From HF in AM to Digital Networks: The Evolution of Military Radios, Between Technology and Operational Reality

Published on 25/01/2026

Today, as in the past, radio remains one of the central channels through which decisions and coordination pass: technology evolves, but the essence does not change, because in the field, connectivity is the condition that makes **maneuver and command** possible.

Until the 1990s, this truth was clearly visible in operational choices: over long distances, **HF in AM/SSB** was often used, while **FM** was the most natural tool for short-range communications. It wasn't a matter of “old” or “new,” but of **propagation**, **orography**, **available power**, and, above all, **reliability** in not always ideal conditions.

During that period, networks were “simpler” in structure but required solid skills. HF, with its limitations (noise, fading, variability linked to time and ionospheric conditions), allowed covering distances that VHF/FM could not guarantee. FM, on the other hand, offered superior audio

quality and more immediate management but remained bound to line of sight and thus primarily for tactical, local use. In between were **procedures**, **radio discipline**, and **good practices** that often made the difference between a connection that held and one that “dropped” at the crucial moment.

In practical terms, from **the post-World War II period until the 1990s, the evolution of military radio communications was more incremental than revolutionary**. Reliability, robustness, power, and standardization improved, but **the fundamental logic remained the same**: **HF** for long-range, **VHF/FM** for tactical, with a strong emphasis on the operator's experience.

The real discontinuity comes with **digitalization** and “network” management, which changes not only the equipment but also the way of conceiving **C2**.

In the 1980s, the Italian Army also used nationally produced analog devices, such as the ER 95-A/I (RV3) in vehicular configuration, fully integrated into tactical unit networks before the introduction of new generation digitalized systems - Photo Radiosurplus Elettronica

Security as an "optional"

Historically, communication security **did not originate as an automatic requirement**, but as a problem to be managed.

Already in **World War I**, when radio and field telephones began to be used on a large scale, traffic protection was almost exclusively entrusted to **codes, manual ciphers, and procedural discipline**. Technology transmitted; security was entrusted to humans.

During **World War II**, the situation improved but did not change in substance. More advanced encryption systems appeared, but they remained **complex, bulky, and limited to specific command levels**. In most cases, security continued to rely on procedures, code rotation, brevity of messages, and operators' ability not to “say more than necessary.”

This approach remained essentially valid even in the post-war period and throughout the Cold War. Until the 1990s, in many operational configurations, encryption **was not native** or not always available: dedicated modules and key loading tools, depending on equipment and missions, could be present or not.

The radio still worked, but **security was not guaranteed by default**.

Consequently, traffic protection did not depend solely on hardware. **COMSEC procedures**, rigorous key management, disciplined use, and coordination between network stations were crucial. A human error, a skipped procedure, or imperfect synchronization could nullify any technological advantage.

In other words, technology mattered, indeed, but it mattered just as much **how** it was used. A lesson that, decades later, remains surprisingly relevant.

In the 1980s and 1990s, encryption was not always native: in NATO contexts, external COMSEC modules like the KY-57 VINSON (pictured) were used, also by the Italian Army in specific operational contexts - Source Crypto Museum

The turning point: digital systems

At the beginning of the century, with the introduction of the first tactical digital systems and the progressive spread of the **SINCGARS** family, the change was not only technological but above all **methodological**.

Frequency hopping, a more structured network management, and greater attention to **protection** imposed new operational standards, changing the very way of planning and conducting tactical communications. The radio was no longer just a device to “turn on,” but a system to configure, synchronize, and manage within a network.

At the same time, however, an increasingly large part of **C2** began to rely on complex architectures: **data networks, relays, SATCOM, integrated command and control systems**.

The result has been an enormous growth in capacity, but also an increasing dependence on infrastructure.

The SINCGARS used by the Italian Army between the late '90s and early 2000s were based on the AN/PRC-119 family and the corresponding VRC vehicle versions. In the equipment, they were identified with codes like "635" or "637", which indicated the operational configuration of the asset. In the photo, a "635" in vehicle/command post setup, with side-by-side modules and external encryption: not a different radio, but a more complete configuration of the same system, adapted to the operational context - Photo by flickr

Towards the future with a look at the past

It is here that, in recent years, many armies have pragmatically returned to looking at what does not depend on space and "long" technological chains. In modern scenarios, especially high-intensity ones, the **electromagnetic domain** is no longer a background context, but a

real field of confrontation: **interference, jamming, GPS degradation, network attacks, and loss of connections** are no longer remote hypotheses, but operational conditions to be considered from the planning stage.

This battlefield is often linked to the **cyber domain**, because today a significant part of communications depends on **digital networks**, protocols, software, and key management. On the ground, however, the operational effect arises from the intersection between the **electromagnetic spectrum** and **electronic warfare**, that is, from the physical context in which those systems operate and are contested.

Modern communications are not just "radio" nor just "networks": they are **digital systems traveling on the spectrum**, and can be hit both on the physical level, interference, jamming, spoofing, and on the logical level, service degradation, node compromise, alteration of information flows.

It is in this overlap zone that the loss of a connection, even without a single shot fired, can produce immediate effects on **command and control**.

When digital connectivity degrades or is interrupted, a reality emerges that those who operated thirty years ago know well: an **essential, resilient, and replicable** communication capability is needed, even in the worst conditions. In this context, **HF**, with updated procedures and more modern technologies, continues to represent one of the pillars of **real fallback**: not a return to the past, but a concrete response to the fragility of more complex architectures.

In thirty years, therefore, not only have the devices changed. The way networks are built, security management, the philosophy of **C2**, awareness of electromagnetic risk, and, more generally, the way of fighting have changed.

Today there is much talk of multi-domain, but on the ground, this translates into one concrete thing: knowing how to **switch with clarity from advanced systems to essential procedures**, when needed, without losing the command thread.

In the image: AN/PRC-163 (handheld), AN/PRC-167 (manpack), and Web UI on rugged device. New generation multiband tactical radios of the Falcon IV family, now a reference in the NATO context: software-defined systems designed to integrate voice, data, and native encryption within command and control networks - Copyright L3Harris Technologies

Don't miss the Live on Wednesday, October 28

We will discuss it **Wednesday 28 at 9 PM live** on our YouTube and Facebook with two special guests: **Danilo Amelotti**, Retired Incursor of the 9º Col Moschin, and **Nello Di Savio**, Retired Special Forces Radio Operator and Head of J6 Cell of the legendary Task Force 45.

In this live session, we will analyze:

- **How communication was done in the '90s**: devices, procedures, radio discipline, and real limitations
- **Reliability vs modernity**: from analog to digital, pros and cons
- **Security**: interception, triangulation, encryption, and the value of radio silence
- **Integration**: from "talking" to working in a network (units, supports, command)
- **Resilience**: what happens when technology is unavailable or unusable
- **Anecdotes from the field**: episodes (even humorous) that explain military communication better than a thousand slides

We will tell you what has really changed in the field over 30 years: **not just devices, but procedures, security, and ways of fighting.**

We look forward to your questions!

YouTube Live

Facebook Live

BRIGATAFOLGORE.NET is live on Wednesday, January 28 YouTube and Facebook Live at 21:00