Written evidence submitted by Dr Max Hashem Eiza (Liverpool John Moores University) (CYB0016)

Introduction

I am a senior lecturer in Computer Security at Liverpool John Moores University (LJMU). This written evidence is based on my work at the research centre for Critical Infrastructure Computer Technology and Protection (PROTECT) at LJMU. I have over 7 years of experience and published several research outputs in the areas of 5G security, smart grid security and resilience, and the use of emerging technologies/concepts such as Blockchain and Zero Trust (ZT) in communication networks. Most of this written evidence comes from my recent investigation on the security and resilience of Open Radio Access Networks (OpenRAN). I would be happy to appear in front of the Committee to give an oral submission, answer any questions, and provide the Committee with any more detail if needed.

Scope

This written evidence focuses on the cyber threats to OpenRAN architecture and functions. OpenRAN will be the foundation of the next-generation of communication networks, which are essential for the UK digital economy and interconnecting the national critical infrastructure-based services. While the focus on OpenRAN might seem very narrow, it is of paramount importance to address the security challenges posed by its openness, softwareisation, virtualisation, and disaggregation of networking devices/functions, which will be at the core of the UK's future mobile networks. Note that this written evidence will address fully or partially three of the six topics in the call for evidence.

Executive Summary

- OpenRAN is an exciting new approach that creates a multi-vendor telecoms ecosystem that drives competition and innovation and solves an important national security issue regarding the telecoms supply chain in the UK.
- Despite the many security benefits OpenRAN brings, its architecture extends the threat surface due to its openness, virtualisation, and cloud deployment of networking devices and functions.
- The UK Government should extend their cyber security strategies to address the paradigm shift in the threats facing a core part of the UK's future telecoms networks especially insider threats.
- Through legislation and regulations, the UK Government should accelerate the adoption and implementation of Zero Trust Architecture (ZTA) in OpenRAN and the CNI organisations most critical to the UK digital economy.
- A guidance and/or regulation mandating an X Bill of Materials (XBOM) for every software library/system or hardware component, which will be used in the UK's CNI, is essential to manage supply chain risks and vulnerabilities and ensure cyber resilience of telecoms networks.

1. **The types and sources of cyber threats to Critical National Infrastructure (CNI) most critical to the function of the UK digital economy: Communications (including space);**
   - In December 2021, the Government, and the UK's Mobile Network Operators (MNOs) announced their ambition for 35% of the UK's mobile network traffic to be carried over OpenRAN architectures by 2030 [1]. This is partly driven by the Government telecoms diversification taskforce recommendations [2] and the UK's evolving strategy towards the six

generation (6G) networks. The telecoms supply chain is a national security issue for the UK and other advanced economies, as they aim to reduce their reliant on a small number of vendors, some of which have been identified as high-risk (e.g., Huawei [3]).

- OpenRAN provides the ideal solution to create a robust multi-vendor ecosystem that drives competition and innovation and improve the telecoms networks' agility, resiliency, and flexibility. Figure 1 illustrates the high-level technical differences between OpenRAN and traditional RAN across the stack from hardware to service management.

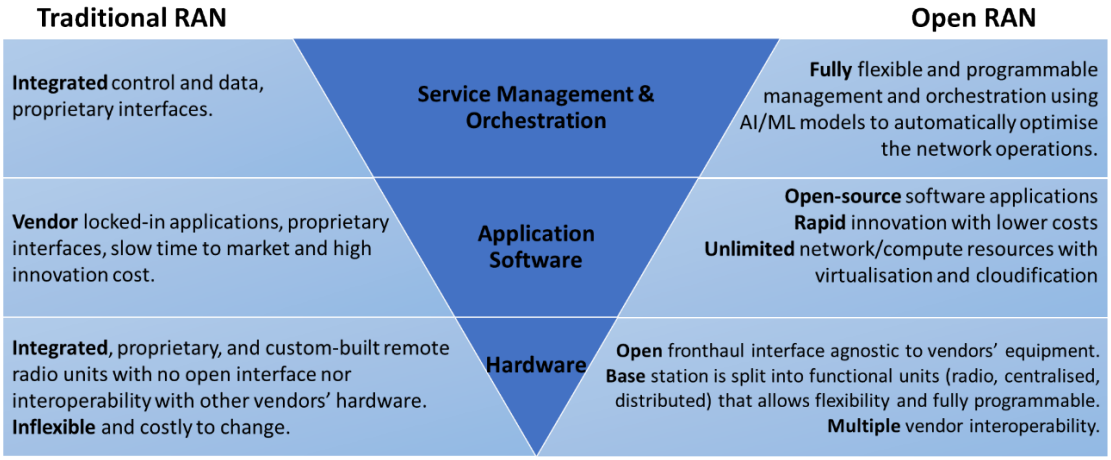

Figure 1. Traditional RAN vs. OpenRAN

- Due to its openness, OpenRAN brings many security benefits where operators have a more predominant role in securing the infrastructure by assessing and vetting the security level of open components from different vendors. Moreover, the introduction of intelligence, cloud-native deployment, and unprecedented monitoring capabilities can provide invaluable insights to implement advanced intrusion detection/prevention solutions to detect and prevent threats [4]. Of course, this is the view of glass half full, which should not be adopted for the security of an integral part of our critical national infrastructure.
- The glass half empty view is the identification, as of October 2023, of eight threat categories and a total of 178 possible threats against 39 OpenRAN-specific critical assets related to interfaces and data, and 43 related to logical/virtual/physical components [5]. This is besides existing threats against the core network and users' equipment as described in [4], which is outside the scope of this written evidence. In the following, where appropriate, a note will be made when the threat is specific/unique to OpenRAN architecture. **Threat types against OpenRAN as a CNI are**:
  - *Threats against OpenRAN architectural elements and interfaces*. These threats could compromise the availability of the infrastructure (e.g., an attacker exploits misconfigured or weak authentication/authorisation of an OpenRAN component to deteriorate the performance of the network or shut it down), data and infrastructure integrity (e.g., an attacker exploits a vulnerable software component in the supply chain to cause data tampering), and data confidentiality.
  - *Threats against the OpenRAN-Cloud (O-Cloud)*. Cloud-native telecoms networks are a lucrative target for cyber threat actors in addition to the security challenges of multitenancy in cloud infrastructure and cloud insecure interfaces (e.g., insecure cloud interface of crypto-ATM manufacturer, General Bytes, was abused in a hack to steal $1.5M, leading to discontinuation of the cloud service and temporary shutdown of

thousands of ATMs across the US in March 2023 [6]). While the threats against cloud platforms are not new, when a core part of the UK's future telecoms networks operate in the cloud, these threats become unique to OpenRAN considering their devastating impact on the CNI.

- *Threats to open-source code*. Developers could use components with known vulnerabilities and/or untrusted libraries that can be exploited by attackers to establish a foothold inside the network. This could be intentional from an insider threat agent (i.e., a developer inserts a backdoor into the software to facilitate an attack later).
- *Threats to physical components*. These include attackers gaining physical access to hardware units to cause damage or access sensitive data. This is possible via a hardware backdoor as well.
- *Threats against the radio network*. Attacks against the radio units via signal jamming, sniffing, and spoofing can cause Denial of Service (DoS) and lead to a massive performance degradation on the air interface.
- *Threats against the Artificial Intelligence (AI)/Machine Learning (ML) components*. These threats can vary from poisoning the ML training data to altering the ML model to feed misleading data to the AI/ML components. This could result in AI/ML solutions that output incorrect predictions or make wrong control decisions that lead to performance degradation or outages.
- *Protocol Stack Threats*. OpenRAN interfaces (A1 and R1) use the REST protocol stack which includes the JSON, HTTP, TCP, and IP protocols. Different attacks can be launched against these protocols such as injection, cross-site scripting, DoS, and exposure of object identifiers without proper authorisation checks. These threats are unique to OpenRAN.
- *Service Management and Orchestration (SMO) Threats*. With its vital role in OpenRAN, attacks on SMO can have devastating impact including confidentiality, integrity, and availability of data and services. Attacks vary from exploiting weak authentication/authorisation to DoS attacks against the SMO functions.

➢ The sources of the cyber threats above can be one or a combination of the following threat agents ranked in order of concern and threat to OpenRAN as a CNI:

- Insiders who are authorised inside the system and may facilitate or commit a malicious attack against the network. This group is by far the most dangerous to OpenRAN.
- Organised crime/hackers/Advanced Persistent Threat (APT) who could be affiliated with hostile nations. These attackers have access to vast resources to attack and gain access to public and private CNI networks to compromise, steal, or destroy information.
- Cyber terrorists who launch attacks against critical infrastructure with the sole aim of violence against groups of people.
- Hacktivists who perform cyber-attacks to achieve political or social gains.

2. The strengths and weaknesses of the UK Government's National Cyber Strategy 2022 and Government Cyber Security Strategy 2022-2030 in relation to CNI for the digital economy;

➢ Both the UK Government's strategies above have the following **strengths** in relation to CNI in general and telecoms networks (including OpenRAN) in particular:

- Countering threats against CNI has been recognised in both documents as an essential element of building the UK's cyber resilience.

- Demanding governmental departments, public sector and regulated operators of CNI, and providers of digital services and platforms to raise their standards and manage risks more proactively. This includes the adoption of the Cyber Assessment Framework (CAF) to provide consistent cyber security assurance across organisations that operate the UK's essential services.
- Commitment to establish the UK Telecoms Lab in collaboration with the regulator and industry to support the new telecoms security framework and help to increase the diversity of telecoms equipment vendors in the UK's supply chain. In fact, this commitment resulted in establishing the new security framework via the Telecommunications Security Act (TSA) [7], which came into force on the 1st of October 2022. This is further supported by the UK Product Security and Telecommunications Infrastructure (Product Security) regime [8], which will come into force on 29 April 2024.

➢ On the other hand, both strategies lack the following points (i.e., **weaknesses**):
- A clear categorisation and reference to the 13 CNI sectors in the UK, as published by the National Protective Security Authority (NPSA) [9], and how cyber security strategies can be tailored to some of these sectors. Note that NPSA does not categorise Information Technology as a CNI sector, which is something that should be addressed giving the dependence of the UK digital economy on that sector.
- A reference to any commitment to implement a Zero Trust Architecture (ZTA) strategy to improve the cyber security posture of Government's departments and CNI organisations most critical to the UK digital economy and national services. Zero Trust (ZT) is a concept whereby no digital system or a human user, whether external or internal, can be trusted, regardless of ownership and location [10]. ZTA is a plan to implement ZT in digital systems. As pointed out earlier in the threats against OpenRAN, we need to adopt the mindset of ZT (i.e., 'assume breach') and eliminate implicit trust in any system/component especially when parts of our CNI are deployed in the cloud and use open-source software.

3. What are the interventions that are required from Government, and CNI organisations most critical to the UK digital economy to ensure the Government's cyber resilience targets by 2025 are achieved;

➢ Signalling a clear commitment via policies and/or legislation to implement ZTA strategy across Government's departments and public/private sectors that operate UK's CNI especially the Information Technology and Communications sectors. For instance, in the US, the White House Office of National Cyber Director (ONCD) included a reference to ZTA in their National Cyber security Strategy, which was published in March 2023 [11] : "*This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a ZTA strategy and modernize IT and OT networks*."

➢ Accelerating the adoption of the National Cyber Security Centre (NCSC) eight design principles for ZTA implementation [12] in the CNI organisations most critical to the UK digital economy by requiring an annual update of progress towards a fully mature ZTA system. The UK Government, via NCSC and collaboration with international partners, is in a great position to lead international efforts on ZT maturity model for OpenRAN and the telecoms industry, while also considering additional UK specific needs for CNI operators.

- Embedding a legal and/or regulation requirement of providing an X Bill of Materials (XBOM) to every system/component that will be used in CNI whether it is a software or a hardware. XBOM extends the concept of Software Bill of Materials (SBOM), which focuses on software supply chain risk management [13]. The UK should lead the charge to facilitate this feature that will ensure we can trace every library and hardware/software component we use in our digital systems especially OpenRAN.

28 November 2023

References

[1] Department for Digital, Culture, Media & Sport, "A joint statement on the sunsetting of 2G and 3G networks and public ambition for Open RAN rollout as part of the Telecoms Supply Chain Diversification Strategy," 8 Dec 2021. [Online]. Available: https://www.gov.uk/government/news/a-joint-statement-on-the-sunsetting-of-2g-and-3g-networks-and-public-ambition-for-open-ran-rollout-as-part-of-the-telecoms-supply-chain-diversificatio. [Accessed 28 Oct 2023].

[2] Telecoms Diversification Taskforce, April 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975007/April_2021_Telecoms_Diversification_Taskforce_Findings_and_Report_v2.pdf. [Accessed 28 Oct 2023].

[3] National Cyber Security Centre (NCSC), "Summary of NCSC's security analysis for the UK telecoms sector," 28 Jan 2020. [Online]. Available: https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector. [Accessed 28 Oct 2023].

[4] M. Polese, L. Bonati, S. D'Oro, S. Basagni and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 2, pp. 1376-1411, 2023.

[5] O-RAN Work Group 11 (Security Working Group), "O-RAN Security Threat Modeling and Risk Assessment," O-RAN Alliance, 2023.

[6] J. Redman, "Major Cryptocurrency ATM Manufacturer General Bytes Hacked, Over $1.5M in Bitcoin Stolen," 19 Mar 2023. [Online]. Available: https://news.bitcoin.com/major-cryptocurrency-atm-manufacturer-general-bytes-hacked-over-1-5m-in-bitcoin-stolen/. [Accessed 02 Nov 2023].

[7] UK Government, "Telecommunications (Security) Act 2021," 2021. [Online]. Available: https://www.legislation.gov.uk/ukpga/2021/31/enacted. [Accessed 02 Nov 2023].

[8] Department for Science, Innovation and Technology - UK Government, "The UK Product Security and Telecommunications Infrastructure (Product Security) regime," 29 Apr 2023. [Online]. Available: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime. [Accessed 02 Nov 2023].

[9] National Protective Security Authority (NPSA), "Critical National Infrastructure," 25 Apr 2023. [Online]. Available: https://www.npsa.gov.uk/critical-national-infrastructure-0. [Accessed 02 Nov 2023].

[10] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, 2020.

[11] US Government, "National Cybersecurity Strategy," The White House , Washington, 2023.

[12] National Cyber Security Centre (NCSC), "Zero trust architecture design principles," 23 July 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture. [Accessed 02 Nov 2023].

[13] Cybersecurity & Infrastrcuture Security Agency (CISA), "Software Bill of Materials (SBOM)," [Online]. Available: https://www.cisa.gov/sbom. [Accessed 02 Nov 2023].