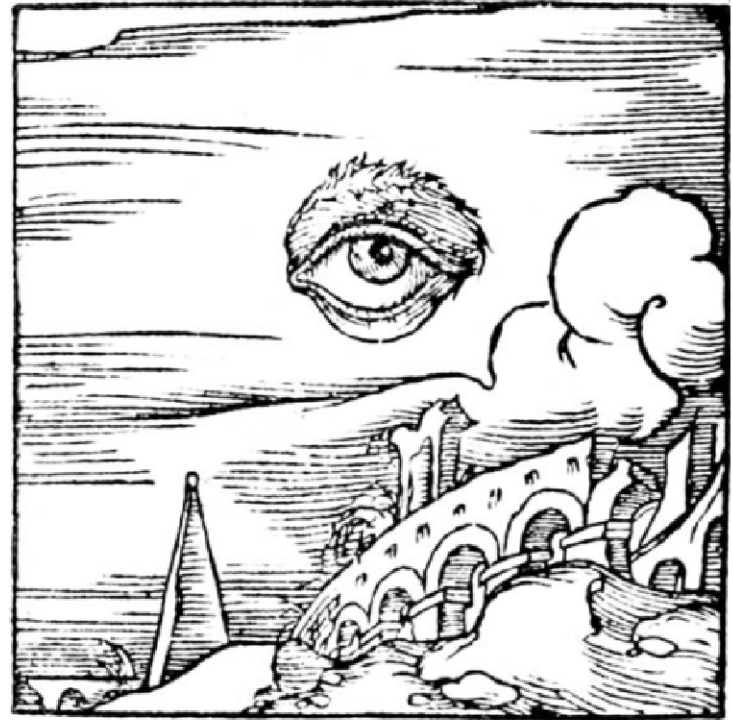


Snooping eyes

Report on Methods and Tools of Digital Repression



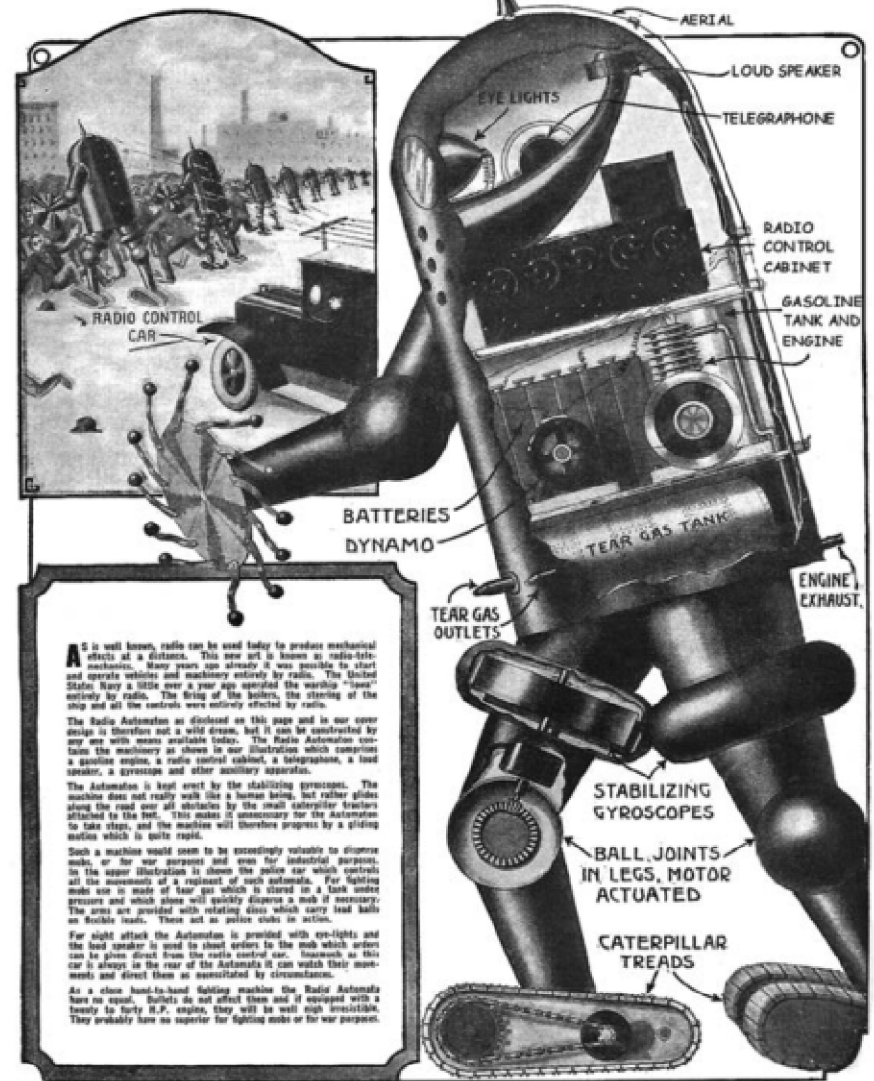
arachidi@autistiche.org
arachidi.noblogs.org



Radio Police Automaton

Distant Control by Radio Makes Mechanical Cop Possible

By H. GERNSBACK



As is well known, radio can be used today to produce mechanical effects at a distance. This new art is known as radio-telemechanics. Many years ago already it was possible to start and operate vehicles and machinery entirely by radio. The United States Navy a little over a year ago operated the warship "Albatross" entirely by radio. The firing of the boilers, the steering of the ship and all the controls were entirely effected by radio.

The Radio Automaton as disclosed on this page and in our cover design is therefore not a wild dream, but it can be constructed by any one with means available today. The Radio Automaton contains the machinery as shown in our illustration which comprises a gasoline engine, a radio control cabinet, a telegraphone, a loud speaker, a gyroscope and other auxiliary apparatus.

The Automaton is kept erect by the stabilizing gyroscopes. The machine does not really walk like a human being, but rather glides along the road over all obstacles by the small caterpillar tractors attached to the feet. This makes it unnecessary for the Automaton to take steps, and the machine will therefore progress by a gliding motion which is quite rapid.

Such a machine would seem to be exceedingly valuable to disperse mobs, or for war purposes and even for industrial purposes. In the above illustration it shows the police car which controls all the movements of a regiment of such automata. For fighting mobs use is made of tear gas which is stored in a tank under pressure and which alone will quickly disperse a mob if necessary. The arms are provided with rotating discs which carry lead balls or flechette loads. These act as police clubs in action.

For night attack the Automaton is provided with eye-lights and the loud speaker is used to issue orders to the mob which orders can be given direct from the radio control car. Inasmuch as this car is always in the rear of the Automata it can watch their movements and direct them as necessitated by circumstances.

As a close hand-to-hand fighting machine the Radio Automaton has no equal. Robots do not affect them and if equipped with a twenty to forty H.P. engine, they will be well nigh invincible. They probably have no superior for fighting mobs or for war purposes.

A radio-controlled police automaton. From Hugo Gernsback, "Radio Police Automaton," *Science and Invention* 12, no. 1 (May 1924): 14.

What kind of conclusions can we take from all of this?
 Even if they are possible and necessary, what we have to search for are not technical solutions to this enormous problems. It's obvious that 4 crazy scientists will always find the way to elude these controls; the problem is more how to ensure that we won't get used to providing online verification whenever requested, just as we got used to accepting cookies. There's not a single way to practice technological self-defense, nor a way that is definitive and all-inclusive. Each situation and each person needs specific tools and unique balances. Not even the complete refusal of the phone is a perfect solution, because it still exposes to the risks of cameras, or microphones; or simply it requires for all the people around us to be willing to make our same choice, or support us.

Even though this text aims to provide a summary of technical surveillance tools, we would like to emphasize that they are not the only instruments of repression.

Since we truly believe that surveillance is a social problem, even before being a technical one, we research and wish to keep the discussion open between more and less nerdy people, who will evade with creativity state, big tech and general control mechanisms, included the patriarchal ones, building relationship models that allow us to go beyond technologies. And this way, for what it concerns us, must be extended and spread outside our bubbles and circles, not just because security is a collective and communal problem, but also because the only to truly defend ourselves is for this culture to spread and multiply, until the last camera will be burned down.

Intro	-----	4
0. Cameras	-----	5
0a. Private cameras (with microphones)		
0b. Reading PINs via HD cameras		
0c. Long-distance video cameras with facial recognition		
0d. Highway camera monitoring		
1. Phones	-----	6
1a. Forensic extraction – local attack		
1b. “Preview” procedure		
1c. Location tracking (via cell towers)		
2. Targeted Interceptions	-----	8
2a. “Normal” calls and SMS		
2b. Passive Electronic Interception – Remote Attack		
2c. Active Electronic Interception – SPYWARE		
2d. Imsicatcher – “Spy” Cell Towers		
2e. Ambient and directional microphones		
3. Blog & social	-----	13
3a. Attack to the website		
3b. Watch out for metadata and services we use!		
3c. Social media and blog monitoring		
3d. Whatsapp and Telegram chats		
4. Misc	-----	16
4a. Controlling bank movements		
Considerations	-----	17

Cover: The eye of God. From Horapollo, *Ori Apollinis Niliaci: De sacris notis et sculpturis libri duo* (Paris: Kerver, 1551), 222.

Intro

Digital technology touches every part of our lives – and the repression of social struggles is no different.

As friends and tech-savvy comrades, we are often approached with questions about what the police and other law enforcement agencies can do. At the same time, we frequently notice behaviors that show a certain carelessness, overlooking the tools these authorities have at their disposal and the growing budgets allocated to advanced surveillance technologies in recent years.

For these reasons, among others, we decided to compile this text to provide, in a structured way, some information about what we have seen or read over the past years.

This text is NOT intended to create paranoia, but rather to foster collective awareness. At the same time, in it does not claim to cover all the techniques used by the state, as most only become known after investigations are concluded.

To keep the main text readable, reflections and analyses are placed at the end for those who wish to read them, and can be skipped by others.

Disclaimer

This information mainly concerns operations and techniques used by the Italian law enforcement, but we think it can be useful for people living in other territories as well.

.....

Operations/investigations mentioned:

Diana (2022):

• <https://ilrovescio.info/2025/06/28/sulloperazione-diana-contro-lanarchismo-in-trentino-cose-utili-da-sapere/>

Scintilla (2019):

• <https://ilrovescio.info/2023/01/18/torino-sentenza-di-primo-grado-del-processo-scintilla/>

Sismi (2022-2024):s

• <https://ilrovescio.info/2023/07/11/le-solite/>

Carnevale No Ponte (2025):

• <https://brughiere.noblogs.org/post/2025/09/11/sugli-arresti-moltopost-carnevale-no-ponte/>

And others that we forgot or that have no name...

Considerations

This texts has followed a quite long period of sharing of reflections, chit-chats, reading and writing on technologies in general. To give a frame of the context in which we are moving and thinking:

In the last year spyware have returned to the media spotlight:

• <https://www.amnesty.org/en/documents/eur70/8814/2024/en/>

• <https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/>

In a more private dimension, we see the increase of usage of stalkerware and parental control apps to stalk partners/exes. Recently the European regulation Chatcontrol has been approved, even if the mandatory requirement for generalized scanning of messaging service has been removed from the text, as a form of protection of privacy and cryptography. This nonetheless does not make us hope that it won't be submitted again, especially given the repeated insistence in the recent years (it was first submitted in 2022).

But here we are not talking “just” about a new Chatcontrol, spyware, stalkerware, artificial intelligence, cameras, microphones – and the list can be long. Recent legislation (for example, look at article 13bis of the Caivano decree) aim at restricting more and more internet use: today we have age verification on porn websites through ID checks. Tomorrow, the same mechanism could be extended to websites that provide anonymity tools, or even to those that are perceived as promoting hate and violence. It is easy to see how such restrictions could gradually expand and, over time, turn into forms of censorship affecting information websites, blogs, and other types of online content.

And there's more! Soon the possibility to install open source software (which means that it's possible for everyone to fully read it and modify it) will be limited, for example by making it impossible to spread smartphone apps without authorization from Google and Android.

Even if we believe that these events fit perfectly into a broader picture of increasingly invasive, controlling and repressive technology, we would like to share some thoughts.

Diving into the spyware world during the last year, we realized that Big Tech companies, Google in pole position (https://storage.googleapis.com/qweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_TAG_report.pdf), are starting to narrate themselves as the privacy protectors. This, besides being clearly a lie, is a significant factor for the social level, because it excludes even the possibility of building, using and spreading alternatives. The world ahead of us is becoming increasingly monolithic, with only one possible path: surveillance, whether done by Microsoft or by the states. All this leads us to believe that using technology for our advantage will be a slippery and complex path, as we have less and less control over it, and all the security drifts will make it even more difficult.

4. Misc

4a. Controlling bank movements

This is an activity common to different inquiries; it has been used for example to verify the existence of suspicious money movements aimed at helping fugitives, or to verify which transactions were linked to solidarity funds for prisoners.

0. Cameras

0a. Private cameras (with microphones)

In the operation following “Carnevale No Ponte,” case files indicate that recordings with audio from a private shop inside a covered market were reviewed. These recordings covered areas where the defendants met and discussed plans for the demonstration, and were used to support charges of premeditation.

0b. Reading PINs via HD cameras

According to the text “*On Operation ‘Diana’ against anarchism in Trentino: Useful Things to Know*”, a high-resolution camera installed inside a car allowed investigators to read a phone PIN as it was typed.

0c. Long-distance video cameras with facial recognition

In Operation Diana, facial recognition cameras were monitored in busy transit areas, such as train and bus stations, to locate a specific individual. If there was reason to believe the person had boarded a bus, the internal cameras of the vehicle were also reviewed.

- <https://irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza>
- www.poliziadistato.it/statics/17/lotto-2---sari-sistema-di-acquisizione-e-trasmissione-v23---finale--2-.pdf

0d. Highway camera monitoring

During Operation Sisimi, investigators checked highway license plates to identify who had hung a banner from a bridge, and later attempted to estimate individuals’ heights from the footage. Urban and highway cameras are frequently used in many operations.

1. Phones

1a. Forensic extraction – local attack

One case involved three phones seized on March 20, 2024, during an action at Malpensa Airport. These phones, protected by PINs and encryption, were returned showing clear signs of compromise: two had the PIN written on a sticker on the back, indicating they had been unlocked and analyzed. As long as we know, the devices were powered off and fairly up to date, requiring a *Before First Unlock (BFU)* attack – one of the most complex and expensive forensic procedures according to Cellebrite.

How to protect ourselves?

Mobile device security depends heavily on model and software/hardware updates, which can be costly.

- **GrapheneOS** is an open-source project providing strong security, but it requires a specific phone model (as of November 2025, the cheapest is Google Pixel 6, ~€100).
- For other Android phones, there are no inexpensive fully secure options. However, some apps from alternative app stores (**F-Droid**) allow data wiping if unauthorized access is attempted. (See apps like **Wasted** and **Duress**)

For further reading:

- <https://search.f-droid.org/?q=wasted&lang=en>
- <https://osservatorionessuno.org/it/blog/2025/03/cellebrite-e-luso-ordinario-della-sorveglianza-digitale-in-italia/>
- <https://nocprtorino.noblogs.org/post/2025/02/11/da-malpensa-a-tel-aviv-come-le-aziende-di-sicurezza-informatica-israeliane-collaborano-con-le-autorita-italiane-per-accedere-ai-dispositivi-mobili/>
- <https://www.anarsec.guide/posts/grapheneos/>
- <https://telefonisicuri.noblogs.org/>
- <https://bruciailtelefono.noblogs.org/>

1b. “Preview” procedure

Once a phone is unlocked, its contents (chats, photos) are manually reviewed while recording screen and audio.

How to protect ourselves?

- Do **not** provide your PIN. In Italy, it is legal to “forget” it when requested by police (though this is not a guarantee).
- Check the rules carefully if abroad – laws vary, and authorities may justify seizure depending on the alleged offense.
- Avoid short or easily guessable PINs. Using a PIN like “1312” is the same as handing it over willingly. The recommended PIN should consist

Essentially, each ID GAIA can have multiple email addresses and phone numbers referencing it, and once that the police has obtained a piece of this data it can try to recover the rest.

3c. Social media and blog monitoring

It’s almost as cops follow them as a soap opera... They are most certainly more informed than all of us are.

In many court documents they cite a constant monitoring activity.

3d. Whatsapp and Telegram chats

Diana Op: although there is no trace of this in the interceptions, on several occasions the DIGOS [italian *General Investigations and Special Operations Division* police] has requested authorization to download WhatsApp chats, and in at least one case also Telegram data.

It is not known whether these requests would have been complied with, but it is known that, following the arrest of Pavel Durov, Telegram updated its privacy policy. It is also possible to verify how many requests have been submitted in each country: for example, in Italy in 2024 there were 158 requests affecting a total of 419 users, while in the first six months of 2025 there were 428 requests involving 1,852 users.

In terms of end-to-end encryption, WhatsApp offers stronger guarantees than Telegram. However, Meta has been subject to investigations in Italy and across Europe concerning privacy issues and the forced integration of artificial intelligence into the WhatsApp application. In addition, chat backups are not encrypted by default.

Each year, Meta receives hundreds of thousands of requests from law enforcement agencies. It is not known how many of these are actually complied with, but the company does hold certain categories of data, including phone numbers, activity duration, connection times, account usage information, and metadata related to messages and calls.

- <https://te-k.github.io/telegram-transparency/>

How to protect ourselves?

More information on messaging apps →

- <https://cloud.systemli.org/s/cmJzEFXHqjwLs39>

For us the best options, which means the best balance between security, ease of use and popularity is still Signal, but there are many apps that guarantee anonymity that can be used when needed.

- <https://www.notrace.how/resources/download/the-guide-to-peer-to-peer-encryption-and-tor/the-guide-to-peer-to-peer-encryption-and-tor-read.pdf>

Subsequently, a request was made to Google to obtain the IP addresses linked with the email. The IP address was then associated with a user thanks to the collaboration of the telephone provider.

How to protect ourselves?

Use email providers that do not collaborate with police or state forces (<https://riseup.net/en/security/resources/radical-servers>), or use systems that mask your IP (Tor, VPN, Proxy).

Gmail, Microsoft, Meta, Proton, etc, do they always give out the requested information?

Diana Op: after an environmental wiretapping where an email address is mentioned, they (police) ask Microsoft the registry, the account billing data, the connection IP logs, all email addresses and phone numbers associated with that address, as well as all the users that registered with a name connected to that email. They also asked the provider "subito.it" the records of the log file and IP addresses used by that email.

Although collaboration between Italian providers and law enforcement agencies is well established and mathematical, the same cannot be affirmed for big tech companies.

Protonmail is considered, and presents itself, as a valid and privacy-oriented alternative; but it's important to remember that in 2020 the company has provided information on the IP address of a French climate activist, who was later arrested.

In the same year, Proton Technologies received 3572 orders (compared to the 13 of 2017) from Swiss authorities to share information on the users. Of those 3572 orders, 195 were coming from abroad. The company contested 750 orders and complied with 2017 requests.

Remember, companies cannot provide data they don't actually have!

• <https://proton.me/blog/climate-activist-arrest>

• <https://privacyradar.com/news/privacy/proton-mail-payment-data-stop-cop-city-activist-identified/>

• <https://transparencyreport.google.com/user-data/overview?hl=it>

ID GAIA

Diana Op: analysis of ID GAIA (Google Account and ID Administration) is mentioned; when there's an attempt to connect to a Gmail account from a different device than the usual, there's a request for an additional verification through SMS. Given that the number linked with the user receives this code, the investigators searched for data related to this account. After having obtained ID GAIA for the account, through the url <https://google.com/maps/contrib/IDGAIA> they saw all the reviews of that account, and through tshat traced back the connected email addresses. They request from Google all log files for each connection to the account. It seems that they never received an answer.

of 8-10 alphanumeric characters.

• <https://archerpoint.com/wp-content/uploads/2025/06/blog-2025-cybersecurity-brute-force-update-01.jpg>

1c. Location tracking (via cell towers)

There are two main ways to track phones via cell towers: **aggregated traffic** and **disaggregated traffic**.

- **Aggregated traffic:** the operator reports the main cell a phone connects to. Transit cells (while moving) are generally not visible, unless events such as signal loss, phone shutdown, or connection to Wi-Fi occur, so movement cannot be precisely tracked.
- **Disaggregated traffic:** shows transit and disconnection cells, allowing more precise movement tracking.

In the documents we reviewed, there was no evidence of disaggregated traffic, though some providers may provide it in certain cases.

How to protect ourselves?

Depending on risk level, it may be safer to leave the phone at home or enable airplane mode.

However, not carrying a phone at all may also be considered an aggravating factor.

2. Targeted interceptions

At this link it's possible to see data relating to various types of interceptions in Italy, from 2014 to 2024:

<https://datiostatistiche.giustizia.it/it/intercettazioni.page>

2a. "Normal" calls and SMS

Remember we always have something to hide, because every piece of information can be useful during an investigation; we cannot predict what will be used against us, and analyzing unencrypted traffic is very easy and inexpensive.

Data retention by telephone providers is regulated according to article 132 of the Privacy Code, with some specific differences depending on the data type:

- data relating to phone traffic (not the content of the calls, but how long, when and who): retained for 24 months starting from the date of the communication.
- data relating to electronic traffic (excluding the content of the communications, such as internet connection data or SMS): retained for 12 months.
- data relating to unanswered calls: retained for 30 days.

Some recent laws have discussed extending this period to 6 years for security reasons; the retention would also apply to cell tower connection data, which falls under the category of electronic traffic.

During the Diana Operation, records from public payphones were also reviewed.

How to protect ourselves?

Don't use calls and SMS! Use encrypted messaging apps such as Signal, we'll talk about this more in section 3d.

2b. Passive Electronic Interception – Remote Attack

Sismi Op: In the pricelist, passive electronic interception (which cost €30/day in 2022) is described as "passive interception of the electronic data flow relating to fixed ADSL or mobile users (data transmission via 2G, 3G, and 4G) for operators capable of autonomously capturing such data." If the operator does not provide this service, the cost increases to €60/day.

Essentially, this type of interception enables law enforcement to access and monitor data traffic, including DNS requests, the current operating system version, the presence of antivirus software, installed applications, and device usage patterns.

In the 2023 pricelist, it was extensively emphasized that this form of interception is instrumental to active electronic interception (i.e.,

3. Blog, social and miscellaneous

3a. Attack to websites

Some court documents state: "activity aimed, with OSINT techniques and Ethical Hacking, at analyzing the structure of the platform... to highlight vulnerabilities useful for a subsequent intrusion". It's not said whether the intrusion actually happened, but that it could have been authorized if necessary.

We will try to briefly describe here what happened. Police has:

1. Carried out OSINT analysis on the website and its contents (research on public information on the blog and its infrastructure)
2. Identified names and nicknames of the authors of the articles (public information, but concealable on wordpress (!))
3. Collected data on users visiting the blog, requesting access logs to the website provider (Aruba, Hostinger, etc). Obtained IP addresses that visited the website in certain hours (data was given by the provider without notifying the website managers).
4. Requested to the ISP (Fastweb, Tim, Vodafone, etc) to identify the IP addresses by associating them with a user (account holder, address).
5. Correlated data with telephone wiretapping and other phone records to strengthen the attribution of the articles to a specific person.
6. Obtained the authorization for a possible technical analysis of the website (research for vulnerabilities) to evaluate the possibility of intrusion or to acquire further technical evidence.

How to protect ourselves?

In this case as well, having used the TOR network or a VPN would have made the inquiries much more complex for the investigators; moreover, it's possible to hide on wordpress the name of whoever is uploading the articles.

3b. Watch out for metadata and services we use!

Meta can provide the account that created a specific page or group.

In the Scintilla Operation the management of a Facebook page was used as evidence; the page was linked to certain people through email addresses associated with the accounts that had created or managed the page.

in-the-middle attacks. At this time, there is no evidence of its use, but it could be used for eavesdropping and traffic diversion. In Italy, the State Police and the Finance Police have issued warrants for mobile and fixed IMSI catchers.

How can we protect ourselves?

Some phones allow disabling 2G calls in the network settings, reducing the risk of unauthorized interception. In any case, a device that is turned on –with or without a SIM card and not in airplane mode–will still connect to a cell tower, making it possible to track its location.

- <https://www.lanotiziagiornale.it/tempi-duri-per-gli-evasori-la-guardia-di-finanza-acquista-gli-imsi-catcher-per-rintracciare-i-cellulari/>
- <https://efforg.github.io/rayhunter/>

2e. Ambient and directional microphones

If cops know the usual meeting places, they can install there videocameras-microphones. Even if you change location, remember that it's not always easy to tell if you are being followed; therefore, it's essential to verify the safety of the meeting places and check whether the use of an ambient microphone is possible.

Bugs, with microphone or GPS tracker, were found during many investigations in cars, homes and even bicycles.

How to protect ourselves?

To detect bugs, a manual search is best, as technological tools are often expensive or ineffective. In cars, they are usually connected to the battery and hidden inside the passenger compartment; in homes, they are found near outlets or inside appliances such as refrigerators and microwaves. Battery-powered versions exist as well, for short-term surveillance, and they are usually harder to find. They often include a SIM card for connectivity and an internal memory/microSD to save recordings.

- https://hackrf.readthedocs.io/en/latest/hackrf_one.html
- <https://www.notrace.how/earsandeyes/#>

spyware deployment), both because successfully infecting a device requires prior knowledge of the user's habits, and because it helps determine whether deploying spyware (which is significantly more expensive) is actually necessary.

How to protect ourselves?

Using TOR connection (<https://www.torproject.org/>) or a VPN will encrypt the information mentioned above.

For the curious ones:

We still need to pay attention to the various nuances. For example, if we use Tails within a network that is being monitored (whether a home network or a hotspot), it will not be possible to observe any unencrypted traffic. By contrast, if we use the Tor Browser, only the websites accessed through that application will be protected from surveillance.

<https://tails.net/>

2c. Active Electronic Interception – SPYWARE

Disclaimer

The cases we were able to analyze all involved smartphones, but similar techniques could also be used to infect laptops. Moreover, attack methods may now be different and more sophisticated.

In the Operation Sismi case, devices were infected with spyware called "Spyrtacus." Based on the information available, this appears to have been the third occurrence in recent years, and several elements of the attack are consistent across all the cases we were able to examine.

In 2023, the cost was €250 for the infection (charged only if successful), plus €170 per day to rent a PC workstation equipped with the relevant management software.

How does the infection happen?

Cooperation from the telecommunications provider and the creation of tailored social engineering attacks are vital.

The target is studied—to a greater or lesser extent—through traditional telephone wiretaps or via the passive electronic surveillance mentioned above.

The most commonly used procedure is as follows:

1. Data and/or phone connectivity to the targeted device is interrupted, if necessary for days.

2. To seek clarification, the targeted user then voluntarily calls customer support, or all outgoing calls are automatically redirected to customer support. In reality, they will be put in contact with a technical department that will instead install the malware.

3. The technical support team will prompt the targeted user to install an application either from the Play Store or from a seemingly legitimate website, which may also be delivered via text message, potentially appearing to come from the mobile operator's number. The user will then be guided through granting the permissions required for the installation and proper functioning of the app, such as enabling installation from unknown sources, allowing the app to run in the background, exempting it from Google Play Protect checks, and granting access to the microphone, location, and other system features.

During Operation Sismi, however, the attackers chose to impersonate Trenitalia and, using various promises, convinced the victim to install the malicious app.

Is it possible they use other methods to install the spyware?

There are methods of installation which are more expensive and more effective as well, such as a one-click attack (a message containing a malicious link, a pdf or an excel file that, if clicked, installs a spyware without the user noticing).

Even more expensive and sophisticated attacks are called zero-click, because no interaction is needed from the user, as was the case for the spyware "Graphite" of the "Paragon Solutions" company, or "Pegasus" of "NSO Group" from some years ago.

It's also possible for this software to be installed during a more or less prolonged police seizure, even though in Italy we still have no evidence of this.

• <https://www.amnesty.it/serbia-ecco-come-attivisti-e-giornalisti-indipendenti-vengono-spiati/>

• <https://decrypto.org/caso-paragon-analisi-dello-spyware-graphite-e-come-ha-infettato-i-telefonini-di-giornalisti-e-attivisti/>

• <https://brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso/>

• <https://techcrunch.com/2025/02/13/spyware-maker-caught-distributing-malicious-android-apps-for-years>

What can a spyware usually do?

- remotely activate the microphone
- read notifications
- view the screen in real time
- take screenshots
- determine the device's exact location
- potentially gain full control of the device

- for an additional fee, it may also be possible to access messaging applications such as WhatsApp, Telegram, and Messenger, although there is no evidence that this actually occurred

How to protect ourselves?

We should not underestimate social engineering attacks. When they are carefully tailored to a specific individual, falling for them is far easier than one might expect.

Take the Trenitalia case, for example. Would it really seem suspicious if, during the call, the attacker listed your recent trips to establish credibility? Or if the call came immediately after you had purchased a ticket?

If the call arrives at a moment when your guard is down, and everything sounds entirely plausible, falling for it becomes much more likely.

Even in such cases, operating systems like GrapheneOS can provide a higher level of protection, though not complete security. Avoiding suspicious links and not trusting questionable "support" teams remain the first-and-often only-line of defense.

How to understand whether a phone is infected?

The application can be hidden or seem something else, but it will probably use a lot of battery and, as mentioned above, we will install it ourselves, so we just need to remember whether we have been guided to install any application.

If you happen to notice any infection attempt, or if your phone has been seized by police, there's a network of people that is interested in analyzing potentially compromised phones. You can contact them through this mail: "cispiano@anche.no". Keep in contact with your trusted hacklab (because you have one, right?) as well.

Is it possible for the spyware to survive a factory reset?

Most likely no.

Is it possible for the spyware to survive a reboot?

Most likely yes.

2d. Imsicatcher – "Spy" Cell Towers

An IMSI catcher mimics a cell tower, tricking nearby phones into connecting to it. This allows it to intercept IMSI, IMEI, calls, messages, location data, and internet traffic, as well as enable machine-