Policing the radio-frequency spectrum: Unintentional interference and jamming — Are the security of the spectrum, cybersecurity and electronic warfare a single combat?

Catherine Gabay,
ANFR

Abstract:
Unintentional interference on radio frequencies and deliberate jamming are dangers for the economy and state on par with menaces from cyberattacks. The frequencies undergoing interference can hardly, or not at all, be used in the zone affected, and this jeopardizes all sorts of applications. The security of the radio-frequency spectrum is a matter of sovereignty. To prevent and handle cases of interference, a police is needed. The Agence Nationale des Fréquences (ANFR) has this role among its assignments for overseeing the spectrum: more than 1400 cases of prejudicial interference are reported to it each year. To cope with trends in technology and uses, the ANFR is continually bolstering its means and methods of control; and it advocates making all users aware of issues related to the security of the spectrum.

The radio-frequency spectrum is the set of frequencies between 9 kHz and 3000 GHz. This strategic resource is invisible, immaterial and scarce. It is shared by various services: broadcasting, fixed and mobile services, terrestrial radio determination (localization services), radio navigation, experimental stations (research), radio astronomy, etc.[1]

Regulating the spectrum

International and national regulations ensure an efficient use of the radio-frequency spectrum and a harmonious cohabitation of these services in this limited space. The International Telecommunication Union (ITU) is in charge of regulation at the international level. The ANFR (Agence Nationale des Fréquences, a public administration under the minister of the Economy and Finance) is in charge of planning, managing and controlling the spectrum in France. In the newspaper *Ouest France* on 26 April 2015, a journalist described the ANFR's role as the "*conductor of an orchestra*" and added "*This wide spectrum is shared between various users […] Like on a wide superhighway where everyone has to drive in his lane, the users must not trespass on neighboring bands. The Agency does everything so that frequencies not enter into conflict with each other.*"

[1]This article, including quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in November 2020.

Policing the spectrum

To enforce the laws and regulations governing the use of the spectrum and intervene in case of violations, a "police of the radio waves" is necessary. In France, this duty falls on the ANFR as part of its role to manage and control the spectrum.

Figure 1: The ANFR is present throughout the country to perform its duties as a police of the spectrum.
Source: ©ANFR

The ANFR's controllers are sworn in and certified. They have a power of inquiry for investigating and notifying violations of the legislation on radio communications. They also intervene as experts during criminal investigations; and public authorities may, under exceptional circumstances, requisition their services.

The words used in the press to describe the role of these controllers and their assignments are telling. The ANFR has been said to be the "*gendarme of the frequencies*" (Tony Robin in *L'Est Républicain* in 2019), the "*police of the frequencies*" (Romain Bosso in *L'Express* in 2019), the "*gendarme of the radio waves*" (François Chrétien in *Ouest France* in 2017); and its agents have been called the "*guardians of the spectrum*" (Ghislain Utard in *L'Est Républicain* in 2017). The investigations conducted by the agency have been described as "*literal detective work*" (Olivier Berrezai in *Ouest France* in 2019). Already in 1998, these controllers were said to be "*keen sleuths*"; and the Direction of Control of the Spectrum, a "*spearhead squad*" (Jérôme Dupuis in *L'Express*).

Defining interference

Interference occurs when the electromagnetic energy of radio transmissions, whether by radiation or induction, hinders, interrupts or alters the operation of transmitting and/or receiving radio stations. The ITU has defined harmful interference as "*interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations*".[2]

Interference has quite different causes, voluntary or involuntary, ranging from signals from unauthorized sources or faulty equipment to parasitic signals generated by electric, electronic or radio equipment that is too old, poorly regulated or not in conformity with regulations. In effect, parasitic emissions represent 25% of the annual number of cases of interference investigated by the ANFR. Interference on a frequency band hampers or even halts all uses of the band within a given area. All sectors and domains, not just radio services, might be affected, including services critical to safety and security — with the risk of jeopardizing lives or wreaking damage to the economy. Some radio systems are more vulnerable than others, since they depend on being able to detect weak signals.

A distinction is made between deliberate and involuntary interference. Interference caused by parasitical emissions from an old machine is deemed unintentional. On the contrary, using a jamming device is an act of deliberate interference. Interference might also be qualified as motivated by deception — what is called baiting or spoofing — a deliberate transmission of misleading, aggressive signals. "Offensive actions" are a category of voluntary interference that seems well suited to qualify the use of jammers or hostile denial-of-service attacks on satellites or television services when the motivations are geopolitical or economic.

The fight against unlawful interference

The ANFR is active in the fight against the proliferation of illegal jamming devices that target global navigation satellite systems (GNSS, such as GPS, Glonass and Galileo). Protecting the signals from systems of geolocation by satellite is crucial, since these systems are essential to an ever growing range of uses, whether for precisely positioning satellites or synchronizing their time systems.

According to the Code of Electronic Communications (CPCE), a jammer is a "*device for making machines of electronic communication of all sorts nonoperational for transmitting or for receiving*". This box with one or more small antennas, depending on the targeted frequency bands, normally works by transmitting a signal stronger than the useful signal so as to cover it up. French law has pronounced a general prohibition on jammers (importation, advertisement, transfer of ownership whether for free or at a price, distribution, installation, detention and utilization). It provides for a penal sanction of up to six months of incarceration and a fine of €30,000. The state may be dispensed from this general prohibition for needs related to "*public order, defense and national security, or the public service of justice*".

[2] Chapter 1, Section 7: ITU (2016) *Radio Regulations*, 4 volumes (Geneva, CH: ITU) available at http://www.itu.int/pub/R-REG-RR-2016.

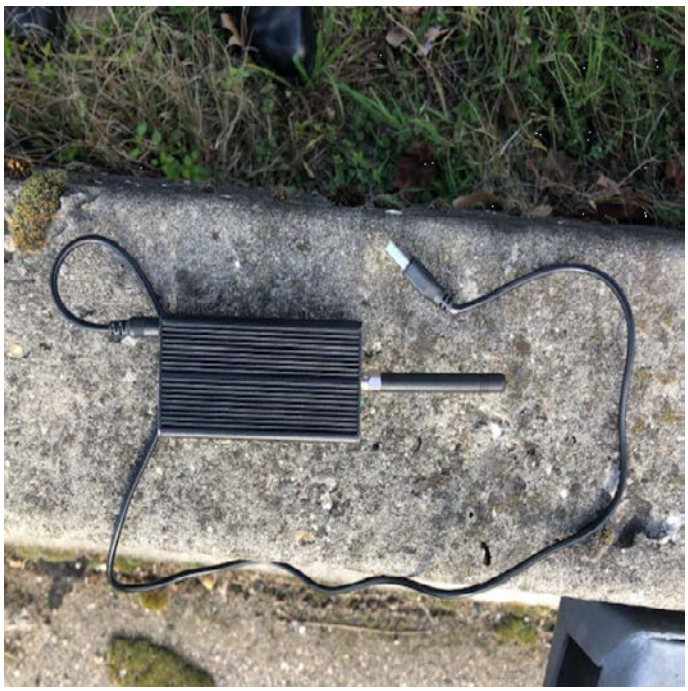

Figure 2: A GPS spoofing device seized during an intervention by the ANFR.
Source: ©ANFR

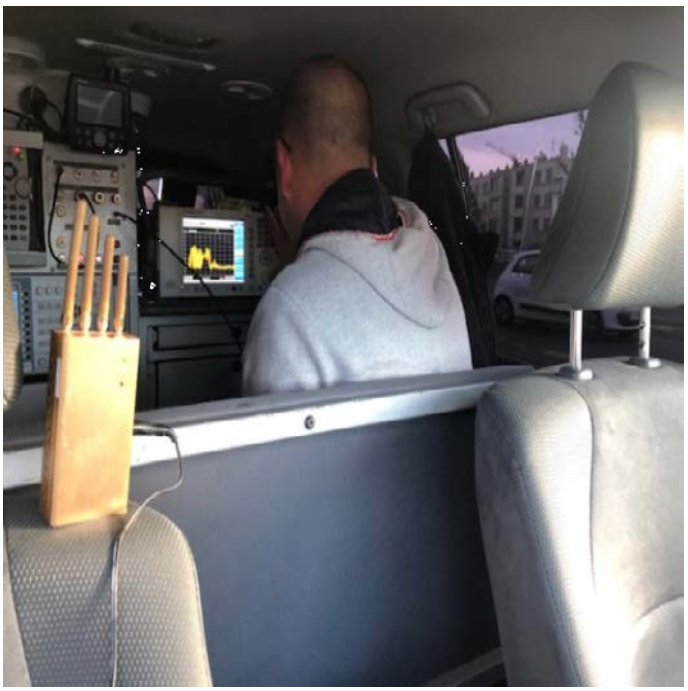

Figure 3: A multi-band jamming device analyzed in a laboratory vehicle of the ANFR.
Source: ©ANFR

Jamming devices ever more often figure in the arsenal used by criminals. The use of a jammer can have serious effects on security and safety, owing, in particular, to their collateral impact on a much larger zone than imagined. For example, a jammer that prevents using mobile telephones in a classroom can interfere with phones in the neighborhood; and a GPS spoofing device used by an employee who does not want his employer to geolocate his truck can disturb the flight of airplanes at an altitude of 2000 meters or the GPS of vehicles parked 500 meters away. Mention might also be made of VIPs who want to ward off paparazzi drones by using jammers powerful enough to broadcast signals over a wide area. For this, the owner of a luxury hotel on the Riviera imagined installing a device for jamming GPS radio waves.[3] In the past few years, the number of cases investigated by the ANFR that are related to small GNSS jamming devices has increased. These devices are now a cause of concern.

The ANFR is very active in the fight against jammers. The user of such device feels he is invisible to his boss; but he is not invisible to the ANFR's controllers. Several users of GNSS jamming devices have, in recent years, had their vehicles intercepted and been arraigned following operations conducted by the ANFR. Such operations involve using innovative detection devices and cooperating with the police.

[3] A case cited in Elisa BRAUN (2018) "La chasse aux drones, le sport de l'été", *Le Figaro*, 31 August.

The detective work of investigating interference

Cases of interference — once reported to the ANFR: approximately 1,500 cases per year — are investigated in the field by the agency's controllers. They are equipped with sophisticated equipment for detecting, identifying and locating sources of interference. In some situations, devices are installed on location for the time needed to fully identify the interference. Once the equipment causing the interference and the persons responsible have been identified, the ANFR notifies instructions for putting an end to the interference. It may also give notice of a flat tax of €450 to cover the cost of its intervention. When it decides to hand the matter over to the courts, it writes a report of the violation and forwards it to the public prosecutor's office. ANFR agents may, if needed (for example, to seize contentious radio equipment), ask for support from an officer of criminal investigation. On authorization from the president of the competent court of first instance, the agents may themselves seize equipment. Most cases of interference are, however, settled out of court.

Figure 4: Measurements to investigate interference.
Source: ©ANFR

Preventive actions

To prevent the interference caused by noncompliant equipment or uses, controls may be performed on location and in the radio equipment market. Since protecting the spectrum is partly based on following the conditions set for using radio frequencies, one axis of the ANFR's work is to conduct information campaigns to make stakeholders aware of these issues.

Figure 5: A poster for an information campaign on the risks related to GPS spoofers.
Source: ©ANFR

Figure 6: A brochure of information on wireless networks (RLAN and WIFI).
Source: ©ANFR

Cybersecurity, cyberdefense and electronic warfare: The same combat?

The police of the spectrum should (unfortunately) have no complex of inferiority with regard to cybercriminality.

Wireless connections, despite their advantages, also have drawbacks that can become a target for attacks. The threats are real even though the public, apart from a few groups of experts, are not yet aware of them. Unlike most cybercriminal attacks, many of the cases of interference investigated by the ANFR are not intentional and are not reported in the media. The situation is changing however, following the recent publication of a few articles.

In fact, attacks on the radio-frequency spectrum are no less serious than attacks on information systems or acts of electronic warfare. Interference inhibits the use of the air waves and can result in a denial of service. In addition, baiting operations might compromise the integrity of the information conveyed. The three concepts fundamental to the security of information systems are confidentiality, integrity and availability. For several applications and in many sectors however, the availability of the system under attack is an issue that overrides confidentiality (or authentication). Furthermore, even if interference might not be intentional, this is no reason for reassurance since the effects of interference, whether from an attack or not, are the same. Besides, the ITU does not make a distinction between deliberate and unintentional interference when it is harmful.

Like cybersecurity and the security of information systems, the ANFR's policing of the spectrum is an aspect of digital security and, more broadly, of the security of both the economy and state. In recent years, our understanding of cyberwarfare has grown. We must also become more conscious of the need to police the spectrum and protect radio frequencies.

Maintain and reinforce the capacity for responding to interference

The importance of policing the spectrum means maintaining and reinforcing the means of action. The ANFR has tried to do this, among its efforts: the prospective analysis of menaces by monitoring technological and societal trends and through regular exchanges with the competent authorities; repeated comparisons of methods with those used by equivalent organizations at the international level; long-term investments for modernizing equipment and methods; the ongoing training of the specialists who use this equipment and apply these methods; and, finally, the vigilance for seeing to it that the legal, regulatory frameworks (national as well as international) continue providing the legal grounds for acts of prevention and, in cases of violations, repression.

In addition, the ANFR fosters partnerships and operational actions between administrations so as to bring together skills and qualifications, competence and expertise.

Involve all users in limiting interference and its effects

Everyone has to be as cautious with the air waves as in the digital realm or in 3D-space. Educational efforts about using radio frequencies must be pursued.

For the most critical uses, it is essential to foster resilience (robust equipment, redundancy, the capacity for operating in a downgraded mode, etc.) and favor the return to normal.

Detect and report harmful interference so as to improve security

Detecting harmful interference might not prevent an attack from happening, but it is the first, indispensable step toward solving the problems caused by interference. Detection work provides the grounds for interventions by the police of the spectrum and for responses to the situation. The public authorities and administrations competent for managing the spectrum, mobile operators and many other entities are already highly vigilant and regularly reinforce their capacities for detection. However this is not necessarily the case of other users of radio frequencies, who are less specialized but for whom the spectrum is or will be a critical asset (*e.g.*, driverless vehicles, smart cities, connected health). These users must "mature" in matters related to radio frequencies and learn how to recognize harmful interference when it occurs. This might require installing specific pieces of equipment on location.

Detection has to be followed up with reports of the interference to the ANFR. Not only does this enable the agency to intervene and eventually settle the problem of interference and sanction its authors, it also helps us better measure the phenomenon of interference and thus build up our knowledge. We can thus maintain and reinforce our means of protection and defense.