SPECIAL INFILTRATION
By Paolo Mondani
With the contribution of Norma Ferrara and Guglielmo Mattioli
Video by Alessandro Spinnato
Edited by Giorgio Vallati

SIGFRIDO RANUCCI IN STUDIO
Having to pay a ransom following a cyber attack is nothing in comparison with what could happen - and in fact has already happened. About one hundred Italians have been illegally tracked and spied on by a government-authorised trojan. What has happened to that data? And who was behind those activities? What we do know is that in recent years espionage techniques have evolved in unimaginable ways. Malware and spyware has been utilised by governments to contrast organised crime and terrorism, but also against political opponents and reporters, ultimately degenerating into a sort of mass surveillance. They can infiltrate anything. Televisions, GPS navigators, and even alarm systems They can even break into what we consider must sacred, such as messaging apps like WhatsApp or Telegram, stealing our photos, our messages, our emotions and our very identity. And everybody's vulnerable. Because trojans, these little bastards, have been able to infect the craftiest criminals, the shrewdest judges, and even the accounts of former ECB presidents and prime ministers. Surveillance technologies gleaned the secrets of Giulio Regeni, the researcher killed in Egypt in circumstances yet to be clarified, and also of journalist Jamal Khashoggi, who was killed inside the Saudi consulate in Instanbul - killed and dismembered. Tonight's episode will mark a point of no return; it will forever change the way we look at the most ubiquitous and possibly most beloved item of our time. Our Paolo Modani reports.

PAOLO MONDANI VOICEOVER
When you have a secret that can't be shared with anyone, you can be sure that you will reveal it as soon as possible. And the first one to listen in will be your cell phone. Technology moves faster than laws and governments, and that void has been filled by trojans. It's a type of software used for spying criminals. But many countries use it against reporters, political opponents, or simply to make sure that things don't change. Trojans risk becoming the norm.

PAOLO MONDANI
Let's try infecting this cell phone with a trojan.

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
We're going to create our malware, which we will then use to infect the selected device.

PAOLO MONDANI
Let's open WhatsApp...

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
We'll use WhatsApp to send an image...

PAOLO MONDANI
An image to the person we want to infect. The image is...

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
...a cute little horse. Now, we got you!

PAOLO MONDANI
As soon as I tapped it, I was infected with the trojan. But can you send this malicious message, which conceals the trojan, as if the sender was...

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Someone else?

PAOLO MONDANI
Like a friend of mine?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Absolutely. Technically, now I am the phone.

PAOLO MONDANI
And what does this allow you to do?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Technically, anything I want.

PAOLO MONDANI
Such as?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
The only limit is what I set as a limit. For example, we can open the microphone and record any conversation we want. We need to say something...

PAOLO MONDANI
I'll use this Altan cartoon: two men, one says to the other: "Spies spy". And the other one replies: "That's crazy!"

PAOLO MONDANI FROM THE COMPUTER
Two men, one says to the other: "Spies spy". And the other one replies: "That's crazy!"

PAOLO MONDANI
Outstanding quality.

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Now try doing the same thing with your phone turned off.

PAOLO MONDANI
Another cartoon, this one by Sergio Staino. A woman in bed with Bobo: "Can you keep a secret?" And Bobo says: "No way!"

PAOLO MONDANI FROM THE COMPUTER

…Sergio Staino. A woman in bed with Bobo: "Can you keep a secret?" And Bobo says: "No way!"

PAOLO MONDANI
You have completely replaced me as the owner.

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Exactly. Tell me a message you want to write... Don't write it, just tell me. Whatever you want.

PAOLO MONDANI
I am truly amazed.

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
And technically, while your phone was actually turned off, looking at my phone I see that you just wrote to me: "I am truly amazed."

PAOLO MONDANI
So basically, you're writing from my phone?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
As if it were you. And technically, it is your phone that's writing.

PAOLO MONDANI
So, can you add messages, or even photos, to my phone?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Content, photos, whatever.

PAOLO MONDANI
Videos?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Absolutely.

PAOLO MONDANI
Documents?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
I can also delete them.

PAOLO MONDANI
Can you manipulate them?

FRANCESCO ZORZI - COURT-APPOINTED EXPERT - CYBER INTELLIGENCE SPECIALIST
Absolutely.

PAOLO MONDANI
A trojan can directly infect your cell phone, computer or tablet.

GIOVANNI ZICCARDI – PROFESSOR OF IT LAW - UNIVERSITY OF MILAN
Or even a GPS navigator, a video game console, a satellite dish, a smart TV, any device...

PAOLO MONDANI
An alarm system...

GIOVANNI ZICCARDI – PROFESSOR OF IT LAW - UNIVERSITY OF MILAN
An alarm system.

PAOLO MONDANI VOICEOVER
The trojans used in investigations capture everything that's on the phone, but there are also commercial ones available on the market that cannot be inoculated remotely, like the ones used by law enforcement, but only by having access to the phone. The cost is about 250 dollars for a 2-month lease. They can do everything.

MARCO ZONARO - FORENSIC CONSULTANT
Capture conversations, obtain call logs, do call recording, record VOIP calls, etc.

PAOLO MONDANI
Call recording means to tape calls, record phone calls.

MARZO ZONARO
Yes. Or activate a key log function. This, for example, is what it obtained, these are test messages that I had sent...

PAOLO MONDANI
So it captured WhatsApp, Telegram...

MARCO ZONARO
It captured Whatsapp, it captured…

PAOLO MONDANI
Google Play.

MARCO ZONARO
Google Play.

PAOLO MONDANI
Instagram.

MARZO ZONARO
Instagram, Internet Samsung, I can see…

PAOLO MONDANI
MMS messages.

MARCO ZONARO
Or see the images that are stored in the phone, these are some test photos that I took...

PAOLO MONDANI

Photos and videos.

MARCO ZONARO
Capture any audio files that may be present inside the phone. Provide the phone's location, by activating the GPS and telling me where it is. Activate a Rem Cam function: namely, take pictures with either the front or rear cameras.

PAOLO MONDANI
But you have to have access to the phone.

MARCO ZONARO
Absolutely.

PAOLO MONDANI
And since it can be hard to gain access, what you can do is give your son or your girlfriend a phone that's already...

MARCO ZONARO
Already infected, yes.

PAOLO MONDANI
Pre-infected with the trojan.

MARCO ZONARO
There are companies - I know a few in Italy that sell hacked phones ready for use.

PAOLO MONDANI VOICEOVER
Malware, spyware, viruses and trojans: in legal terms, they are called "IT capture tools", and thanks to the reform introduced by minister of justice Bonafede, approved in January 2019, they can also be used to investigate corruption. Until then, they could only be used for mafia and terrorism investigations. Luca Palamara is the Roman magistrate at the centre of the scandal which hit the High Council of the Judiciary in the summer. Accused of corruption, he was infected with a trojan by the Perugia Prosecutor's Office. His phone was hacked using a fake Vodafone message.

LUCA PALAMARA - MAGISTRATE
On the day of May 3, 2019, my phone carrier blocked my cell phone, having previously informed me that I would be called by a technician for a software update, and that my cell phone would again be operational within a couple of hours.

PAOLO MONDANI VOICEOVER
The malicious update contained the trojan. Luigi De Ficchy was the Chief Public Prosecutor of Perugia who asked that Palamara's phone be hacked.

PAOLO MONDANI
You're saying that traditional phone tapping is ineffective because people don't talk much any more.

LUIGI DE FICCHY - FORMER CHIEF PUBLIC PROSECUTOR OF PERUGIA
People don't talk much, and even with WhatsApp, which is what everyone uses now, people will make an appointment and say "let's meet in that place" and you may not know what "that place" is. And if you can't place a recording device under the table, then you can't capture the conversation. The trojan is like a recording device. It's more

spontaneous. It's harder to think that you're being monitored 24/7, so it's a very effective tool.

PAOLO MONDANI
Lawyers Giuseppe Calafiore and Piero Amara, who were being investigated together with you on corruption charges, were also targeted but were not infected because they didn't fall for the trick. However, the phone company was not mobilised for them as it was for you. Another oddity is that not even your alleged corruptor, Fabrizio Centofanti, was infected with the trojan. How do you explain this?

LUCA PALAMARA - MAGISTRATE
I'm lead to believe that investigators must have been especially interested in my activity, particularly with regard to the appointments for judicial offices.

PAOLO MONDANI VOICEOVER
Luca Palamara, a former member of the High Council of the Judiciary and former president of the National Association of Magistrates, is accused of receiving money from Roman entrepreneur Fabrizio Centofanti, arrested on corruption charges in February 2018. Also ending up behind bars were lawyers Piero Amara and Giuseppe Calafiore, involved in a corruption scheme aimed at rigging trials and sentences whose referent in Rome was allegedly Palamara himself. Through his cell phone, the Perugia magistrates also listened in on the meetings discussing future appointments to Italy's highest prosecutor posts.

LUCA PALAMARA - MAGISTRATE
All I can say is that I never would have traded my position for any appointment.

PAOLO MONDANI
But you are accused of a disciplinary offence, a serious misconduct, for having participated in a meeting on the 9th of May with two politicians: Cosimo Ferri and Luca Lotti.

LUCA PALAMARA - MAGISTRATE
To think that mine was the only table where we talked about the Prosecutor's Office of Rome or Perugia or Brescia would be to say something that does not correspond to reality. Mine was but one of the tables where such topics were discussed.

PAOLO MONDANI VOICEOVER
As if it were normal, politicians and magistrates were sitting around a table discussing appointments to Italy's most important judicial offices. And the honourable Luca Lotti was pushing to influence the appointment of the new Prosecutor of Rome, while being investigated by that very same office for the CONSIP case.

PAOLO MONDANI
You sensed that your were being monitored, correct? Because what emerges from your deposition is that you seem to have learned from Cosimo Ferri, or at least you got the feeling...

LUCA PALAMARA
During a dinner...

PAOLO MONDANI
...from the honourable Cosimo Ferri that they might have been watching you.

LUCA PALAMARA
During a dinner it came up that I might be the one infected with the trojan. I said: it seems impossible, but even if that's the case, they'll hear me talking about the appointments.

PAOLO MONDANI
In May 2018, the Rome Prosecutor's Office sent a memo from the Guardia di Finanza about your purported corruption to the Perugia office, which is tasked with investigating Roman magistrates. So why were you infected with the trojan exactly one year later, in May 2019? By that time, investigators would have presumably had very little hope of gathering any evidence of this corruption. Perhaps they were really trying to catch you red-handed while you were negotiating the appointments?

LUCA PALAMARA
You said it, not me...

PAOLO MONDANI
It's been said that you were like the P2. That's a rather bold statement.

LUCA PALAMARA
My cell phone was seized. I have everything in my phone. I have never gone to clandestine meetings.

PAOLO MONDANI VOICEOVER
Indeed, today the P2 would probably use a secret Telegram chat. Even though some trojans can already crack the webchat's encryption. Such as the last Italian trojan, called Exodus, which was invented by Diego Fasano, an entrepreneur from Calabria who was arrested last may on charges of having illegally monitored tens of unaware citizens. Exodus was also sold to the ministry of the Interior and our secret services, which ended up being investigated for this reason. Fasano was recently released from home confinement.

PAOLO MONDANI
Exodus did something more than ordinary spyware. What, exactly?

DIEGO FASANO - EX CEO OF E-SURV
Firstly, it was a platform that could function on both Android and iOS cell phones.

PAOLO MONDANI
But the others also manage to intercept...

DIEGO FASANO - EX CEO OF E-SURV
In most cases, they specialize in either one or the other. Exodus worked on both. It had, basically, two main abilities: the first was what is known as "stealthness", namely its ability to hide and become undetectable. The second, aside from stealthness, was that on many devices it could access encrypted chats.

PAOLO MONDANI
How many Prosecutor's Office employ your trojan?

DIEGO FASANO - EX CEO OF E-SURV
I would say that a good 80 or 90% of Italian prosecutor's offices used the Exodus platform, through the partners to whom we leased the software.

PAOLO MONDANI
The Judicial Police used your trojan to infect cell phones using a trap, namely an app that people would download from Google Play. How did you make it enticing for users...?

DIEGO FASANO - EX CEO OF E-SURV
That depended, sometimes it may have been a porn app.

PAOLO MONDANI
We've read that the data would end up on the Amazon cloud in Oregon.

DIEGO FASANO - EX CEO OF E-SURV
When the virus was on the phone, it had to collect data and send it to prosecutor's office's servers. One crucial precaution we took was to make sure that the data always went through proxy servers. It's what we call the anonymisation chain. Why? Because in the event that someone found the virus on their phone, a skilled IT person could have seen the destination IP. Without these intermediary servers, they would have immediately seen the prosecutor's office's server.

PAOLO MONDANI
In the case of Exodus, the data had ended up in Oregon.

TOMMASO PALOMBO - PRESIDENT OF ILIIA - ASSOCIATION OF INTELLIGENCE SERVICE PROVIDERS - INTERCEPTIONS
By law, technically, all intercepted data must be delivered to the authorities, and must not transit through any server other than those belonging to the Prosecutor's Office.

PAOLO MONDANI
Your arrest warrant mentions that many individuals are presumed to have been illegally monitored using your software.

DIEGO FASANO - EX CEO OF E-SURV
They are still being identified, one year later.

PAOLO MONDANI
Can you explain what happened?

DIEGO FASANO - EX CEO OF E-SURV
The filter we used to avoid that someone other than the person of interest would download the app, during the time frame when it was in the Play Store, was a filter based on the IMEI number. Namely...

PAOLO MONDANI
The IMEI number is basically like the device's license plate.

DIEGO FASANO - EX CEO OF E-SURV
Correct. The Judicial Police would insert the IMEI number of the hacked phone, the app would be downloaded, it compared it with the phone and if they matched, the virus would be downloaded. If not, it wouldn't. In a few tens of cases, this filter did not work properly. Look, what I can tell you is that we never illegally spied on anyone nor did we compile illegal dossiers on anyone.

PAOLO MONDANI VOICEOVER

A former employee of the company disagrees. He is among the developers of the Exodus trojan, and he told his side of the story to the Naples magistrates who are investigating the matter.

PAOLO MONDANI
Did you know that totally unknown and unaware people were being illegally monitored?

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
Yes, I found out.

PAOLO MONDANI
What were those people called?

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
Volunteers.

PAOLO MONDANI
Volunteers? At the company, you must have asked yourselves: why were they illegally spying on citizens?

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
A strong belief that we could do whatever we wanted. Perhaps, I mean, that's the conclusion we reached at first.

PAOLO MONDANI
The managers were... They felt very strong, they felt basically untouchable? Is that what you're saying?

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
You could say that.

PAOLO MONDANI
At one point, to justify the fact that they were spying on those they called volunteers, but were actually victims, didn't your bosses tell you that they had powerful backers?

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
They always conveyed to us that what we did was totally legal.

PAOLO MONDANI
That they weren't worried.

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
Yes.

PAOLO MONDANI
That operating in that way wasn't a problem.

FRANCESCO POMPÒ - FORMER E-SURV DEVELOPER
Yes.

PAOLO MONDANI
One of your former employees told the Naples Prosecutor's Office that your colleague Ansani was listening in on the conversations.

DIEGO FASANO - EX CEO OF E-SURV
Yes, I read that.

PAOLO MONDANI
So, I mean, it's as if he was perfectly aware that it wasn't an accident. He either listened because he knew such a thing was common, even encouraged, or because, I don't know, maybe he enjoyed it. Either way, it's very serious, don't you think?

DIEGO FASANO - EX CEO OF E-SURV
That's serious, because he wasn't allowed to. If this former employee is telling the truth, that would be very serious.

PAOLO MONDANI
E-SURV, which also worked for several Prosecutor's Offices in Calabria, is accused of spying on totally unaware citizens that had never been involved in any illegal activity, nor had ever been questioned by any prosecutor or magistrate. Why was E-SURV doing this?

NICOLA GRATTERI - PUBLIC PROSECUTOR OF CATANZARO
Someone may feel compelled to illegally spy on his girlfriend or wife if he thinks she's cheating on him. But anyone who has the capacity to systematically spy people for months or years, is certainly doing it for people who have lots of money.

SIGFRIDO RANUCCI IN STUDIO
Money is the motor, data is the fuel. The name Exodus evokes biblical images of departure, but here it entered into people's lives - the lives of about a hundred people. The former head of E-SURV says "it was a mistake", but one of his employees disagrees. He believes there's something or someone important behind this company, and that taking a peek into people's lives was common practice. What we know for sure is that all this data ended up on an Amazon cloud, in the United States. "It's to prevent those under surveillance from tracing the spyware back to Prosecutor's Office" says the former head of the company. However, that would be illegal. And therein lies the paradox. That all this information, terabytes of data, is stored on a server that is not at the Prosecutor's Office, but rather in the US. Also ending up in American servers was the data which two siblings, the Occhionero siblings, stole from 6000 people. We're talking about 3 million emails, which even included ones written by former ECB president Mario Draghi, and by former prime ministers Matteo Renzi and Mario Monti. Basically, they were extracting information through a Trojan. Until someone else ultimately gave a Trojan to them.

PAOLO MONDANI VOICEOVER
Spyware is very expensive, but it can also make lots of money for people: for example with industrial and financial espionage. The case of siblings Giulio and Francesca Occhionero made waves across the world. Two very well-known figures in Rome's financial circles, they were arrested in January 2017 and spent one year behind bars for operating a vast cyberespionage ring. The Rome prosecutor's office stopped them after infecting their computer with a trojan.

PAOLO MONDANI
Last year, you were sentenced to five years and your sister to four, on first instance, for alleged cyber espionage activities. Purportedly, you had access to a database with 18,000 usernames, 1,800 passwords, and even tried to infiltrate the email accounts of Renzi, Monti and Draghi?

GIULIO OCCHIONERO - ENGINEER

We were indicted on two counts. The first one, which spurned the whole investigation, was this cyber attack against the ENAV head of security, Francesco Di Maio. The second one claims that we had access to an unspecified number of emails - because if you read the indictment, you'll see that it doesn't specify the emails, nor when they were accessed, nor where nor by whom. The emails are just identified through domains. Well, we have already shown that the first count is completely fabricated, to the point that the evidence presented by the prosecutor, for a crime that took place on 26 January 2016, was on a CD which was burned on 21 January 2016.

PAOLO MONDANI
So five days earlier?

GIULIO OCCHIONERO - ENGINEER
It's like producing a smoking gun as evidence for a crime that will happen five days later.

PAOLO MONDANI
Please explain, sir: the prosecutor's expert was investigating you before being issued a warrant to do so?

GIULIO OCCHIONERO - ENGINEER
Absolutely, without a doubt.

PAOLO MONDANI VOICEOVER
The expert had already hacked into the Occhioneros' computers on the insistence of ENI and ENAV, which believed they were being spied on by the two siblings. Now, the Perugia Prosecutor's Office has placed both the expert and the magistrate Eugenio Albamonte under investigation, for official misconduct. But Albamonte is still overseeing the Occhionero investigation.

PAOLO MONDANI
At one point, the Rome prosecutor's office infected your PC with a trojan. You believe such activity to have been illegal. Why?

GIULIO OCCHIONERO - ENGINEER
As far as the trojan, current guidelines still indicate that it can only be used in mafia and terrorism investigations, but we weren't accused of either mafia or terrorism.

PAOLO MONDANI
According to the judge who sentenced you, you sent out a malware via email and used it to accumulate vast amounts of data and documents, thus compiling a series of bona fide dossiers. This malware is called Eye Pyramid, and it is a known fact that you are a Freemason. Is that name what prompted you to buy it?

GIULIO OCCHIONERO - ENGINEER
First of all, this malware was never a part of the trial, the trial was carried out without accounting for the malware.

PAOLO MONDANI
It's a fact that you have good relations with the US embassy and American Republicans, and some people from the embassy - if I understand correctly - even visited you in jail... It begs the question: were you a secret agent?

GIULIO OCCHIONERO - ENGINEER

No, I've never been involved with that. I've worked on projects connected to the US government, but I've never worked for an intelligence agency, be it Italian or foreign.

PAOLO MONDANI VOICEOVER
Giulio Occhionero believes he was placed under investigation because someone wanted to link him with the Russiagate scandal. It's the story of Hillary Clinton's personal emails, which tainted the 2016 US presidential campaign. Occhionero, who has solid relations with American Republicans, believes they were trying to paint him as the one responsible for hacking into her emails, in order to frame Donald Trump.

GIULIO OCCHIONERO - ENGINEER
In January of 2017, finding the emails would have automatically meant finding the email thief, and showing a link between the thief and the Trump administration would have put tremendous pressure on the president to resign or on congress to initiate impeachment procedures.

PAOLO MONDANI
And you believe that someone was trying to stick Mrs. Clinton's emails onto you?

GIULIO OCCHIONERO - ENGINEER
We believe that this was the subject matter, and that it was the object of discussions between the Rome Prosecutor's Office, the FBI and the Department of Justice.

PAOLO MONDANI
What do you suspect?

GIULIO OCCHIONERO - ENGINEER
I suspect an involvement of the Italian government.

PAOLO MONDANI VOICEOVER
Who knows if this conspiracy is real or just a vile excuse. What we do know is that, through a trojan, magistrates discovered 3.5 million emails swiped from six thousand people who were being spied on, and whose sensitive information ended up on American servers. The investigation hasn't yet concluded, but we know that the Occhioneros spied on other politicians with institutional roles, in addition to Renzi and Draghi. Who was paying them, and why they did this, remains a mystery. We just know that their bank accounts are in Malta, which does not cooperate with the Italian judicial system. But how much does lawful interception cost the government?

NICOLA GRATTERI - PUBLIC PROSECUTOR OF CATANZARO
Phone tapping costs one Euro a day, here at the Catanzaro office.

PAOLO MONDANI
For traditional wire tapping?

NICOLA GRATTERI - PUBLIC PROSECUTOR OF CATANZARO
Traditional.

PAOLO MONDANI
What about a hidden recorder?

NICOLA GRATTERI - PUBLIC PROSECUTOR OF CATANZARO
Bugging is 20.

PAOLO MONDANI
And electronic? In other words, trojans?

NICOLA GRATTERI - PUBLIC PROSECUTOR OF CATANZARO
That is around 110-120.

PAOLO MONDANI
How much does it cost here in Milan?

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
Traditional phone tapping is 4 Euro a day, while the average price we apply for audio recording is about 60 Euro.

PAOLO MONDANI
Per day?

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
Per day. Active electronic interception is about 150 Euro.

PAOLO MONDANI VOICEOVER
For years, prosecutor offices have been asking for a standardised price list and an official roster of service providers. Currently there are about 70 of them, often with shady corporate structures. In 2017 there were 106,000 traditional wire taps, 16,000 audio recordings and 4,500 electronic interceptions. In 2018 the total cost of these operations was 205 million Euro. In the past two years, the number of trojan interceptions has skyrocketed. The 2017 law by minister Orlando and the 2019 "Spazzacorrotti" law of minister Bonafede regulated the use of trojans, but the most important part is missing.

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
We lack a ministerial decree regulating the technical characteristics of the intruder software, because so far we've been tackling the issue of infection, but an other important issue concerns deactivation. One further aspect is the so-called "search function", because capturing all data inside a cell phone is a form of search and seizure. And all of this is still not regulated.

PAOLO MONDANI
What should be covered in the procedural guidelines regulating the use of trojans on the part of law enforcement?

GIOVANNI ZICCARDI – PROFESSOR OF IT LAW, UNIVERSITY OF MILAN
I believe the first requirement should be some kind of independent third party monitoring. As long as these activities remain confined to the prosecutor offices or the companies providing the services, and results are being brought as evidence in trials but we don't have the possibility of knowing step by step what has been done, I don't think it can be considered an acceptable process. Or rather, it's all just based on trust.

PAOLO MONDANI
Is there a public entity, in this case, which can monitor what the trojan is doing either during its activity or upon its completion?

ROBERTO DE VITA - LAWYER - PRESIDENT OF EURISPES CYBERSECURITY WATCH
No. And that's not all. When, in the course of intelligence or prevention activities, we utilise tools over which we do not have full control, we have no way of guaranteeing that such classified information will remain within our perimeter of national interest. If these programs are developed by third parties, the possibility exists that they could be used to spy the inner workings of our judicial system.

PAOLO MONDANI
Hypothetical scenario: you request a trojan to be placed on the phone of a known mafia boss. Do those phone calls end up directly on your server or not?

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
No.

PAOLO MONDANI
Where do they end up?

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
They end up on a temporary server managed by the company from whom we're leasing the equipment, and the following step is the transmission to our server. So what's the problem? The problem is monitoring the investigative chain.

PAOLO MONDANI
Exactly, who's monitoring it?

ALESSANDRA DOLCI - ADJUNTC PROSECUTOR - HEAD OF ANTI-MAFIA BUREAU, MILAN
Ehh... who's monitoring it... we certainly are not able to.

PAOLO MONDANI VOICEOVER
And that's not all.

PAOLO MONDANI
So, you perform phone tapping and bugging operations, but are you physically the ones placing the bug, for example... can it happen?

TOMMASO PALOMBO - PRESIDENT OF ILIIA - ASSOCIATION OF INTELLIGENCE SERVICE PROVIDERS - INTERCEPTIONS
In 99% of cases, yes.

PAOLO MONDANI VOICEOVER
So it's the private companies who are placing the bugs and trojans. And they all refused to comment. Except for SIO, located in Cantù, one of the leading intelligence service providers for Italian law enforcement. And they manufacture bugs and cameras in-house.

PAOLO MONDANI
You know that Italian prosecutor offices are basically renting trojans and spyware from the Germans, from an Anglo-German company or from Israel, but there's nothing Italian.

ELIO CATTANEO - PRESIDENT OF SIO SPA - INTELLIGENCE SOLUTIONS
It would be nice if the Italian Government could form a pool of companies and invest some money on...

PAOLO MONDANI
...a governmental trojan?

ELIO CATTANEO - PRESIDENT OF SIO SPA - INTELLIGENCE SOLUTIONS
Exactly, yes, a governmental trojan.

PAOLO MONDANI VOICEOVER
And without a trojan entirely controlled by the Government, the risks are unimaginable.

GIOVANNI ZICCARDI - PROFESSOR OF IT LAW, UNIVERSITY OF MILAN
If we lose control of these tools, there's a risk of creating a system of mass surveillance. In other words, the virus may suddenly mutate, escape the context for which it was created, namely the individual cell phone where it was sent to, and end up in a store where it will downloaded by millions of unwitting citizens.

PAOLO MONDANI
Indeed, you write in your book that these trojans are, or could be, polymorphic, namely capable of adapting to the system.

GIOVANNI ZICCARDI - PROFESSOR OF IT LAW, UNIVERSITY OF MILAN
Just like viruses in nature. We may have individuals that take the code of these trojans designed for law enforcement and intended for legal investigations, and transform it, adapting it for their own criminal use.

SIGFRIDO RANUCCI IN STUDIO
"Espionage might perhaps be tolerable, were it practised exclusively by honest men". Thus wrote Montesquieu in "The Spirit of Laws", about 250 years ago. The message, however, is still very current. Because when it comes to electronic surveillance, it's a lawless frontier: there are no limitations. "We set the limitations", says the expert. Sounding the alarm - or perhaps waving a white flag - is adjunct prosecutor Alessandra Dolci, who also heads Milan's Anti-Mafia Bureau: we lack strict norms preventing data manipulation. This is no small matter because, as we've seen, these types of software can write text messages on our behalf and even listen to us while the phone is turned off. Perhaps that's why phones must always be charged - they now make them with batteries that cannot be removed. The other point that Dolci calls attention to is that we are unable to monitor the various steps of electronic interception. We cannot see when the trojan is activated and when it is deactivated. What if it continues collecting information? The 2017 Orlando reform allowed trojans and electronic interception to be used in contrasting terrorism and organised crime. Their use had been extended by Minister Bonafede in 2019, who this year further extended it to anti-corruption activities within public administrations. But we lack clear rules, it's all a bit vague. And this doesn't help magistrates - because there are no regulations - nor does it help the companies who carry out these interceptions. It also doesn't help the Judicial system, because there are countless appeals pending in the Court of Cassation, and because there isn't a standardised price list of services, nor an official roster of companies that provide intelligence services. And we should be able to demand transparency from these companies, as far as their corporate structure and dealings. Finally, we lack a governmental trojan - something that is designed, monitored, utilised and deactivated by governmental officers. Without it, we're forced to rely on those developed by others, and we should have realized sooner how many potential drawbaks there are.

PAOLO MONDANI VOICEOVER
We never learn the lesson. And yet, the story of Hacking Team should have taught us a lot. The Milan-based company was a giant of the spyware industry, to the point that its "Galileo" was long considered the world's best trojan. But on 6 July 2015, it fell under the attacks of a hacker named Phineas Fisher, who aimed to denounce what Hacking Team was really doing.

FORMER HACKING TEAM EMPLOYEE
We used to operate in the defensive security sector, but we closed that division in 2012 and began making attack software. Our flagship product was Galileo. But with the advent of next generation cell phones, security features on those devices began improving. And when Israel's NSO Group entered the market, we could no longer compete. So our company went from being the market leader to selling to technologically underdeveloped countries.

PAOLO MONDANI
You sold to countries like Kazakhstan, Azerbaijan, Singapore, the UAE, Saudi Arabia, Nigeria, Sudan, Egypt, Panama and Mexico. All countries that could use trojans against political opponents or journalists. Certainly not against terrorists.

FORMER HACKING TEAM EMPLOYEE
All transactions were authorised by the Ministry of Economic Development. Clearly those countries could have used the software against political opponents and reporters, but the same can be said of certain so-called democratic countries. The Snowden case is telling.

OLIVER STONE - WRITER AND DIRECTOR OF "SNOWDEN"
For my film on Snowden, I pieced together the story that he told me. At first he was OK with monitoring dangerous individuals, but then he realised that the agency, the NSA, ended up doing mass surveillance on anyone around the world, and he was shocked. Snowden says: why do we need all this information if we're just fighting terrorism? There's really no point in keeping the entire planet under surveillance, other than to randomly accumulate data, to know everything about everyone, and perhaps use that data to destabilise foreign countries or to destroy companies.

PAOLO MONDANI
In Arab countries and former Soviet republics, you used to sell Galileo through two Israeli companies: Verint and Nice Systems. Why did the Israelis distribute your product rather than sell theirs directly?

FORMER HACKING TEAM EMPLOYEE
Israel at the time did not have a spyware as effective as ours, and it couldn't sell to certain Arab countries. So it took our products and peddled them onto the Arabs while making a profit. But basically it was us selling to the Arabs; it was a triangulation.

PAOLO MONDANI
And how did your flagship spyware Galileo work?

FORMER HACKING TEAM EMPLOYEE
Once inside, Galileo could basically access everything that was in the device. Consider that in the US, we used to hold classes for the FBI and the DEA, we even held courses in Israel: we were really good.

PAOLO MONDANI
In November 2014, however, the ministry of Economic Development introduced a "catch-all" clause mandating that all your foreign sales needed to be pre-approved, to prevent your spyware from ending up in countries which violated human rights.

FORMER HACKING TEAM EMPLOYEE
That clause would have forced us to close, but our company was able to block the ministry.

PAOLO MONDANI
I believe it was the Renzi government and Italy's secret services that helped you out; after all, you were selling Galileo to AISE and the Prime Minister Office.

FORMER HACKING TEAM EMPLOYEE
Well, let's say that the matter was resolved very quickly. We did have strong ties with both the government and secret services. But I don't want to say anything else.

PAOLO MONDANI VOICEOVER
Worldwide, the surveillance industry consists of 528 companies. Very few are as qualified as Hacking Team. London's Privacy International has released a report on these companies.

EDIN OMANOVIC - PRIVACY INTERNATIONAL'S STATE SURVEILLANCE
The main ones are the Anglo-German Gamma Group, BAE Systems here in the UK and NSO Group in Israel. NSO Group developed what is currently the world's most advanced technology: the so-called zero-click attack. It means they can send a message to a target and he doesn't even need to fall for the trap and click on the link for his device to be infected by the spyware.

PAOLO MONDANI VOICEOVER
The managers of NSO Group belong to the exclusive club of Israeli intelligence units. The company does many of its operations abroad to ensure greater secrecy. They have two research centres in Ukraine and Bulgaria. And their corporate structure branches out to Luxembourg and Malta.

PAOLO MONDANI
Great Britain has the Investigatory Powers Act of 2016, which regulates use of spyware by secret services. What does this law provide for and what are your objections to it?

EDIN OMANOVIC - PRIVACY INTERNATIONAL'S STATE SURVEILLANCE
It provides for mass electronic intrusion. Now, secret services can track not just an individual target, but entire neighbourhoods or cities. It's such an aimless practice, just mopping up all internet traffic that enters or exits the UK.

SIGFRIDO RANUCCI IN STUDIO
Israel's NSO Group is the world leader in the field of espionage software. Their gem is Pegasus, which was likely used by Saudi Arabia to monitor and track the movements of opposition journalist Jamal Khashoggi. He was then killed inside the Saudi consulate in Istanbul. But Pegasus was also used by other governments, like those of Uganda, Bahrein and South Sudan. Used against their political opponents, against reporters, against human rights activists and also to monitor foreign diplomacy on their territory. It was used by Mexico's government to monitor activists - those who fight against drug cartels - but also to monitor union leaders. It was even used against a scientist, Professor Simon Barquera, who for years has been studying the adverse health effects

of sugary beverages like Coca Cola, and demands that they be taxed more heavily. Coca Cola is so powerful in Mexico that it can even influence the Mexican government. All of this was done in part by breaking into WhatsApp, because the Israeli experts have identified a flaw, where all they need is for someone to answer an anonymous phone call to turn their private life into an open book. WhatsApp, which is owned by Facebook, is seeking millions in compensation from NSO, after 1,400 user profiles in 20 different countries were violated over the course of 14 days. This is a lawless environment, which means that efforts by actual good guys to spy on bad guys can be rendered futile. And now let's talk about the surveillance software used to track the movements of Giulio Regeni, the Italian researcher killed in Egypt in circumstances yet to be clarified.

PAOLO MONDANI VOICEOVER
The United States are witnessing a spyware boom. Investigators have noticed that more and more people are buying them online. Companies spying their employees, husbands and wives, parents.

JUDD BANK - PRESIDENT OF CPI INVESTIGATIONS - NEW YORK
A little while ago a woman came in. Her fifteen-year-old daughter had been coming home visibly intoxicated. They lived outside New York, and having her followed would have been expensive. So we had the mother buy a new cell phone for the daughter, already infected with a trojan. We didn’t need a warrant because it was the mother purchasing it. It turned out the girl had fallen for a 35-year-old, who worked as a pimp and was giving her drugs. We had him arrested and now the girl is doing much better.

PAOLO MONDANI VOICEOVER
But how do things work for those actually investigating?

ADAM WANDT - PROFESSOR AT JOHN JAY COLLEGE OF CRIMINAL JUSTICE - NEW YORK
Usually police departments here don’t want to use spyware; they’re too complicated to manage. Basically only the FBI does that. And of course intelligence agencies, who for reasons of national security turn to a FISA court, the secret federal court which will issue a warrant every single time.

PAOLO MONDANI VOICEOVER
But trojans don’t always solve things. In fact, they complicate them.

JOSEPH P. FACCIPONTI – LAWYER - FORMER MANHATTAN FEDERAL PROSECUTOR
Let me tell you about the child pornography website called Playpen. For two years, between 2015 and 2017, the FBI infected it with a trojan. 870 people ended up behind bars and 259 children were saved. But a few defendants, as was their right, asked to know the trojan's source code. Well, the FBI opted to drop the charges rather than reveal the trojan's source code to the defendants.

PAOLO MONDANI VOICEOVER
Cyber-espionage often clashes with the rights sanctioned by the law. When that happens, which do we choose: safety or freedom?

PAUL ROSENZWEIG - GEORGE WASHINGTON UNIVERSITY - DEPARTMENT OF NATIONAL SECURITY
Look at the Carpenter case. I’m talking about a gang that committed a slew of robberies some years ago between Ohio and Michigan. The FBI obtained the cell phone location data for one of the members, Timothy Carpenter, who was sentenced to jail. But the

FBI had acquired the data without a properly issued warrant. And last year the Supreme Court sided with Carpenter. There was a time when the FBI could just tell the phone company: give me the data. Now that's no longer the case. Personally, I prefer a law that safeguards privacy and freedom rather than indiscriminate mass surveillance.

PAOLO MONDANI VOICEOVER
Last summer, the United Nations issued a special report on the dangers of mass surveillance. David Kaye is its writer.

DAVID KAYE - UN SPECIAL RAPPORTEUR FOR FREEDOM OF EXPRESSION
In the report, we propose a moratorium on the sale and exportation of these technologies. We need governments, civil society and companies to give themselves some rules. It won't be easy because we're talking about an industry worth tens of billions of dollars. But our very freedom is at stake.

PAOLO MONDANI VOICEOVER
Every year in Germany, about 40,000 wire taps are performed. The German Constitutional Court has sanctioned the right to integrity and confidentiality of IT system - a first in Europe. But this right does not apply when the government monitors transiting data: therefore, trojans are fair game.

ULF BUERMEYER - FORMER JUDGE - PRESIDENT OF THE SOCIETY FOR FREEDOM RIGHTS.
And the parliament simply does not care. Even though the police has bought trojans from private companies, most notably FinFisher. And their source code remains in the hands of these private entities. Instead, the government needs to own these technologies, otherwise they'll never know what they might be doing.

PAOLO MONDANI
These trojans may be tremendously invasive and detrimental to individual freedoms, but when it comes to organised crime, terrorism and corruption, they are the most prominent investigative tool in history.

ULF BUERMEYER - FORMER JUDGE - PRESIDENT OF THE SOCIETY FOR FREEDOM RIGHTS.
No trojan, in Germany, has ever prevented a terrorist attack or led to the capture of any important criminals. And yet they've cost us tens of millions of Euro. Would it not have been better to hire more policemen?

PAOLO MONDANI VOICEOVER
Claudio Guarnieri is one of the world's best hackers. He now lives in Berlin and heads a team of IT experts for Amnesty International. Drawing awareness to cases such as that of Ahmed Mansoor, who for years was tracked via trojan by the UAE government.

CLAUDIO GUARNIERI - HEAD OF SECURITY LAB, AMNESTY INTERNATIONAL
Ahmed Mansoor is a human rights activist. There are documented cases of him being targeted using software developed by Hacking Team, at first, then by FinFisher, which is another German company, and recently by NSO Group, the aforementioned Israeli company.

PAOLO MONDANI
Where is he today?

CLAUDIO GUARNIERI - HEAD OF SECURITY LAB, AMNESTY INTERNATIONAL

A year and a half ago he was arrested again, for a tweet, and sentenced to ten years in prison.

PAOLO MONDANI
Marietje Schaake is a Dutch politician who tried for a decade to introduce regulations for the spyware industry in the European Parliament.

MARIETJE SHAAKE - DIRECTOR OF THE CYBER POLICY CENTER STANFORD UNIVERSITY - CALIFORNIA
Trojans are digital weapons. As such, their export should be regulated just like for real weapons. But in Europe we still haven't been able to get this simple concept through.

PAOLO MONDANI
In 2017, the Netherlands passed a law that allows massive use of surveillance techniques, including online via trojans.

QUIRINE EIJKMAN - LAWYER- PROFESSOR AT THE UNIVERSITY OF UTRECHT
The Intelligence Security Service Act regulates the powers of intelligence agencies, which will now be allowed to carry out mass interceptions. In Italy, if law enforcement wants to monitor someone, they must always obtain an authorisation from the leading prosecutor of Rome's Court of Appeals. Here in the Netherlands, the request will no longer be examined by a judge, but rather by a special commission; a choice which does not convince me.

PAOLO MONDANI
In 2018, a referendum was held and the Intelligence Security Service Act was rejected by the population. Then what happened?

QUIRINE EIJKMAN - LAWYER- PROFESSOR AT THE UNIVERSITY OF UTRECHT
What happened was that the government said it was merely a consultative referendum, and left the law in place. If that weren't enough, they decided it would be the last popular consultation to be held in the Netherlands, and abolished referendums shortly thereafter.

PAOLO MONDANI
How will we live in a world where these spyware tools will have become ubiquitous?

MARIETJE SHAAKE - DIRECTOR OF THE CYBER POLICY CENTER STANFORD UNIVERSITY - CALIFORNIA
No need to look ahead, that future is already here. Do you know the story of Giulio Regeni, brutally murdered in Egypt? Do you know that the spyware which the Egyptian secret services used to track him was produced in Italy? Think about that.

PAOLO MONDANI VOICEOVER
The future is already here. Ryan Gallagher is the Scottish journalist who, a few months ago, posed as a buyer and discovered that a spyware company is working of monitoring millions of Chinese.

RYAN GALLAGHER - JOURNALIST, THE INTERCEPT AND BLOOMBERG NEWS
Semptian, an intelligence company based in Shenzhen, China, has developed a surveillance system named Aegis, which boasts it can spy 200 million Chinese citizens. Part of its know-how was derived through its collaboration with American company IMB.

PAOLO MONDANI

Those who favour the proliferation of spyware say that giving up one’s privacy is no big deal when you have nothing to hide, so we shouldn’t be scared of mass surveillance.

RYAN GALLAGHER - JOURNALIST, THE INTERCEPT AND BLOOMBERG NEWS
If that were the case, we wouldn’t have locks on our front doors or passwords to access our email accounts. Privacy gives us the freedom to be ourselves, to explore our curiosity, to talk freely with our friends without the fear of someone listening and judging us.

SIGFRIDO RANUCCI IN STUDIO
Privacy is an integral part of human liberty. Which is sanctioned in the Universal Declaration of Human Rights. But can privacy and safety coexist? Can there be one without the other? The debate is open. Technologies are a great opportunity but they must be regulated, and human rights can be seriously threatened by these new surveillance tools, which are very useful in contrasting mafias, terrorism and corruption, but which risk becoming instruments of mass surveillance if not properly governed. That's not our opinion, but what Italy’s Privacy Authority wrote in an official memo to Parliament and the Government, asking that some critical issues be solved lest the rights and protections of suspects be at risk. The Authority asks that certain things be clearly specified, such as the limitations of lawful interception, the tools and methods being used, how data is transmitted, and also how it is stored and archived. The Authority also asks that the full integrity, safety and authenticity of the data be guaranteed. To rule out the risk of someone planting criminal evidence in our phone, should they not find what they're looking for. Individual citizens run the risk of succumbing to a dynamic that's far greater than them What are the weapons used in today's cold wars? We just need to look at how the budgets of superpowers have changed over the years. In the 70s, the leading export category was weapons, then came the audio-visual industry, TV formats, news channels. Today, the leading categories are those of web platforms, internet multinationals, big data, phone companies. Could it be a new form of colonisation? We just need to know, so we may choose the lesser evil.