European Parliament
2019-2024

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

27.10.2022

MISSION REPORT

following the PEGA committee delegation to Israel, 18-20 July 2022

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Members of the mission:

Jeroen Lenaers	(PPE) (Leader of the mission)
Diana Riba i Giner	(Verts/ALE)
Juan Ignacio Zoido Álvarez	(PPE)
Gilles Lebreton	(ID)
Sophia in 't Veld	(Renew)
Hannes Heide	(S&D)
Dragoş Tudorache	(Renew)
Lars Patrick Berg	(ECR)
Anne-Sophie Pelletier	(The Left)

Introduction

The aim established for the delegation to Israel was to gather information and facts, both as regards private companies that produce and sell the main spywares (notably “Pegasus”) and from public authorities that deliver licenses and exercise control over their use, in order to better understand the nature and the functioning of the matter.
The information gathered during this delegation, for instance as regards the technical and legal framework of the use of these spywares, will be essential for the effectiveness and relevance of the work of the PEGA Committee.

Summary account of meetings

I. MEETINGS ON TUESDAY 19 JULY

Meeting with Ministry for Foreign Affairs:

The EP delegation was received by the following representatives of the Israeli Ministry of Foreign Affairs (MFA):

- Ms **Michal Weiler-Tal**, Director for export control matters
- Mr **Assaf Moran**, Director for the Department for European Multilateral Organisations and NATO

The meeting was held under the *Chatham House Rules*.

The PEGA Committee raised the concerns that no representative of the Ministry of Defence was present as they were the principally responsible for defence export control. MFA stated that they would give a full and complete picture of the Israeli export.

MFA continued by describing the Israeli export control system for cyber capabilities, such as spyware. The first regulation that applies to such capabilities came into force in 2010 and, though Israel is not a party, it follows largely the Wasenaar Arrangement. It is a two-phases system, where a company would first need a marketing license to start negotiations for a sale and subsequently an export license if a deal is made. The total amount of licences per year is 30-40 000 for all defence products (no specific figure for cyber capabilities was give), however, as not all negotiations lead to a deal, the number of marketing licenses are much higher than the final number of export licenses. The MFA has to approve every marketing and export license. In the MFA, there are five persons working on defence export control. Requests for a license are assessed on the basis of a number of criteria, including human rights.

Cyber capabilities may only be exported to government, and only for the purpose of crime and terrorism prevention. The MFA declined to answer how many requests were refused per

year and said that they had no knowledge about any Pegasus licenses being terminated.

If a defence company acts in contravention of any license given, it may be given a fine. The use of commercial intermediaries, such as brokers, is standard practice and would not violate the terms of the export license as long as the party to the end-user agreement is a state entity.

MFA further stated that a process to make the rules for export of cyber capabilities stricter was initiated in the autumn of 2021. As a first step, the End-User Declaration that client countries have to sign was redefined. The new rules apply to new export licenses while existing licenses are subject to the old rules[1]. The End-User Declaration sets out definitions of serious crimes and terrorism. The MFA did not specify what further steps to which this process would lead.

MFA also stated that the EU Member States are viewed as countries with the highest respect for human rights and that no differentiation is made between EU MS with respect to defence export control. Israel is aware of discussions of whether all MS uphold human rights to the necessary degree but views that as an internal matter for the EU. Nevertheless, the assessment of a specific request is done upon the information available regarding the specific country.

As regards systems as Pegasus, the Israeli government has no access to any data collected. The MFA does not have the technical capabilities to assess cyber systems from a technical point of view.

As regards abuse of exported systems, MFA said that indications of such abuse would be taken into account in subsequent requests for export licenses but that it would not lead to any revocation of a given license[2]. The MFA presupposes in their assessment of an application for an export license that cyber capabilities will be used in accordance with the undertaking in the End-User Declaration while no active follow-up whether this is the case is carried out. The sale of cyber capabilities is based on trust between countries, and Israeli authorities would only act upon 'official' proof of abuse.

As regards statistics on how many terrorist events or serious crimes the use of cyber capabilities had helped to prevent, MFA stated that they did not have such statistics, but that they thought that Europol should have it as regards the EU.

[1] (Please see here MoD press release: https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021. Please see also for instance: https://www.reuters.com/technology/israel-issues-stricter-guidelines-use-its-cyber-tech-exports-2021-12-06/)

[2] Please note that the MoD press release mentioned above states that the declaration 'explicitly specifics the possible sanctions in the event of non-compliance with the obligations set forth in the declaration (including restricting the use of the cyber system or shutting down the system)'.

Meeting at the Knesset with MoK Mossi Raz:

The delegation has been then received at the Knesset by MoK **Mossi Raz**.

Mr Raz introduced the meeting saying that a lot of laws and rules in Israel control spywares and weapons sales. Israeli Government tries to determine which countries are qualified to establish this kind of commercial relationship, and those which are banned for human rights issues.

Mr **Lenaers** asked about the role of the Israeli parliament and its possible surveillance activity.

Mr Raz explained that the topic of "spywares" had not been debated in the Knesset before last November : the topic met the interest of the national public opinion when, and only when, it was revealed that Israeli citizens were also targeted. For the rest – especially for what NSO sells or runs outside Israel – he said that there was no debate in the country, where the osmosis between the cybersecurity companies and the authorities of Defence and National Security is not challenged. The majority of the Knesset agrees on the use of the system by the police which is using it in compliance with Israeli law, especially within the occupied territories.

The rapporteur **In't'Veld** queried Mr Raz regarding the export licenses process to Member States, asking again if there was any parliamentary scrutiny, and if - because of the latest developments of the file - the number of MS beneficiaries has been reduced.

Mr Raz answered that any modification on licenses is not a government decision but of MAE and MOD without parliamentary control. Members of Knesset had a debate after revelations raised at EU level but it did not lead to anything.

Mr **Zoïdo** pointed out that the strenghtening of standards followed the revelations about Pegasus. He asked if there was since any sunset clause for the licenses and if there was any political will within the Knesset to establish it.

Mr Raz said that sadly, while there is a consensus on the defence of Human Rights in the Knesset, it has to be understood as fundamental rights for Israeli citizens.

Mr **Heide** asked if Mr Raz which EU MS were concerned.

Mr Raz responded that this was not a relevant political question in Israel: nobody really cares. He agreed on the fact that Israel has not only a commercial responsibility when selling spyware.

Mr **Tudorache** came back on the question of establishing checks and balance; and on the possibility of opening a wide debate after the incoming election.

Mr Raz reiterated that they observe some interest only when Israeli citizens are concerned. So far there is no debate, because the general opinion is that only very few people are affected. But the political party he represents would like to redefine the legal framework.

Ms **Riba i Giner** underlined that with NSO we were talking about a private entity whose activity is clear. But the Government is delivering licences: did any meeting happen with it? Is there any transparency between Israeli government and parliament? Will you try again to set up an inquiry committee?

Mr Raz answered that all that referring to Security and Defence, there is no real debate. The work of the special committee did not provide the Knesset with any concrete result. He added that in Israel the Ministry of Defence prevails over Ministry of Foreign Affairs since 1948.

Mr **Lebreton** said that there is a huge contrast between the power of Knesset to control the domestic dimension, but not once outside the country. Could the Committee of Defence carry out this duty of surveillance and control ?

Mr Raz said that this control is made through a secret committee, and he stated that this control is not really effective. In other words, the Ministry of Defence does what they want without boundaries.

Mr **Berg** queried whether the “national security” dimension of these spywares could be invoked when they are sold to countries like Azerbaijan, without even mentioning the human rights situation in this country.

Mr Raz admitted that he is not a military expert, neither expert of all countries of the world, and therefore has no comment on the situation in Azerbaijan.

Meeting with Mr Gabi Siboni:

Later on, the delegation received Mr **Gabi Siboni**, Director of the Military and Strategic Affairs Programme and the Cyber Security Program at the Institute for National Security Studies.

Mr Siboni had been suggested by the EU delegation to Israel and also contacted by them. When he arrived, he did not know that the PEGA Members were interested in cyber capabilities and spyware, and he seemed surprised at this. He propagated a total deregulation - Israeli companies should be allowed to sell spyware to whomever they wanted.

Meeting with Academics:

Immediately following this meeting, the delegation received, in presence of the EU Head of Mission in Israel, Mr **Dimiter Tzantchev**, four academics :

- Dr. **Tchilla Shwartz Altshuler** from the Israel Democracy Institute,
- Professor **Anat Ben David**, expert on digital rights and surveillance at the Open University and founder of "*Privacy Israel*",
- Dr. **Natalie Davidson Buchmann** from the Faculty of Law Tel Aviv University,
- Dr. **Tamar Megiddo**, researcher.

There was agreement amongst the speakers that the area of cyber intelligence needs to be regulated. The speakers had different opinions regarding the area, some advocating for a ban or a moratorium (general or temporary ban), some looking more into ways of regulation, as a ban could be ineffective (it will be used anyways)

One of the speakers mentioned the importance of defining what needs to be regulated: currently we speak of spyware on phones and laptops, but the area is a lot broader and the future will bring other similar tools that can infringe privacy and data protection in similar ways. The speaker used the word cyber intelligence or "remotely hacking devices" instead of spyware, as we should not focus on the technology itself but on the methodology used and its outcome. It is not comparable to regular wiretapping.

The use of these tools against human rights activists, journalists and politicians is clearly illegal and needs to be regulated nationally and internationally. Updating the Wassenaar arrangement was mentioned several times in this regard (spyware as dual-use item). When international/European regulation shall be drafted, this should happen through a public debate, with a maximum of transparency. There is a need of a tool to assist victims, as well as stronger import restrictions and restrictions regarding the trade in vulnerabilities, among others. Regulate spyware as if it were unconventional weapons.

One of the speakers spoke about the cycle of normality and warned against the normalisation of the use of such spyware (it started in very restricted terms by very few actors and has now expanded to many State entities).

The speakers confirmed that there was very little debate in Israel about the use of spyware in third countries, but it got media attention when it became public that spyware was also being used to target Israeli citizens (https://www.washingtonpost.com/world/2022/01/26/nso-israel-spyware-pegasus/ "swordtail scandal").

There was a discussion about the new export licence regime by the Israeli government: the licences are not public, also the list of countries is not made public by the defence ministry. It is unclear if the new regime regards export or marketing licences. It is unclear if the new regime is actually enforced or merely a PR stunt to improve relations with the US.

I. MEETINGS ON WEDNESDAY 20 JULY

Meeting with Mr Shalev Hulio, CEO of NSO:

The mission of PEGA delegation ended with the meeting with **Shalev Hulio**, at that time CEO of NSO, and **Chaïm Geilfand,** chief compliance officer, at their headquarters in Tel-Aviv.

The meeting was held under the *Chatham House Rules*.

Four different categories of companies in the field of cyber capabilities were highlighted:

- companies working on a regulated market subject to export control , etc. (such as NSO),
- companies protected by regulation shelters without restrictions (Singapore for instance),
- “hackers for hire”, and
- state operators that provide cyber capabilities often in exchange of influence (Chinese and Russian tools).

Cyber capabilities is a very large and diverse industry with a lot of competition. There is a lack of transparency and of information. NSO is only one of many operators.

NSO presented its human rights and due diligence processes (see transparency report). They use data from Freedom House, among others. Investigations show are initiated following alerts from civil society/media. At current there is an ongoing investigation into the use in Spain. If NSO finds that there has been abuse they will terminate the contract of a state. To date, they have terminated the contracts of two Member States.

Manipulating content is not possible and not allowed technologically and by law. Pegasus is configured so that users cannot turn on the video, they can only use the microphone.

There have been 12000 installations per year worldwide, which is attempts in total; this is equivalent to around 4000 targeted phone numbers.

NSO does not operate the spyware systems. NSO cannot disclose former clients; the Israel MoD would have to give permission. The one to blame for abuse of spyware is the end-user, not the company developing it.

Conclusion

Despite the lack of availability of the Israeli national authorities at the highest level the mission gave the opportunity to engage very enlightening exchanges of views with the various interlocutors, and to get a more precise idea of the processing of sales of spywares.