dual-Use Regulation through the Commission Delegated Regulation (EU) No. 1382/2014 effective 1 January 2015. There are no transitional provisions,

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1382>; last accessed 2 July 2019.

II. EXPORT WITHOUT THE REQUIRED LICENCE

The suspects exported FinSpy to Turkey presumably between October 2016 and June 2017. The export of software is legally defined in section 2 para. 3 no. 2 AWG as the transmission of software and technology from Germany to a third country including making it available by electronic means to natural and legal persons in third countries. In Art. 2 no. 2 iii, the Dual-Use Regulation defines export as the ‘transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone’.

As described in Section E, numerous pieces of evidence are available for the use of FinSpy by a Turkish customer. The A-Malware, which was found on the fake Adalet website is, with a probability bordering on certainty, the FinSpy malware as it is produced and distributed by the suspects,

cf. Section E. II.

An analysis of the software shows that the A-Malware was created at the earliest in October 2016,

cf. Section E. III.

There are many indications that the development and distribution of FinSpy and other FinFisher products take place in Munich. In particular, FinSpy is no longer produced and distributed in England. In the OECD proceedings against Gamma International UK LTD before the UK National Contact Point for the OECD Guidelines for Multinational Enterprises (reference number BIS/15/93), in which the British Contact Point determined infractions by Gamma International UK LTD against the OECD Guidelines for Multinational Enterprises, the company representative of Gamma pointed out that exports of FinFisher products from Great Britain had been terminated in April 2012,

‘Gamma has declined to tell the UK NCP whether any supply was made (for customer confidentiality reasons), but has told the UK NCP that Gamma International UK Limited ceased any exports of Finfisher software in April 2012 and soon after that (around July 2012) ceased any exports of hardware components of the system (some components continued to be shipped to Germany later in 2012 but not as exports)’, UK National Contact Point for the OECD Guidelines for Multinational Enterprises: Privacy International & Gamma International UK Ltd: Final statement after examination of complaint, December 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf, last accessed 27 June 2019.

FinFisher Labs GmbH, with headquarters in Munich, replaced Gamma International GmbH with its entry into the Commercial Register of 26 September 2013. FinFisher GmbH, with headquarters in Munich, replaced Gamma International Sales GmbH with its entry into the Commercial Register of 13 October 2013. Finfisher Limited, with headquarters in Winchester, Hampshire, United Kingdom, was closed on 24 February 2014,

cf. <https://beta.companieshouse.gov.uk/company/07346435>, last accessed 27 June 2019.

According to the information in the Commercial Register, Elaman GmbH, FinFisher GmbH, and FinFisher Labs GmbH are concerned with trade and distribution of software products connected to the current subject. None of the three companies had a licence for export after January 2015,

Bundestag document 19/3334, pp. 5 ff.; Bundestag document 19/2419, p. 34; confirmed in Bundestag document 19/2610, p. 38; confirmed in Bundestag document 19/3384, p. 56.

III. **THE SUSPECTS' CRIMINAL RESPONSIBILITY**

The suspects made themselves liable to prosecution under section 18 para. 2 no. 1 and section 18 para. 5 no. 1 AWG by exporting FinSpy between October 2016 and June 2017 without the required licence. The facts and circumstances suggest that the suspects intentionally violated the export provisions (and did not merely commit an administrative offence in accordance with section 19 para. 1 AWG).

During the period in question, the suspects were CEOs of Elaman GmbH, FinFisher Labs GmbH, and FinFisher GmbH. Since the companies distribute only to a limited circle of customers, namely governments and government-related organisations, there is no doubt that they must be aware of all ongoing supply relationships with foreign governments – in this case, with Turkey. The companies are neither so large nor is the number of potential FinSpy customers so high that it would suggest itself to decide about and carry out exports without the knowledge of the CEOs. The fact that the federal government, according to the information it gave on 19 June 2019, has not issued an export licence for intrusion software requiring a licence since January 2015 additionally either suggests that the export of such software is not routine business, which would support all the more that the CEOs knew about it, or that numerous additional exports violating the export provisions have taken place in recent years, above and beyond the business deals with Turkey.

The suspicion is also directed against those responsible at the executive levels within the companies; they cannot be mentioned here by name due to a lack of knowledge about the companies' structures.

IV. **ABOUT THE STATUTE OF LIMITATIONS**

Since it suggests itself that the suspects delivered FinSpy to Turkey until July 2017,

cf. Annex 1, Part 4,

criminal liability in accordance with section 18 para. 2 no. 1 and section 18 para. 5 no. 1 AWG does not become time-barred before July 2022, section 78 para. 3 no. 4 Criminal Code.

G. **POTENTIAL INVESTIGATIVE MEASURES**

We encourage further clarification of the facts and circumstances by means of the following investigative measures:

Interviews of the following expert witnesses:

- Gustaf Björkstén, Chief Technologist, Access Now, gustaf@accessnow.org

Witness Björkstén is a co-author of the Access Now study and will testify as to the validity of the technical analysis.

- Dr.-Ing. Mario Heiderich, Cure53, Bielefelder Str. 14, D-10709 Berlin

Witness Heiderich works for the IT company Cure53 and reviewed the validity of the statements of the Access Now study, cf. Annex 6.

- Matt Miller; Microsoft Security Response Center

Witness Miller is a co-author of the Microsoft Security Intelligence Reports, Volume 21. The witness will confirm the correctness of the statements made in this report concerning finding FinSpy in Turkey.

Searches and seizures:

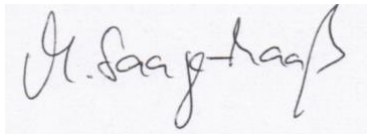
Search of the premises of the aforementioned companies in Munich and seizure of documents and data carriers, securing

- copies of the FinSpy malware; it is anticipated that it will be possible to find copies that are identical to the A-Software which is the subject of the present proceedings,
- customer correspondence with the Turkish government or other relevant actors as well as internal correspondence that gives information about the actions and the knowledge of the suspects and additional employees of the companies,
- other documents indicative of the facts and circumstances described above, particularly of the income from unlicensed exports, which should be relevant concerning confiscation of assets generated through them.

Yours faithfully,



Ulf Buermeyer, Chair of Gesellschaft für Freiheitsrechte e.V.



Miriam Saage-Maaß, Vice Legal Director of the European Center for Constitutional and Human Rights



Christian Mihr, Executive Director, Reporter ohne Grenzen

Andre Meister, Netzpolitik.org

H. **ANNEXES**

1. Technical Appendix

2. USB stick with

- a sample of the A-Malware
- a sample of the B-Malware
- a sample of the FinSpy malware 2014
- a digital version of the criminal complaint and the annexes

3. Relevant excerpts from the Commercial Register

4. Hard copy of the Access Now report: FinFisher changes tactics to hook critics, May 2018

5. Hard copy of the Microsoft Security Report, pages 22-29

6. Hard copy of the review of the statements of the Access Now report conducted by the IT company Cure53, March 2018