# Hybrid 5G–Tactical Radio Networks

Pouyan Ebrahimbabaie, 1LT Nathan Prakopetz, MAJ Mathias Becquaert
{pouyan.ebrahimbabaievarnosfaderani, nathan.prakopetz, mathias.becquaert}@mil.be

## I. INTRODUCTION

The fifth generation of mobile technology (5G) is a key enabler for modern military communications, offering high data rates, low latency, and flexible service capabilities for demanding operational scenarios. NATO considers 5G the cornerstone of its Next Generation Networks (NGN) strategy and has conducted substantial research and standardization activities to assess its operational potential and associated risks.

## II. 5G VULNERABILITIES

While 5G offers notable operational advantages, its civilian-oriented design poses challenges when deployed in contested or combat environments. In our previous work presented at BeMilCIS 2025 [1], the Royal Military Academy (RMA), in collaboration with Belgian Defence, conducted a real-world evaluation of a 5G Standalone (SA) system at Beauvechain Air Base (ICAO: EBBE). The study included laboratory and field testing of Electronic Warfare (EW) threats, such as jamming and false base station attacks. The results confirmed the vulnerability of the 5G air interface to these threats, leading to communication disruption and potential security risks.

## III. PROPOSED MITIGATION MEASURE

To mitigate previously identified vulnerabilities associated with the use of 5G in military deployments, this work investigates and implements Multi-Access (MA) connectivity as a practical, standards-based solution. MA allows a device to maintain simultaneous connections to the 5G core through multiple access networks, enabling the use of both 5G and alternative links such as tactical radios. This capability enables the use of Access Traffic Steering, Switching, and Splitting (ATSSS), which dynamically manages traffic across available links. As a result, communication can be maintained even if one access becomes degraded or unavailable, while traffic can also be distributed across multiple paths to improve resilience and reduce the amount of information exposed if one link is compromised. Fig. 1 illustrates the architecture of the multi-access (hybrid) 5G system.

## IV. EXPERIMENTAL SETUP

To validate the proposed approach, a real-world prototype was developed by integrating L3Harris Falcon III AN/PRC-152A tactical radios as an additional access network into a 5G system. The experimental setup comprises a 5G User Equipment (UE), a 5G Core (5GC), software-defined radios (SDRs), and tactical radios, forming a hybrid communication system. This setup enables the simultaneous use of multiple access networks and allows traffic to be redirected or distributed based on link conditions. Fig. 2 illustrates the experimental setup.

## V. CONCLUSION

The present work demonstrates that MA connectivity, combined with ATSSS, provides an effective mechanism to enhance the resilience of 5G systems in military deployments. The results show that communication can be seamlessly maintained through failover when one access link becomes degraded or unavailable. In addition, distributing traffic across multiple paths reduces the risk of full data exposure, improving robustness against interception. These findings confirm the practical value of hybrid 5G–tactical radio architectures for reliable and secure military communications.

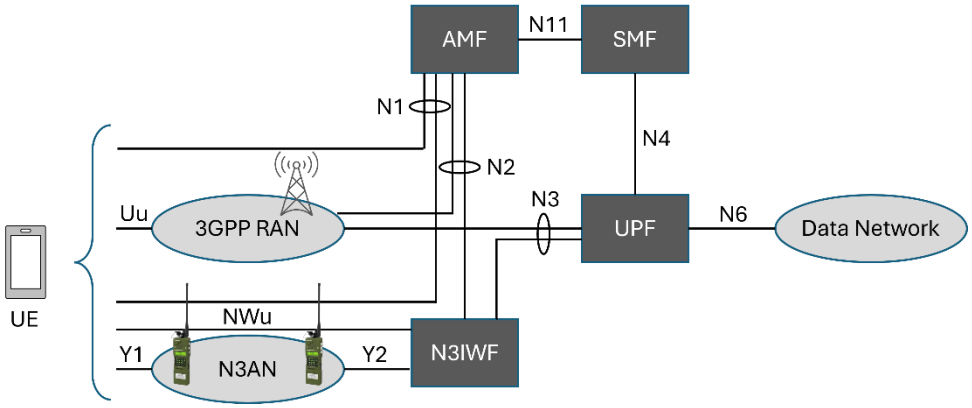


*Figure 1: Multi-Access (MA) 5G system architecture integrating L3Harris tactical radios as an additional Non-3GPP Access Network (N3AN). UPF (User Plane Function), AMF (Access and Mobility Management Function), SMF (Session Management Function), and N3IWF (Non-3GPP Interworking Function) denote core network functions; N2–N11 represent 3GPP-defined interfaces.*


*Figure 2: Experimental hybrid 5G-tactical radio network.*

## REFERENCES

[1] N. Prakopetz, “Security audit: 5G standalone installation at Beauvechain air base,” Royal Military Academy (RMA), Brussels, Belgium, Technical Report, 2025.