# The Spyware that can control your Phone | Interview with Dr. Shir Hever

*This transcript may not be 100% accurate due to audio quality or other factors.*

**Zain Raza (ZR):** Thank you guys for tuning in today and welcome to another episode of The Source. Welcome to part two with Dr. Shir Hever and we will continue our discussion. So if you haven't watched part one where we talked about the uprising in the West Bank, make sure to check it out. And today, we will focus on the Pegasus spyware software. Dr. Shir Hever, thank you so much for your time.

**Shir Hever (SH):** Thank you very much for having me.

**ZR:** Can you first explain to our viewers, what is this Pegasus spyware software?

**SH:** Yeah. So Pegasus is just one of the programmes made by a company called NSO Group. There are about six Israeli spyware companies that produce different kinds of software which have the ability to hack into phones and computers. Now, the spyware is a new kind of technology, which was developed by Israeli graduates of a specific intelligence unit, signal intelligence unit, called 8200. And this unit hacked people's phones and spied on them, surveillanced them, on all Palestinians, in order to blackmail them with information that they collect from them and turn them into collaborators. And some members of this unit have been shocked and disgusted by what the unit was doing, and they exposed the way that the unit operates. But the vast majority of these officers think that it's absolutely fine to violate people's privacy and to blackmail them into becoming collaborators. And then they also thought that it's a great way to become rich. And so they took this technology that was used by the Israeli signals intelligence unit and turned it into a product that is sold around the world. According to Amnesty International, Forbidden Stories and Citizen Lab, they published a very comprehensive report last July, they identified 45 countries where this software has been purchased and used against lawyers, against human rights activists, against

politicians, against just civilians. So it's not a military tool, but it's actually a tool against civilians, against civil society and against human rights.

**ZR:** This it's the same software that was used to locate Jamal Khashoggi and to find out more about the activities that he was having and who he was corresponding with, that the Saudi monarchy basically used to hack his phone. Is that the same one, right?

**SH:** It is the same one, although the Pegasus programme has different iterations. The one that was used against Jamal Khashoggi in 2018 is an older version of what is now available on the market. And one of the very disturbing ways that this programme develops is that it allows hacking remotely into devices without the person who has the device has any way of knowing that the device was hacked. So your phone, my phone, everyone, we might be hacked already. We can't know this without actually sending the phone to be forensically analysed by Citizen Lab or a similar organisation, and even then they will only be able to say if it was hacked or not. And what is very disturbing about this situation is that his phone was not hacked, but rather the phone of somebody he corresponded with. He corresponded with a human rights activist in Canada, and the phone in Canada was the one that was hacked. And so the conversations with Jamal Khashoggi were exposed to the Saudi government and the Saudi government then decided that they don't like what Jamal Khashoggi was saying. And they, well in all likelihood, although it has not been proven in court, but I think everyone can see that there is a very high likelihood that Jamal Khashoggi was murdered in the Saudi consulate in Istanbul based on the information that the Israeli company has gathered for the Saudi government. This is how it works, which means that even if our phone is not hacked, we could be corresponding with somebody who's phone is hacked. And once again, our information gets to the wrong hands that this is extremely dangerous and of course, extremely illegal.

**ZR:** It reminds me of what Edward Snowden exposed of the NSA programmes that were actually supposed to surveil foreign targets, but when they were corresponding with Americans, they were able to intercept and expand that to a domestic level. Getting back to this software. Obviously, people here in Germany will ask, well, why does it concern me? What is Germany at the moment doing with Israel? Is it buying the software? Is it involved in any way? And second part of the question which you could address after that is most people would say, I have nothing to hide; the government can go and hack me. So how do you respond to that?

**SH:** Well, first of all, one branch of the German police, the German federal police, has bought Pegasus. They bought the software from NSO Group. And when this was exposed in the media and they were asked questions about this, what are you going to do with this programme and what are you spying on, they responded that they have no intention of using it. This is a very expensive software. So if they're telling the truth, they have wasted millions of euros. If they are lying, then they are spying on German citizens. This is very disturbing

and there needs to be an investigation. Right now there is an investigation conducted by the European Union Parliament. There is a committee of Parliament members who have also travelled to Israel in order to speak with members of the NSO group, to speak with victims of this software and to collect information. And there will be some kind of reckoning, some kind of accountability process within the European Union to those officials on trial for buying the espionage technology, which is normally used by organisations like the NSA that you mentioned for state to state espionage level, of military grade espionage. But here we're talking about a company, a private company that is taking state level espionage technology and also bringing it to the highest bidder. This is a very, very dangerous thing. But I want to address the more important issue, which is when people say, well, maybe this is a tool for law enforcement; the NSO Group themselves, they like to say we use it to stop terrorism, we use it to stop crime. First of all, there has not been even one documented case in which spyware has helped to solve crimes or to stop any kind of crime. And there's a good reason for this. Because the tool itself, technologically speaking, is simply not useful for law enforcement. Law enforcement is about transparency. It's about going through very clear procedures. And if you want to collect evidence that can be usable in court, then you need to have a process of collecting that evidence that can be retraced and observed by the courts. Otherwise, whatever evidence you collect is useless. That's exactly the point, because like I said before, when your phone is then analysed in a forensics lab, they can know that the phone was hacked, but they don't know when and they don't know by whom and they don't know what was done to the phone exactly. And this spyware allows somebody full control over a device, that means they can remotely activate the camera, the microphone, to listen to whatever is happening around the phone. They can also download data from the phone, but they can also write on the phone. They can write on your social media account using your account in a way that will make it seem like you wrote something that you didn't want to write. This gives a lot of power to the police or anyone who has access to the software. Basically, they could incriminate innocent people with fake evidence; there's no way to find out. And because there is no way to know when exactly they use this programme and what they wrote in the phone or the computer then this is not something that law enforcement can use. This is something that only works for two innings. For authoritarian regimes, that have no process of internal accountability. And if you look at who are the biggest customers of NSO Group and Pegasus, these are absolutely authoritarian regimes in countries which are not even close to democracies. We've spoken about Saudi Arabia, we should also mention the United Arab Emirates. We should mention Honduras. We should mention Uganda and Chad, Hungary and Belarus. These are places where Israeli spyware has been used against people. And, of course, Hong Kong, where the spyware technology was provided to the Chinese authorities in order to crush the freedom movement there.

**ZR:** Privacy is an issue that has taken a step back, in my opinion, after the big revelations that we had with Edward Snowden's and Glenn Greenwald's exposure of the NSA leaks. Then we had WikiLeaks always exposing documents, for example, Vault 7 of the CIA where they could use a Samsung TV to monitor you without the TV even being on. So how is this

situation in terms of civil liberties being viewed by Israeli society and media? And the second part of the question, has there been any international lash back on this?

**SH:** Within the Israeli society, it's a very complex issue because most Israelis believe that there's no way the Israeli intelligence organisations will use this kind of technology against Israeli citizens. Because we Israelis don't have to worry about these things. And then there was a very cleverly orchestrated exposé in the Israeli media which exposed that the Israeli police had actually used spyware to spy on Israeli citizens. But the journalist who exposed it was given intentionally false information and published fake evidence and fake testimonies as if the police was using this surveillance. This was a very, very smart operation. It was mainly used in order to try to undermine the credibility of some of the witnesses that were speaking against former Israeli Prime Minister Netanyahu, who is facing corruption charges. And so this exposé was used to say, Look, the prosecution is using Pegasus in order to plant evidence against Netanyahu. And that means that evidence against him has to be disregarded. And after Netanyahu made use of this in his trial, it later came out that the information was fake, was false; that journalists had to retract the accusation. Then everybody came under the false conclusion that that means that actually the spyware was never used against Israeli citizens. But that was a false conclusion. That was a very clever way of people, of just having a backlash and saying, Oh, so that report was fake, which means we are safe. No, actually later the Israeli police admitted in a much less reported document that, yes, they have been using this technology against protesters, against human rights activists within Israel, against Israeli citizens, absolutely. But the second part of your question was?

**ZR:** How is this viewed internationally? Has there been any condemnation from any countries? For example, the NSA revelations were pretty big and there was a big diplomatic fallout. How has the fallout been on this or has it just been accepted as a commodity on the market, which is fine to buy and sell?

**SH:** I think part of the problem is that people who are very much affected by this and furious about this- there are people who have been tortured in Bahrain and Morocco because the authorities used Pegasus to capture human rights activists, especially women's rights activists. And in Mexico, the investigation of the 43 disappeared students, which were actually murdered, and again, lawyers and human rights activists were targeted by Pegasus in order to silence them. This sort of justified fury against the use of a spyware, Israeli spyware, to silence human rights activism is distributed around the world. What we need is for people from all of these countries to work together and to provide the information that they have to make a global campaign to face a global problem. And President Macron of France his own phone was hacked by Israeli spyware. This looked like a moment in which maybe international backlash would have happened because the president of a powerful Western country has been hacked. The Israeli Minister of Defence flew to Paris to personally apologise to Macron and France dropped it, they just allowed it to continue to happen. And this is really a serious problem. We also see a problem with corporations. Two very large

corporations filed lawsuits against NSA Group. Apple, and Facebook. That's because their own devices, their own technology, Facebook, which is now called Meta, they also own WhatsApp, which has been hacked. And Apple phones, the iPhones were hacked by Pegasus. So they launched lawsuits against the company and the people said, Well, if the big corporations are on our side, we're going to win. But it's not so simple, unfortunately, because what they're doing is, they're dragging a very, very long trial. And in the meantime, Apple is already pushing a new set of products where they say we now have phones that are resistant to spyware, so pay double and we'll give you a product which is supposed to protect against spyware. But what they actually are doing, they're profiting from it. They are turning the threatened spyware into another source of profits. It creates demand for a new product and they're happy to provide that product. So they now have an interest that their lawsuit against NSO Group will never end. And so, once again, it's back on our shoulders as citizens of any country in the world, but we're speaking now in Germany, to put an end to this, to launch campaigns and to launch protests so that we make sure that we don't allow these corporations to profit from violating our privacy and human rights.

**ZR:** I think that's a good place to end. Let's hope our viewers will take some action and create awareness of this issue. Independent journalist, economist and author Shir Hever, thank you so much for joining us today.

**SH:** Thank you.

**ZR:** And thank you guys for tuning in today. Don't forget to subscribe to our YouTube channel and to donate so we can continue to produce independent, non-profit news and analysis. I'm your host, Zain Raza. See you guys next time.

**END**