Enlarging Lawful Interception Capabilities with Control-Plane Analysis for User Activity Detection

1st Ingrid Huso
Dept. of Electrical and Information Engineering
Politecnico di Bari, Bari, Italy
CNIT, Consorzio Nazionale Interuniversitario
per le Telecomunicazioni
ingrid.huso@poliba.it

2nd Enrico Boffetti
Dept. of Electrical and Information Engineering
Politecnico di Bari, Bari, Italy
CNIT, Consorzio Nazionale Interuniversitario
per le Telecomunicazioni
e.boffetti@phd.poliba.it

3rd Giuseppe Piro
Dept. of Electrical and Information Engineering
Politecnico di Bari, Bari, Italy
CNIT, Consorzio Nazionale Interuniversitario
per le Telecomunicazioni
giuseppe.piro@poliba.it

4th Gennaro Boggia
Dept. of Electrical and Information Engineering
Politecnico di Bari, Bari, Italy
CNIT, Consorzio Nazionale Interuniversitario
per le Telecomunicazioni
gennaro.boggia@poliba.it

***Abstract*—The continuous usage of end-to-end encryption in 5G and Beyond 5G (B5G) networks presents new challenges for Law Enforcement Agencies (LEAs) seeking to detect user activities without access to encrypted data. This paper presents a control-plane Lawful Interception (LI) procedure, where control-plane signaling messages are used to detect user activity without decrypting data-plane traffic. Specifically, Non-Access Stratum (NAS) signaling messages captured during Packet Data Unit (PDU) session establishment are used to identify the nature of user services (i.e., Data Network Name (DNN)). Moreover, the proposed control-plane LI procedure is validated through a proof-of-concept implementation based on Open5GS, UERANSIM, and OpenLI within a containerized testbed. Herein, validation results confirm that the analysis of control-plane data allows for the reliable identification of active user sessions. This is achieved while ensuring full compliance with LI requirements and maintaining a minimal impact on user privacy.**

***Index Terms*—5G Security, Lawful Interception, Control Plane, End-to-End Encryption.**

I. Introduction

Cybercrime, terrorism-related offenses, and prohibited operations have seen a sharp increase among criminal networks operating within the European Union (EU) [1]. The most current report on EU offenses provides statistical information for the years 2016–2023 [2]. Specifically, it covers a wide range of criminal activities in EU member states, including acts against computer systems (approximately 120k cybercrime events recorded in 2023), participation in organized criminal activities (approximately 8.2k registered activities during the same year), and illegal activities involving illicit substances, which accounted for over 1200k events. This unveils that EU member states are increasingly participating in these initiatives. For example, between 2018 and 2023, the number of cybercrimes in key European nations doubled, while it slightly increased from 2021 [3].

Currently, new-generation mobile systems heavily rely on Instant Messaging (IM) and Voice over New Radio (VoNR) platforms for real-time communication and secure exchange of private information using end-to-end encryption [4]. While end-to-end encryption increases privacy level, it inadvertently contributes to the challenges of combating the aforementioned illicit activities [5]. Moreover, the 5G and Beyond 5G networks leverage emerging technologies like Software-Defined Networking (SDN), Network Function Virtualization (NFV), network slicing, and Edge Computing to introduce a highly dynamic and distributed architecture that offers unprecedented data rates, high channel capacity, and low latency compared to conventional technologies [6]. However, while these emerging technologies enable efficient resource allocation and on-demand network customization, they also complicate the identification of exact interception points and the application of advanced statistical techniques for real-time data interception and processing in future network infrastructures [7].

Indeed, Law Enforcement Agencies (LEAs) are looking for novel and efficient Lawful Interception (LI) tools that operate with the developing 5G and Beyond 5G network architectures. In this context, a set of standards for LI in 5G has been standardized by 3rd Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI). Specifically, procedural and interface-level requirements are defined in TS 33.126, 33.127, and 33.128 [8]–[10]. However, these frameworks are mostly built on static and centralized network topologies, which are becoming more and more incompatible with the distributed, dynamic, and service-oriented characteristics of modern 5G deployments.

In this context, recent research has proposed key escrow-based frameworks to enable controlled decryption within the core network, balancing lawful access with user privacy and

legal protections [3], [11]. Alternative privacy-preserving approaches, such as P3LI5 [12], leverage Private Information Retrieval (PIR) to facilitate low-latency and privacy-aware identifier resolution. Moreover, ensuring the integrity and non-repudiation of intercepted data is equally critical, with solutions addressing data completeness, correctness, and resilience against malicious attribution [13], [14]. However, to the best of the authors' knowledge, no works investigate in the LI field the possibility of intercepting and analyzing control-plane messages to help LEA in classifying user services and understanding their behavior without targeting the encrypted user payload. To bridge this gap, our work presented herein provides the following main scientific contributions:

- We present a LI framework that builds upon our previous proposal [3] by integrating control-plane analysis to enable activity detection, thereby extending interception capabilities by capturing a deterministic Intercept Related Information (IRI) (i.e., the Data Network Name (DNN)) from Non-Access Stratum (NAS) signaling during Packet Data Unit (PDU)) session establishment.
- We deployed a proof-of-concept implementation of the proposed LI framework using Linux-based Docker containers to simulate a 5G network using Open5Gs and UERANSIM. Thus, we use OpenLI software to ensure standard-compliant LI implementation [3]. Our Python scripts and cryptographic libraries enable end-to-end encrypted data exchange, interception, and decryption using Key Escrow at the application layer.
- We validate the proposed approach across two use cases: encrypted end-to-end file exchange and encrypted VoNR service.

The remainder of this paper is organized as follows. Section II provides an overview of the background concepts. Section III introduces the proposed control-plane LI procedure. Section IV details the proof-of-concept implementation and presents the validation results. Finally, Section V concludes the paper and outlines future research activities.

TABLE I: Acronyms Table

Acronym	Extended Version
3GPP	3rd Generation Partnership Project
5GNR	5G New Radio
5GCN	5G Core Network
ADMF	Administration Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
B5G	5G and Beyond 5G
CC	Communication Content
CSP	Communications Service Provider
E2EE	End-to-End Encryption
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GTP-U	GPRS Tunneling Protocol User Plane
gnB	Next Generation Node B
IDBC	ID-based Cryptosystem
IM	Instant Messaging
IMSI	International Mobile Subscriber Identity
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MDF	Mediation and Delivery Function
POI	Point of Interception
SIRF	System Information Retrieval Function
UE	User Equipment
UPF	User Plane Function
NFV	Network Function Virtualization
SDN	Software-Defined Networking
SMF	Session Management Function
VoNR	Voice over New Radio
PDU	Packet Data Unit
DNN	Data Network Name
NAS	Non-Access Stratum
NGAP	Next Generation Application Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
SUPI	Subscription Permanent Identifier
ML	Machine Learning

II. Background

Lawful Interception. The standardized architecture and procedures that allow Communications Service Providers (CSPs) to gather, store, and transmit communication data to authorized LEAs are referred to as LI [8]. The 3GPP TS 33.126 (requirements) [8], TS 33.127 (architecture) [9], and TS 33.128 (protocols) [10] standards all specify LI in 5G networks. In particular, LI functions are distributed over multiple network elements. Specifically, the Administration Function (ADMF) manages the interception lifecycle, which includes managing warrants and Point of Interceptions (POIs) using the System Information Retrieval Function (SIRF) and related interfaces. To detect target communications, extract IRI and Communication Content (CC), and send them to the Mediation and Delivery Function (MDF), POIs are usually deployed within User Plane Functions (UPFs). To guarantee that authorized LEAs may access communications, it then divides and sends the intercepted data to the Law Enforcement Monitoring Facilities (LEMFs) over standardized HI2 and HI3 interfaces.

Control Plane Interfaces and NAS Protocol in 5G Core. In 5G Standalone (SA) networks, control-plane communication is managed via standardized interfaces such as N1 (User Equipment (UE) – Access and Mobility Management Function (AMF), carrying NAS signaling) and N2 (Next Generation Node B (gNB) – AMF, via Next Generation Application Protocol (NGAP)) [15]. The NAS protocol handles registration, authentication, and session management procedures, including the PDU Session Establishment Request, which conveys metadata like DNN, session type, and Single - Network Slice Selection Assistance Information (S-NSSAI) to the Session Management Function (SMF) [15]. Although NAS does not transmit user data, its signaling reveals behavioral metadata, such as service usage, slice selection, and session intents, that can be analyzed to detect user activity without decrypting the user plane data.

III. Proposed control-plane LI procedure

The proposed control-plane LI procedure builds upon the LI framework designed in [3] and leverages standard 5G Network

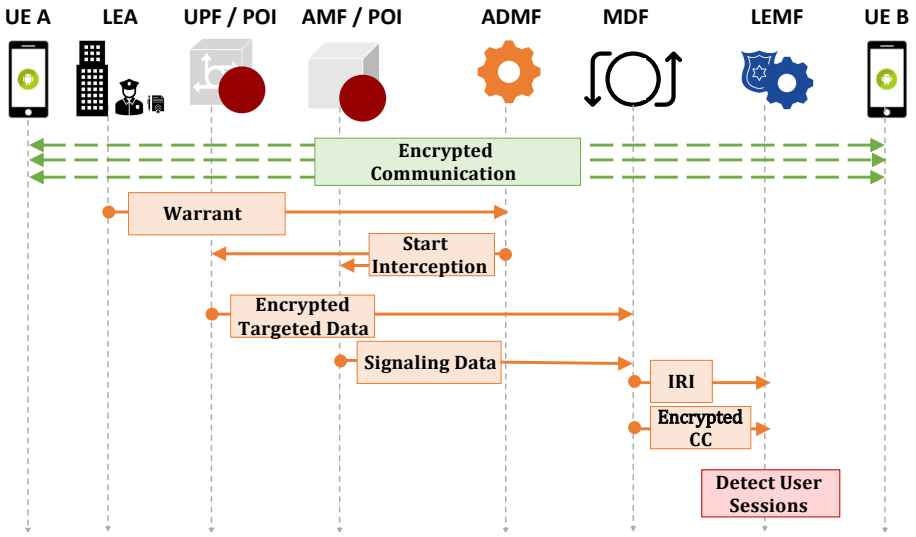

Fig. 1: Message flow of the proposed control-plane LI procedure

Functions (NFs) to facilitate the extraction of metadata from control-plane signaling.

The core network includes essential components such as the AMF, SMF, and UPF, while the 5G New Radio (5GNR) and UEs participate in common signaling protocols, including NAS exchanges. The LI framework consists of four primary components. The ADMF manages the provisioning of interception warrants of a target UE. The POI passively monitors specific control-plane interfaces, particularly at the AMF and SMF, while actively intercepting end-to-end encrypted data from the data plane (i.e., UPF). The acquired data is then processed by the MDF, which formats the IRI and CC, and transmits them to the LEMF, where authorized LEA can access the intercepted data.

Fig. 1 provides a comprehensive overview of the control-plane interception procedure, which operates as follows:

- **Warrant Provisioning:** The LEA issues an interception warrant for a target UE, which is provisioned into the ADMF.
- **POI Activation:** The ADMF instructs the POIs (i.e., IRI and CC) to begin monitoring control-plane traffic associated with the target UE.
- **Service Initiation:** When the UE starts a service, such as a VoNR call or an end-to-end file exchange, it sends a PDU Session Establishment Request to the AMF via the N1 interface. The plaintext DNN in this message indicates the requested service (e.g., `IMS` or `INTERNET`).
- **IRI Capture:** As part of the IRI, the POI gets the DNN and UE identifier from the NAS message on the N1 and N4 interfaces.
- **IRI Delivery:** The MDF sends the IRI information to the LEMF. This information includes the timestamp, DNN, and UE identifier.
- **Activity Detection:** Based on the received DNN, the LEA operating at the LEMF can deduce the type of service requested by the UE (e.g., `IP Multimedia Subsystem (IMS)` for voice and `INTERNET` for data access).

The proposed control-plane LI procedure enables detection of user activity via lawful signaling analysis while maintaining active LI end-to-end encryption on the user plane.

IV. Proof-of-Concept Implementation

To validate the proposed control-plane LI procedure, we deployed a proof-of-concept testbed, as depicted in Fig. 2. The entire environment is containerized using Docker, ensuring the portability and reproducibility of the proof-of-concept.

Testbed Architecture and Components. We used *Open5GS* [16] to emulate the 5G Core Network (5GCN) by configuring one instance for each of the key network functions: the AMF, SMF, and the UPF. To emulate the radio access components, *UERANSIM* [17] was employed by allowing the simulation of both UEs and the gNBs. A total of two UEs were instantiated, each capable of independently initiating service requests. Additionally, we deployed *OpenLI* [18], to emulate the standard LI components. The system was orchestrated as a set of containerized microservices, including the Provisioner, Collector, Mediator, and Agency components. Herein, the *Collector* serves as the primary POI for both control-plane and data-plane communications. Finally, to guarantee application-layer services, a containerized *Asterisk* server was integrated into the environment for VoNR call scenarios between the simulated UEs. Specifically, the network was configured to differentiate services by using distinct DNNs. We defined an `IMS` DNN for VoNR services and an `INTERNET` DNN for an end-to-end data file exchange. This implementation ensures that the primary evidence of user activity is embedded within the control-plane signaling itself, specifically in the NAS messages requesting a PDU session.

Configuration of the Interception Point (POI) A key aspect of our implementation involved the deployment of a multi-point interception strategy, aligned with the 3GPP TS

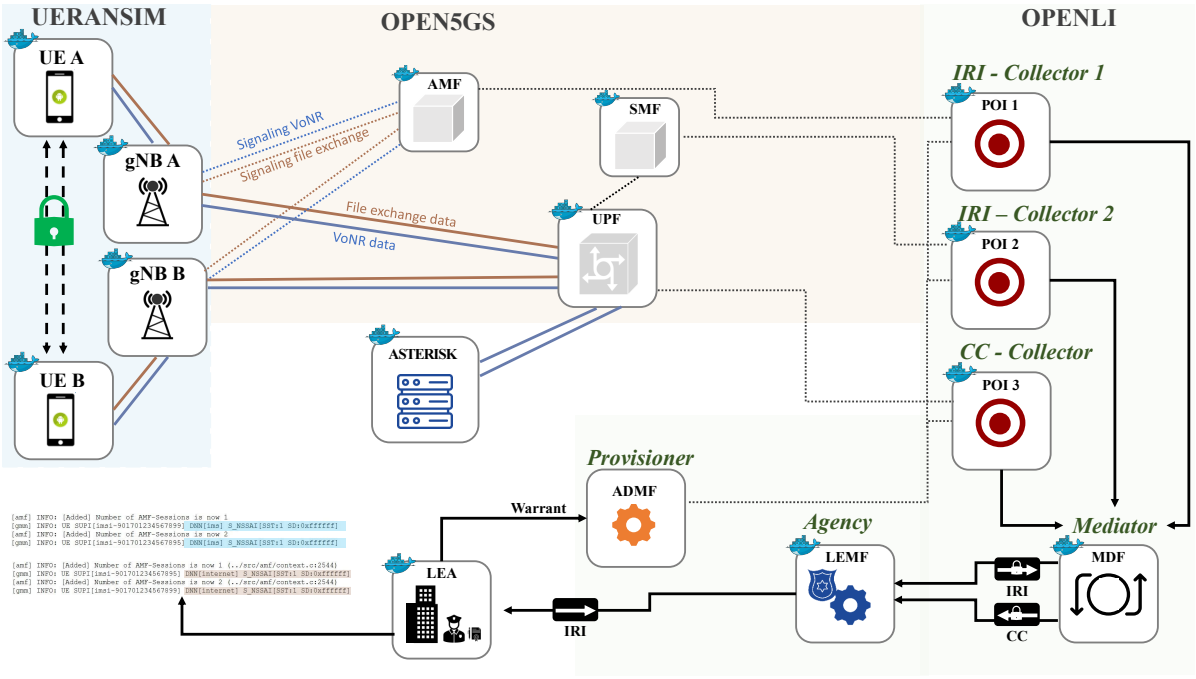

Fig. 2: Proof-of-Concept implementation of the proposed control-plane LI procedure.

```
[amf] INFO: [Added] Number of AMF-Sessions is now 1
[gmm] INFO: UE SUPI[imsi-901701234567899] DNN[ims] S_NSSAI[SST:1 SD:0xffffff]
[amf] INFO: [Added] Number of AMF-Sessions is now 2
[gmm] INFO: UE SUPI[imsi-901701234567895] DNN[ims] S_NSSAI[SST:1 SD:0xffffff]
```

(a) Voice over New Radio use case

```
[amf] INFO: [Added] Number of AMF-Sessions is now 1 (../src/amf/context.c:2544)
[gmm] INFO: UE SUPI[imsi-901701234567895] DNN[internet] S_NSSAI[SST:1 SD:0xffffff]
[amf] INFO: [Added] Number of AMF-Sessions is now 2 (../src/amf/context.c:2544)
[gmm] INFO: UE SUPI[imsi-901701234567899] DNN[internet] S_NSSAI[SST:1 SD:0xffffff]
```

(b) File Exchange use case

Fig. 3: AMF Log Analysis on the N1/N2 interfaces

```
[sbi] INFO: NF registered
[sbi] INFO: NF Profile updated
[smf] INFO: [Added] Number of SMF-UEs is now 1
[smf] INFO: [Added] Number of SMF-Sessions is now 1
[smf] INFO: [Added] Number of SMF-UEs is now 2
[smf] INFO: [Added] Number of SMF-Sessions is now 2
[smf] INFO: UE SUPI[imsi-901701234567895] DNN[internet] IPv4[10.45.0.2] IPv6[]
[smf] INFO: UE SUPI[imsi-901701234567895] DNN[ims] IPv4[10.46.0.2] IPv6[]
[gtp] INFO: gtp_connect() [172.22.0.4]:2152
```

(a) SMF Log Analysis for UE A

```
[sbi] INFO: NF registered
[sbi] INFO: NF Profile updated
[smf] INFO: [Added] Number of SMF-UEs is now 1
[smf] INFO: [Added] Number of SMF-Sessions is now 1
[smf] INFO: [Added] Number of SMF-UEs is now 2
[smf] INFO: [Added] Number of SMF-Sessions is now 2
[smf] INFO: UE SUPI[imsi-901701234567899] DNN[internet] IPv4[10.45.0.3] IPv6[]
[smf] INFO: UE SUPI[imsi-901701234567899] DNN[ims] IPv4[10.46.0.3] IPv6[]
[gtp] INFO: gtp_connect() [172.22.0.4]:2152
```

(b) SMF Log Analysis for UE B

Fig. 4: SMF Log Analysis on the N4 interface

33.127 [9]. In particular, three distinct POIs were configured to capture different categories of data across both the control and user planes. For the control plane, two POIs were deployed to collect IRI. These were implemented by running `TShark` directly on the network interfaces of the AMF and SMF containers, enabling the interception of signaling messages that carry essential metadata related to the communication, such as NAS requests and responses. On the user plane, a third POI was configured to collect the encrypted CC, aligned with the approach presented in [3]. Herein, the collector was responsible for aggregating and processing this mirrored traffic in line with the LI framework present in [3].

Service Initiation and Control-Plane Data Capture. The network was designed to support multiple simultaneous services per user. Each UE in the Open5GS subscriber database was configured to access two separate services, each linked to a unique DNN and its corresponding Internet Protocol (IP) subnet. The `IMS` DNN was allocated for VoNR traffic and assigned to the `10.46.0/24` subnet, while the `INTERNET` DNN was utilized for data sessions related to file exchanges and assigned to the `10.45.0.0/24` subnet. For example, a UE might receive the IP address `10.46.0.2` for its VoNR session and `10.45.0.2` for its data session. Within the UERANSIM environment, these sessions were automatically associated with distinct virtual tunnel interfaces: `uesimtun0` for the `IMS` session and `uesimtun1` for the `INTERNET` session. Thus, when a UE initiates a predefined action, such as starting an end-to-end encrypted VoNR call, it transmits a NAS *PDU Session Establishment Request* message to the AMF. This message explicitly specifies the target DNN (e.g., `IMS`) in plaintext, which serves as the IRI of interest for our capture strategy. As this control-plane signaling traverses the 5G core, the targeted encrypted CC packets are duplicated at the UPF and forwarded to the *Collector* instance. When the control plane is intercepted, *TShark* is employed to monitor the mirrored traffic entering the Collector. It processes the data stream in real-time, extracting and saving significant control-plane messages as structured `.pcap` files for further

processing and analysis.

LI Framework Validation. We validate the proposed framework by analyzing the control-plane signaling generated across two distinct use cases: an end-to-end encrypted VoNR service and an encrypted end-to-end file exchange session. To this end, we configured two UEs to initiate these services sequentially within our testbed. Our validation focused on parsing the logs produced by the AMF and SMF.

Our analysis of the logs confirmed this hypothesis. When the UE initiated a 30 seconds VoNR call, we observed the creation of a PDU session where the AMF log recorded the request against the user's Subscription Permanent Identifier (SUPI) along with the metadata field `DNN[IMS]` (see Fig. 3a). The SMF log correspondingly showed the allocation of an IP address (i.e., `10.46.0.2` for UE A and `10.46.0.3` for UE B) from the designated VoNR subnet, as depicted in Fig. 4. Later, when the same UEs started the 10 MB file exchange session, we observed a second, distinct PDU session establishment. The logs in Fig. 3b marked this new session with the identifier `DNN[INTERNET]`, while the SMF assigned a new IP address (i.e., `10.45.0.2` for UE A and `10.45.0.3` for UE B) from the general data subnet, as shown in Fig. 4.

These findings demonstrate that monitoring of control-plane logs enables reliable detection of the type of service a user is accessing. The DNN identifier, which is transmitted in plaintext during the initial NAS procedure, acts as a high-fidelity IRI. This validates our approach, proving that meaningful user activity can be classified for security applications without requiring the decryption of the user-plane payload.

V. Conclusion

This paper presented a control-plane Lawful Interception (LI) procedure integrated into our designed LI framework, aimed at enabling LI in 5G and Beyond 5G networks, where end-to-end encryption limits access to user payloads. Instead of attempting to decrypt user data, our approach focuses on passively analyzing control-plane metadata to detect user activity. We demonstrated that the Data Network Name (DNN), transmitted in plaintext during the PDU Session Establishment procedure, serves as a reliable source of IRI. Using a testbed based on Open5GS, UERANSIM, and OpenLI, we showed that it is possible to distinguish between different services (i.e., Voice over New Radio (VoNR) calls and file exchange sessions) based solely on the captured DNN values. These findings were validated by correlating logs from the Access and Mobility Management Function (AMF) and Session Management Function (SMF) components. Future activities plan to explore the integration of Machine Learning (ML) techniques to enhance activity detection capabilities based on control-plane patterns.

Acknowledgments

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Mission 4, Component 2, in the context of partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART", CUP:D93C22000910001), national center on "Sustainable Mobility" (CN00000023 - program "MOST", CUP: D93C22000410001), and partnership on "Cybersecurity" (PE00000007 - program "SERICS", CUP:D33C22001300002, project ISP5G+). It was also supported by the PRIN 2022 projects INSPIRE (grant no. 2022BEXMXN 01) and HORUS (grant no. 2022P44KA8) funded by the Italian MUR, and by the HORIZON MSCA project BRIDGITISE (grant no. 101119554).

References

[1] The European Commission, *Eurostat, Recorded offences by offence category - Police data*. The European Commission, 2025.

[2] ——, *Eurostat, Recorded offences by offence category - Police data*. The European Commission, 2021.

[3] I. Huso, M. Olivieri, L. Galgano, A. Rashid, G. Piro, and G. Boggia, "Design and implementation of a looking-forward lawful interception architecture for future mobile communication systems," *Computer Networks*, vol. 249, p. 110518, 2024.

[4] M. Alatawi and N. Saxena, "Sok: An analysis of end-to-end encryption and authentication ceremonies in secure messaging systems," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 187–201.

[5] T. Isobe and R. Ito, "Security analysis of end-to-end encryption for zoom meetings," *IEEE Access*, vol. 9, pp. 90 677–90 689, 2021.

[6] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6g: Visions, requirements, key technologies, and testbeds," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905–974, 2023.

[7] Council of the European Union and EUROPOL, "Position paper on 5G," The European Commission, Tech. Rep., April 2019.

[8] 3GPP, "Lawful interception (li) requirements," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.126, November 2022, Release 18.0.0.

[9] ——, "Lawful interception (li) architecture and functions," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.127, September 2023, Release 18.5.0.

[10] ——, "Protocol and procedures for lawful interception (li)," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 33.128, September 2023, Release 18.5.0.

[11] G. Ungaro, F. Ricchitelli, I. Huso, G. Piro, and G. Boggia, "Design and implementation of a lawful interception architecture for b5g systems based on key escrow," in *2022 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2022, pp. 207–207.

[12] F. Intoci, J. Sturm, D. Fraunholz, A. Pyrgelis, and C. Barschel, "P3li5: Practical and confidential lawful interception on the 5g core," in *2023 IEEE Conference on Communications and Network Security (CNS)*, 2023.

[13] F. Boeira, M. Asplund, and M. Barcellos, "Provable non-frameability for 5g lawful interception," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023.

[14] F. Buccafurri, A. Consoli, C. Labrini, and A. M. Nesurini, "A solution to support integrity in the lawful interception ecosystem," in *Electronic Government and the Information Systems Perspective*, A. Kö, E. Francesconi, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds. Springer International Publishing, 2021.

[15] ETSI, "5g system architecture." European Telecommunications Standards Institute (ETSI), Technical Report (TS) 123 501 V16.6.0, December 2021.

[16] S. Kim and J. Lee, "Open5gs: An open-source 5g core network implementation," *IEEE Access*, vol. 8, pp. 142 447–142 456, 2020.

[17] W. Zhou and A. Smith, "Ueransim: A 5g nr simulator for research and development," *IEEE Access*, vol. 9, pp. 17 823–17 835, 2021.

[18] O. Project, "Openli: An open-source lawful interception system," https://www.openli.nz/, 2023.