

Surveillance and repression practices known in Bure

October 2025



Summary :

Table of contents

Summary :	2
I) Known monitoring method already used in Bure.....	2
Observation and monitoring mission +++.....	3
Police checks, police files, requisitions, prefectural decrees ++.....	6
Use of helicopters and drones +.....	8
Survey of local stores or administrations +.....	10
Requisition of phone operators +.....	12
Use of surveillance cameras +.....	13
Phone tapping +.....	14
Opening of postal mail +-.....	17
Searches +-.....	19
IMSI catcher +-.....	23
Use of undercover cops --.....	24
Proposal to become an informant --.....	25
GPS beacon --.....	25
Wiretapping of places --.....	26
II) Functionning of their monitoring.....	27
The "Cellule Bure".....	28
COSSEN and ODIINUC.....	28
Police files.....	29
Other files.....	30

Other files

FICOBA (Bank and Similar Account Files) is a tax administration file which lists all bank accounts (current, savings, etc.) created in France. It contains the identities of the holders (surname, first name, married name, gender, date of birth), information concerning the accounts held (establishment, number, nature, type) as well as the dates of opening, modification or closure of the accounts held. FICOBA does not keep balances or financial movements. (According to the CNIL, the files have 80 000 000 files)

it's stolen when it's not. The LAPI (Automatic License Plate Reader) is a tool equipped by certain cop vehicles which automatically detects registered plates.

In the FOVES file there are one or more service phone numbers to contact and instructions to follow in the event of discovery of the vehicle, for example :

*“Vehicle surveillance with control but without arrest.
Vehicles placed under surveillance throughout the national territory
Vehicle with occupants :
Report the presence or passage and discreetly identify the occupants.
Do not arrest the occupants for reasons other than those which motivated the check unless these people are the subject of active searches at the FPR.
Notify by phone the service that requested surveillance and confirm by report.
Vehicle without occupant:
Ensuring discreet surveillance for users identification
Immediately seek instructions from the service that requested the surveillance.”*

- **FPR** (Files of Wanted Persons). There are around 600 000 people in it, and it has lots of sub-files, some for people really wanted by the police, others for surveillance. Some examples : judicial control files (when a person has a judicial control awaiting trial and must not go to a territory or be in contact with a person). The S files (around 20 000 people registered in the file), which are the eyes of the intelligence, it gives almost the same information as said in the FOVES but for the person being followed.

I) Known monitoring method already used in Bure

This document was written primarily to inform those planning to remain involved in the struggle in Bure ; not all informations are fully explained.

Warning : The methods listed here pertain to what is known, either through judicial folders or observation, regarding police surveillance and repression methods. They are not exhaustive, contain errors, and it is highly likely that other methods are used by intelligence services or illegally, and are therefore beyond our knowledge.

Warning 2 : The examples of what is being monitored are frightening, but this has never stopped the struggle and will not stop it in the future. This inventory is not intended to neutralize the struggle, but to provide tools for reducing risks. Furthermore, surveillance methods have not necessarily led to prosecutions ; they may serve other purposes.

The methods have been ranked by frequency of known occurrence, using the following indicators : +++ daily, ++ weekly to monthly, + monthly or latent, +- periodic, related to surveys, -- a few known examples, seemingly rare. Sometimes several examples are cited in the same paragraph, but are not used with the same frequency.

Observation and monitoring mission +++

Known infos : a **squadron of 82 gendarmes** is permanently stationed here, providing a long-term presence alongside the local police. In addition to renovating the Gondrecourt gendarmerie, which will now have six holding cells, they plan to construct a €10 million building [by 2027] to replace the temporary modular units at the ANDRA laboratory, providing long-term accommodation for the gendarmes. Their mission is to patrol the various locations of opponents ; they have an address list, and upon arrival, they are given a tour of the different sites. They visit at least once a day, regardless of the time. During periods when they had orders for intense harassment, they visited every 20 minutes, 24/7. They are funded by ANDRA through an agreement¹. Within this framework of observation, there may be collaboration with urban planners or local councils regarding the design of public spaces. For example, the streetlights in Bure are never turned off at night so that opponents can be monitored. The number of gendarmes is increased during certain periods or events.

As part of their observation mission, they may decide to conduct spinning mills on individuals or settle into a hideout to prepare observation reports.

Their objectives :

- To record all license plates
- It depends on their current mission and their personal initiative. In the past, they were instructed to harass and provoke through constant police checks, insults, intimidation, and violence, which led to numerous lawsuits against opponents due to their presence. They had permanent warrants (requisitions) to conduct constant checks (which is illegal), and they contribute to the profiling through these checks or via license plates. In

¹ Each police officer costs ANDRA 447 euros per day : <https://bureburebure.info/a-bure-lagence-des-dechets-nucleaires-se-paie-des-gendarmes/>

COSSEN and ODIINUC

The COSSEN (Specialized Command for Nuclear Security) is a national unit attached to the Gendarmerie, which has 70 people : 37 gendarmes, 15 police officers, 18 civilians. It has several objectives (such as putting in place tools to carry out 470 000 administrative investigations per year of all people entering a nuclear power plant) including participating in the surveillance of anti-nuclear activists in France. It does intelligence work with the particularity of working in conjunction, or even being a client of nuclear authorities (ANDRA, EDF, Orano, framatome). Since April 2024, the COSSEN has been equipped with ODIINUC (Optimization of Data and Information of Nuclear Interest), which is an anti-nuclear file. It may contain a lot of information, some of which is very personal : particular physical signs, nicknames, family situation, psychological or psychiatric disorders, etc. Other data — “*link with extremist groups*” — can shed light on the political opinions of the person registered.

Police files

Many police files can be called upon in the context of a struggle :

- The **TAJ** (Processing of Criminal Records) is the largest police file with a third of the population in it, it includes : the identity of the person, their profession, their family situation, their nationality, their addresses, phone number, email address, their photograph, the facts with which they are accused, their physical characteristics, the dates of the alleged offenses, the data and images relating to these facts, etc. It concerns people suspected of having committed an offense as perpetrator or accomplice, as well as victims. When it includes photos it can be used for facial recognition.
- **FOVES** (File of Reported Objects and Vehicles) : It contains the registration plate, a paragraph of the reason why it must be monitored, the model and color of the vehicle, and technical information about the vehicle. It's the same file as stolen vehicles, so cops can sometimes think

II) Functionning of their monitoring

In this part, we will briefly see the Bure and anti-nuclear special investigation units (but do not address all the other gendarmerie / police / intelligence units which may be called upon in connection with the fight) as well as the main police files with which we may be confronted. It doesn't include intelligence files. It is possible to consult the brochure "The crazy desire to control everything" (present on infokiosques.net in french) for more precise information or for standard letters to make attempts to request consultation or deletion of files.



Bure cell logo

The "Cellule Bure"

On July 4, 2017, a national cell was created, the "Cellule Bure" (Bure cell), which saw up to ten gendarmes employed full time. The Bure cell of Meuse is located in Commercy, presumably at 19 rue de la Porcherie. The beginnings and certain members existed before the creation of the cell. They concentrate investigations linked to Bure and can travel to the other side of France on related cases.

The Bure cell is part of a larger coordination called "CNC-LEX national coordination cell" which liaises on several cross-related cases in France.

Some important gendarmes from the Bure cell in 2019 : Philippe Opigez, Christophe Ange, Frederic Menissier, Raymond Pfeiffer, Kevin Lescouarc, Philippe Robert

more recent periods, they seem to have been instructed to be more distant and discreet.

- Isolate the opponents from the inhabitants, the inhabitants being opponents or appearing with opponents are also subject to controls or intimidation, followed by the police or summoned to hearings. And at public events, they sometimes control anyone coming to the event well in advance on the roads (like for example at the Bure's lesques).

Apart from events, currently their instructions are rather to be distant and not to carry out too many checks, even if there are abuses from time to time.

Example, in the criminal association file :

"Continuing the ongoing investigation, an observation device composed of soldiers from the MEUSE gendarmerie group was set up on July 3, 2017 at 6:00 a.m. near the old station — D138 — commune of LUMEVILLE EN ORNOIS 55.

At 11:12 a.m.: arrival of a cyclist (precise description impossible due to the distance).

At 1:57 p.m.: the latter leaves in the direction of MANDRES EN BARROIS

At 3:17 p.m.: arrival of a blue RENAULT CLIO (illegible registration). 2 women get out.

At 6:26 p.m.: a man whose hair is styled in "drealocks" leaves the house towards the garden.

At 6:42 p.m.: a woman with "salt and pepper" hair walks around the field.

At 9:21 p.m.: departure of the RENAULT CLIO vehicle with the same two women on board, in the direction of MANDRES EN BARROIS.

Surveillance observation highlights very low attendance at this site (5 individuals).

The observation device is lifted on July 3, 2017 at 10:00 p.m.."

////

In September 2017, an investigating cop came across two people, one of whom was the subject of the investigation, during a private trip on the Paris-Meuse TGV train. So he followed them as they got off the train, on the bus to Commercy, then into the city until he lost sight of them in a street. Then 4 days later, in order to find his home, the cops decided to monitor the street in question for 2.5 hours, until they saw the person enter a building.

How to reduce risks ?

- Reflect before coming with vehicles with license plates in our names, parking them far away (difficulty : there is often a lack of vehicles in the area, contribute financially and mechanically to good quality collective vehicles?)
- Remind residents and elected officials that the presence of the police is harmful and violent for everyone, they can show their disagreement with the cops or show forms of support for the people being controlled.
- Hiding the license plate if it is on private land (and not on public roads), even if already registered, it will reduce the precise mapping of where each vehicle is located and make other hidden vehicles less suspicious. Be careful, however, driving or being in a public space with a hidden plate can lead to violent checks and fines.

Police checks, police files, requisitions, prefectural decrees ++

Known infos : 2 elements facilitate or strengthen controls :

- For several years, as soon as an event is publicly announced, a **prefectural decree** is published. Note that since 2025, there have been

Their objectives :

- Collect personal information
- By intrusive methods have the pressure of always being tapped.

How to reduce risks ?

- Pay attention to what people say in certain spaces.
- If people know about it, check the microphone/camera places

GPS beacon --

Known infos : In the criminal association case, GPS beacons were placed on 2 vehicles, geolocation officially lasts 2 months.

Their objectives :

- According to the file "The aim of geolocated tracking is to identify the drop-off points of X", they can complete this by profiling places of frequentation or identifying participation in certain actions/demonstrations of the vehicle (and potentially its owner).

How to reduce risks ?

- Look under cars, in gaps where something seems to have been moved.

- Keep in mind that vehicles often present in the area may at least be registered or subject to geolocation.

Wiretapping of places --

Known infos : In the criminal conspiracy case, the order was given in March 2018 to legally wiretap the Maison de Résistance for 1 month. The cops in their report said that this is not the right place to wiretap because the meetings that mainly interested them took place at Affranchie. It is not specified whether the house was wiretapped during this period or which room, nothing legally appears.

several events without any prefectural decrees. These authorize, over a given time (often the duration of the event $\pm$ 1 day), in given locations, the use of drones/helicopters and prohibit a certain number of items to be transported. For these prohibitions it depends on the decrees, for example the wearing and transport of pyrotechnic materials, fuel, spray paint, objects that could constitute a weapon, alcohol, sound equipment, etc.). Prefectural decrees are never strictly applied, but make it possible to legitimize abusive checks, and sometimes seizures of equipment (which can normally be recovered at the end of the decree at a designated gendarmerie).

- The **prosecutor's requisitions** make it possible to control passengers and search vehicles. They are usable in a specified period and space and the cops must provide the document. In the years following the eviction from Bois Lejus, requisitions were constantly published, which is not legal. Since legal recourses, they are published less frequently.

There were periods when controls regularly led to identity checks at the police station² (gendarmerie). More recently it happens but it is less frequent. When there are several people arrested at the same time, they are separated in several distant gendarmeries which generates transport logistics to pick up and support friends (because there is often only one cell by gendarmerie). The next Gondrecourt gendarmerie will have 6 cells.

Also there are several types of police files linked to surveillance in Bure, some can be linked to vehicles which can lead to their control throughout France as soon as police officers enter the license plate (or use automatic license plate readers). Others may be linked to individuals, and may indicate additional instructions related to control (See chapter II, the part on recording).

2 Period of intense harassment : between February 22, 2018 (expulsion from Bois Lejus) and March 19, 2019 :

- > 73 identity checks, most lasting 4 hours.
- > 25 police custody: 8 of 24-hour, 17 of 48-hour
- > 5 immediate trials
- > 2 pre-trial detentions

Their objectives :

- Show and make their presence commonplace, create confrontation, provoke
- Fuel police files on activists
- Arrest wanted people

How to reduce risks ?

- Train yourself on these questions. The brochure “Legal brief in Bure³” is more complete for this
- Go collectively to support controlled friends, or to checkpoints to make them leave
- Systematically request requisitions and check them before accepting checks
- Contest prefectural decrees with lawyers via associations or inhabitants
- Use collaborative software to indicate where the police are located (the best known is Waze unfortunately (because it belongs to Google) it can also be via an infotrafic phone).
- In the case of seizure, collectively take charge of recovering the material at the end of the order, even if the material can only be recovered with personal identity cards.

³ <https://bureburebure.info/en/brief-legal-en-contexte-burien/>

- Compartmentalize discussion topics that are open to people passing through with fewer bonds of trust
- Document and disseminate known cases of infiltration.
- Stay welcoming and open! At the same time, train yourself to think about creating bonds of trust between people⁴.

Proposal to become an informant --

Known infos : Several people have had direct or indirect offers to become an informant in exchange for money or to obtain a protected status from the cops, either executives with pressure, such as searches, or people who had problems with the police, the latter offered them to go to Bure as an informant. We also know that they can subsequently summon people who have broken away from the struggle and are in a situation of psychological fragility to gather information. An informant unmasked in Paris had come to Bure several times between 2023 and 2025⁵.

Their objectives :

- Obtain internal information
- Stir up paranoia

How can you reduce risk ?

- Train as many people as possible in anti-repression and how to react to police custody. Help each other as much as possible.
- Document and communicate about this type of practice.

⁴ Discussion paper on this subject : Confidence, Courage, Connection, Trust. A proposal for security culture : <https://infokiosques.net/spip.php?article2072>

⁵ See the infiltrator database on this case : <https://www.notrace.how/infiltrators/>

Their objective :

- Identify more precisely the phones used in the Bure fight or at an event. In the criminal association file, an IMSI catcher was used close to all locations early in the morning, the official reason being that since the first searches many opponents had changed their phone numbers.
- Know who communicates with whom.
- Have a geolocation of people with a phone.

How to reduce risks ?

- Leave your phone at home, or turn it off as often as possible. Turn on a specific phone for events likely to be monitored.

Use of undercover cops --

Known infos : Cops have infiltrated demonstrations several times, we do not know the exact frequency.

Their objectives :

- Have internal information
- Stir up paranoia

How to reduce risks ?

- Question people who have shady attitudes (if they have links here, etc.). Be careful, this subject is complicated, we can quickly lose inclusiveness and be violent for people. A shady attitude can only come from people who have different codes!

Use of helicopters and drones +

Known infos : During the occupation of Bois Lejus, the helicopter could be taken out every day. Today drones, helicopters and private surveillance planes are used more during events or on one-off missions and fly over places recognized as opponents for extended periods (sometimes at 3 am). Legally there should be prefectural decrees which authorize, specifying places and times where these tools can be used. In practice they rarely respect this.



Private plane used for surveillance of the Bure struggle

Their objectives :

- Count the opponents, sometimes accompanied by a thermal camera, photograph/identify them. Helicopters have sufficient photo quality to read a license plate on a private land

- Drones are more discreet but require cops within range to use them. The helicopters are more visible in order to maintain pressure

How to reduce risks ?

- Document, take photos of helicopters at times when they are not allowed.

Survey of local stores or administrations +

Known infos :

* After each action, a police investigation is carried out, visiting numerous businesses. Example : after a demonstration, they went to see pharmacies to find out the vital cards and the prescriptions (and the name of the doctor who prescribed) of people who bought medical equipment. They contacted the firefighters who gave them the entirety of a phone call made about an injured person, as well as the file of the person who had been to the hospital. After an action involving the construction of a concrete block wall, they went to see the local material stores to find out if people had paid for a quantity of concrete block. The post office was asked for images from surveillance cameras and information regarding a letter posted, it is in fact stamped with the day and place of departure of the mail.

Conversely, structures can quickly call the cops when it comes to opponents. For example, the manager of Super U (supermarket) called the cops because opponents bought large quantities of methylated spirits, he provided them with the buyers' license plates.

* When there are investigations into people or associations in particular, administrations such as the CPAM, taxes, phone subscriptions, email or internet servers (not militant), banks, the Gondrecourt notary, tax information may be asked to have personal data (identity, phone numbers,

users have carried out searches from the machine : games, TV series, pornography, etc."

Info : There may be additional investigations linked to the discovery of informations on a computer.

How to reduce risks ?

- Before : do some spring cleaning of what we don't want lying around in documents, on computers. Encrypt all digital data and turn off devices in the evening.
- Before : make backups of our data and what could be stolen and put them in other places.
- During : be trained on searches to know what is possible during (know the legal frameworks for searches, put pressure on to have justification for what is taken, etc.)
- After : take care of yourself and others, foster solidarity above all (support people who have experienced this, help buy back stolen equipment, etc.).

IMSI catcher +-

Known infos : An IMSI catcher is a fake relay antenna through which phones pass. It allows, over a distance chosen by the cops, to know which phone is on and communicating with which other. It can also view "clear" text messages. IMSI catchers were used twice in the criminal conspiracy case. We suspect that IMSI catchers were used more often in the context of intelligence, probably at each major event.

activity appears to have occurred after February 2015."

Example on a series of photos found on a computer :

"We analyze the visual content and also use the EXIF metadata of the 11 318 files including 10 386 images and 932 videos.

We specify that all EXIF data (device brand and model, GPS coordinates, etc.) are easily configurable and modifiable elements.*

These elements are therefore useful but must be verified.

In the event that a photographic device held by the accused corresponds to one of those listed in this procedure, it would be appropriate to request a comparison from the Signal-Image-Speech department of the IRCGN capable of confirming that a device can take a photograph."

The photos are classified :

"293 files with Gendarmerie personnel, 102 files presenting either remains of grenades used to maintain order, or material made by the Zadists to participate in demonstrations (helmets, shields, etc.), 265 files whose faces of people can be exploited and could be part of the Zadists or at least supporters, 67 files made during gatherings in Germany, etc."

On these photos, the metadata reveals 44 models of devices that took the photos, including 16 serial numbers, 5 names of device owners. "Open source*" searches are carried out for the names found.

Then searches are carried out on the serial numbers on the internet which do not have the name of the owners to find other photos having been taken with these same serial numbers. Several websites were found that posted other photos that had the same serial numbers. It is specified: "The account holders <http://zopiaz.tumblr.com/>, <http://taipeimevoila.tumblr.com/> and <https://www.flickr.com/> are identifiable by judicial requisition to the companies Tumblr and Flickr." Other photos were taken with the same camera as photos taken on Reporterre (a media). A screenshot is taken of the trombinoscope of the reporterre.net site of the journalists of this site.

Some examples of delving into people's private lives :

"We found an Email messaging service for the XXX account containing 9 315 messages. These are messages relating to theater, reports, discussions on work in the Bure house, articles on CIGEO, etc.

We have not found any messages relating to the facts of this instruction."

On another file :

An example of profiling : *"The variety of navigation suggests that several*

address provided, bank statements, digital copy of checks issued to know the recipients, etc.).

* List of administrations contacted and what they provide :

CAF : history of CAF tracking (previous department), home address, phone and email, benefit amount, bank details

URSSAF : the information collected refers to the periods of hiring and gives the identities of the employers. Several times, requests will be sent to employers in order to obtain additional information on the employees hired (phone contact...)

SIV (Vehicle Registration System), allows cops to recover the identities of vehicle owners.

The post office : The cops send requests to the post office to obtain the list of packages received and sent to a particular address. There is no response in the folder. They do the same to find out if there are mail redirects for a person.

EDF (french electricity) : The cops send requests to EDF to obtain the volumes of electricity consumption as well as the contract information (holder...) for certain collective places. The answers are not in the folder.

Their objectives :

- Distance the businesses and administrations from the opponents. These types of operations in the countryside can sometimes scare stores, which tell themselves that the opponents are criminals and not frequentable, and they can spread that to other people. Several times police investigations have led to consequences : banks suddenly prevented access to their accounts to associations under improper pretexts, and people were subjected to administrative controls or withdrawals of social benefits.

- Collect personal information to incriminate or complete a profiling of activists.

How to reduce risks ?

- Choose friendly shops or places if possible, or find out about the structures that have collaborated more easily in the past. These operations are less carried out on people closer to us, cause cops are not immune from the dissemination of information about ongoing investigations, making them less effective.
- Give only the strict minimum of information to structures that identify us. Don't give your phone number, avoid paying by credit card, don't go into stores equipped with cameras, etc.

Requisition of phone operators +

Known information and their objectives :

- Requisitions can take place on a particular antenna at one time ; this allows you to identify all the phones that are on and are communicating with that antenna at that moment. We don't know exactly how often, but it's practiced at all important events, and it allows them to discreetly know who is there (number of people and identities). They collect phone numbers and physical identifiers of the phone at the same time ; from this, they can know within a few hours the identities linked to the number, or the other SIM cards connected in the past to the same phone (or other phones used with that SIM card). This is not very expensive for them to carry out and the operators respond quickly. They also get numbers of people present in the village / surrounding area, but it gives them a good basis for work.
- They can also do a survey of a particular person, for example to obtain their "detailed invoices" (FADET). The accounts mention the numbers, dates, times, and communication durations. With FADET, the operator, and therefore the police, knows exactly which phone is sending text messages

of a computer.

- The documents which are classified into categories : E-mail, contacts found for example in thunderbird, visible traces of internet browsing, file searches by key words (ranging depending on the computer from 5 key words to more than 80 such as names of people either "victim" or "interesting person", or village, or "Action, ANDRA, Owl, Bindeuil, Fire, demonstration, ZAD...")
- Videos and images of several types : those taken during demonstrations, but also photos of families, classes or on vacation between several people of the fight to show links between people. It is appreciated when faces are recognized "However, many files allow faces to be seen in a way that can be used by facial recognition software without necessarily having a link with the fire or the information in progress.". On quantity documents, these documents are classified by category :
 - Political documents: anti-cops documents, those linked to the fight against CIGEO or nuclear power, etc.
 - Documents bearing administrative identities.
- The presence of encrypted files.
- In the documents, metadata is sometimes consulted, in particular the name of the owner of the document as well as the dates of the last modification of the documents. For photos, the metadata is searched for the Brand, Model, Serial Number, Author.
- Research on software : installed software (in particular security tools such as VPNs, Tor, metadata deletion or password management tools), Firefox forms which sometimes include phone numbers, a date of birth etc.,
- Addresses that have been visited on the Google Maps application
- Deleted documents ("Carving*" method)

Are taken into account :

- All visible data,
- Hidden files,
- Traces of deleted files
- Keywords typed into the search engine (in a folder, that's nearly 900 keywords), browsing history (in that same folder, 44 000 URLs). A classification of the most visited sites can then be made.
- Emails present in messaging systems
- Files present in a folder that lists what was printed from this computer (present on some systems in \var\spool\cups). This presence of files can be an element of accusation of the owner of the computer as the author of the text.
- Periods of hard drive activity or changes in file usage. To allow us to see if the computer was used over the period of interest to the investigators. "No

Searches +-

Known infos : Linked to the Bure struggle, around forty searches took place in the past (not only in Meuse, but elsewhere in France, and also in Germany). They were able to coordinate up to 14 simultaneous searches at several locations in Meuse/France (with up to 200 police officers at 6 am). As these are aggressive interventions, they are practiced rather during specific periods of repression and often in a raid (several places at the same time)

Their objectives :

- Collect personal information and anything that would allow people to be incriminated as part of an investigation
- Legal theft, many materials have never been returned.
- Violate and disgust opponents (brutal awakenings at 6 am can cause trauma)

Concrete example in the criminal association file

During the first search on September 20, 2017, 60 digital media (24 computers, 13 telephones, hard drives, USB sticks, cameras, mp3, SSD card) were analyzed for an initial estimate of 33 000 euros.

What is being sought in this computer investigation ?

In "preliminary analysis", on computers, cops can look at and classify information into this range of choices :

- Technical information related to the computer. This information can possibly be used to trace the use of the computer on the network : the partitioning system, the digital environment (analysis of the hard disk, date of the last updates and date of creation of the operating system, operating system used, partitioning system, the different accounts placed on the system, admin or session passwords, the timestamp of the system in particular its difference with legal time, etc.), extracts any type of information which can identify the owner

to which phone number. It seems that when it comes to exchanges using data (Signal for instance), the operator only knows that data is being used, but not for what purpose. When the phone communicates (sends SMS, calls, data), the operator also records the antenna that was used and which can be requested by the cops giving an approximate location afterwards. The cops can also request a more precise real-time geolocation.

Their objectives :

- Know who is where
- Discreetly identify opponents who have a phone in their name
- Make link graphs between people

How to reduce risks ?

- Train yourself, for example, by reading and disseminating "Mobile telephony : Surveillance, repression, risk reduction" present on infokiosques.net (in french)
- Use encryption tools, don't always pick up your phone, be careful about what you communicate via this tool : no name / description of what is happening. Assume that in a clear communication one of the two phones can be listened to by the cops.

Use of surveillance cameras +

Known infos : There are many high-performance cameras around the ANDRA lab, and many towns are increasingly equipping themselves with cameras in the Meuse.

Boxes that take photos with motion detectors connected to a SIM card were found in the forest. We found some among pro-CIGEO people, showing the active collaboration between the cops and the defenders of the project. Elsewhere in France, we found such boxes installed for simple support evenings for Bure. We sometimes see cops or security guards looking for equipment in areas facing the events.

Their objectives :

- Mapping movements

How can you reduce risk ?

- Map the cameras and send their GPS coordinates to bureburebure@riseup.net (with a photo of the camera if possible), consult where the cameras are on map.bureburebure.info.
- Take legal action against cameras installed without declaration or destroy them.
- Fight locally against video surveillance to limit their diffusion.

How does it work ?

- The cops ask the post office to set aside certain letters sent to targeted addresses and agents come on fixed days to consult the letters, to hold them before they are sent. This can be done in 2 potential locations :

- For some towns, in the Ligny-en-Barrois post office center : 58 Rue du general de gaulle 55500 Ligny-en-Barrois
- At the Grand-Est sorting center : Pic Loraine Pagny-les-Goins, distribution service : Route de l'aéroport, 57420 Pagny-lès-Goin

Their objectives :

- The fact that it is ostensibly open serves to put pressure on and to disgust the opponents of living here. There are indeed discreet opening techniques that are difficult to discern (techniques that are easy to find on a search engine).

- Collect personal information

How to reduce risks ?

- Document and share knowledge of letters deliberately opened (if the postman mails such a letter, have them sign a document attesting to the state of arrival of the document), or with suspicious delays. Possibly take administrative/judicial recourse to the deliverers/post office who provided mail whose “integrity or confidentiality” of documents has been breached. Several steps are possible (with potential help from unions, or recourse to administrative courts). For example, a letter in 2022 was sent to several postal authorities on these issues to trigger an internal investigation.
- Put pressure on structures collaborating with the cops.
- Be careful what you send by mail. Provide people who want to write us private letters with addresses that are less likely to be under surveillance.

Opening of postal mail +-

Known infos : Several places (collective places or shared accommodation – at least 8 places have already had this type of problem) have suffered extreme package delays, arrivals of letters that are visibly open, or, more rarely, whose contents have been partly looted. The most targeted letters are personal letters written by hand (more than letters from administrations). Once a package of brochures arrived a month late, the box was opened, 3 brochures were missing from the lot.



A package arriving at the Maison de Résistance

Phone tapping +

Known infos : During the investigation for criminal conspiracy, 29 phones were officially tapped, and more than 85 000 conversations and messages were intercepted. Legally, phone tapping must be requested by the investigating judge for a period of 4 months, renewable. The maximum was 330 days. This does not include phone tapping for intelligence purposes. All “clear” content (text messages, phone calls without end-to-end encryption application) can be perceived by the wiretapping, but not retrospectively : the cops must decide to wiretap a phone before to listen to it.

Their objective :

- Incriminate people based on facts, understand local modes of organization.
- Collect important personal information to put pressure on. Even if it cannot be legally used in a trial, wiretapping can put pressure on people in police custody to make the person break down.
- Generate significant stress from feeling watched all the time.
- Make organizational methods more complicated.

How does it work ?

In the criminal conspiracy case, the cops used a lot of interception of communications in real time over many months. The cops then transcribe the calls and text messages that interest them on paper (sometimes cut off by “inaudible conversations” or “not of interest to the current investigation”). This work is an intrusive investment for the cops, at any time they can pick up their phone connected to the person being tapped to follow what is being said. The wiretaps will be used to identify possible

order givers, people with influence on the fight or to establish links between people.

What is particularly broadcast :

- Everything that allows you to link nicknames to civil names (especially on collective phones). For example, after cross-referencing a phone number with a real identity via identification with an operator, a conversation heard : "hi, is it *nickname*?" "Yes, it's me" allows the cops to formally link a nickname to an identity. This will also allow them to link emails using these nicknames to real identities.
- During an investigation, when there is the same cop doing the wiretapping, they can identify certain people from the sound of their voice.
- Anything that allows nicknames to be linked to a function/role in the fight. For example, text messages asking a person to publish a text on the internet are enough for the cops to assert that the person receiving the text messages is responsible for site administration or communication around the fight.
- Analyzes of actions that can be discussed, for example in conversations with journalists who ask questions about what the person thinks about a particular action.
- The relational links that may exist between people as well as the mental state of people
- The places frequented by people on the phone (particularly militant places or when people go to actions but also touristic places, family places). It is used several times to confirm that people are indeed present at demonstrations.
- Information related to demonstrations (the course of this one) or to the cops, for example if there are people injured

- Everything linked to conflicts between the different components/people of the movement (useful for pitting one against the other or identifying who/how to make people speak)
- Anything related to action logistics, or what could be interpreted as such by the cops on the phone
- Everything allows the cops to identify the decision-making areas of the fight (meetings, general assemblies, etc.)
- People's concerns about material seized during searches

How to reduce risks ?

- Assume that a conversation between two opponents' phones can be tapped, and be careful about what is said, especially when talking about other people.
- Do not gossip, do not talk about internal conflicts, or about the way events are organized or about non-public structures.
- Train yourself to use encrypted communication tools (signal, secure or even encrypted emails) or learn to make appointments to talk to each other in person.