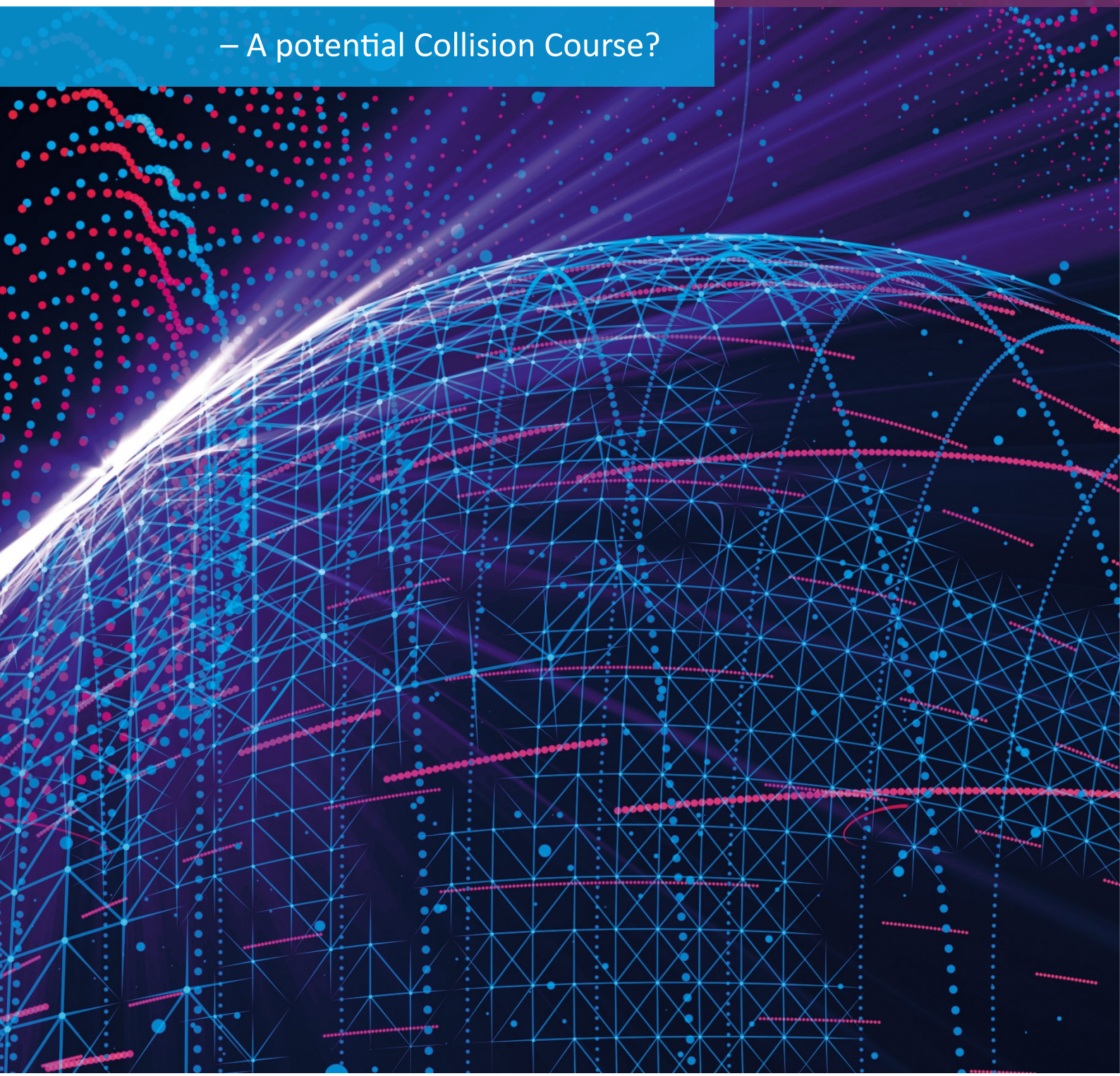
fieldfisher

Open RAN and the Telecoms Security Bill

– A potential Collision Course?

27 November 2020



Open RAN and the Telecoms Security Bill

Introduction

As operators continue the roll-out of 5G infrastructure and seek to introduce new services based on network slicing, there is a growing demand for radio access networks to be increasingly software-driven and based on open interfaces. The potential benefits of introducing Open RAN technology include increased innovation in network sub-systems and the ability for software developers to gain real-time control of radio resources, improve network performance and introduce automation of service management and network orchestration. The requirement for operators to remove Huawei equipment from their networks by 2027 also means there is a strategic need for network operators to have a much wider degree of choice in terms of potential equipment and network solution vendors.

The million dollar question is: how does the industry reconcile the emergence of Open RAN solutions and the need for vendor "diversity of choice" with the increased scrutiny on operators that will be ushered in by the draft Telecoms Security Bill which was published in Parliament on Tuesday?

What is Open RAN?

Open RAN can essentially be thought of as the ability to deploy, integrate and operate radio access networks (so the tower infrastructure, antennas, base stations) using components, systems and software sourced from multiple vendors. The ultimate vision is for the radio access network to be fully programmable with the potential for control of radio network resources by apps (although admittedly this aspect of the vision is still a little distant).

The Open RAN movement is in part a reaction to the limitations of the traditional RAN model and the fact that open practices in adjacent industries such as cloud networking can be applied to the telecoms sector to deliver cost-effective solutions and faster innovation cycles. The traditional RAN deployment involved proprietary hardware, proprietary software and proprietary interfaces which lead to almost inevitable consequences of vendor lock-in and a curb on innovation in the radio access network.

Role of the Standards Bodies and open interfaces

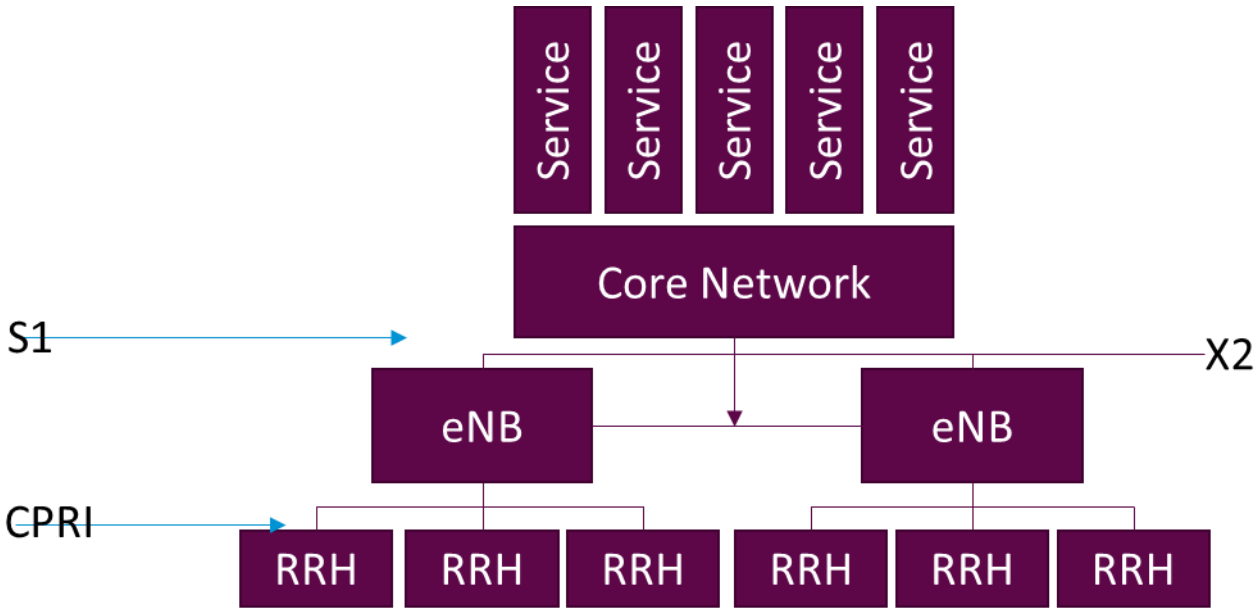
3GPP is one of the key standards bodies in the industry: it unites seven regional standards organisations (e.g. the likes of ETSI for Europe and ATIS for the USA) in order to ensure that there is a level of global standardisation for different technological developments in the telecoms sector. 3GPP Releases 15, 16 and 17 set out the implementation path for 5G network technology for operators across the globe.

Many of the 3GPP interfaces are standardized and open interfaces (such as the S1 interface between the core network and the RAN and the RRC protocol as part of the air interface). However, the same is not true of other interfaces in the radio access network such as the interface between the base station and the remote radio unit (see diagram below) which is based on the CPRI protocol (a proprietary protocol developed by Ericsson, Huawei, NEC and Nokia). Part of the issue is that CPRI interfaces are typically vendor specific implementations and are not necessarily open so organisations like the O-RAN Alliance are working with the industry to replace these CPRI interfaces with open interfaces (eCPRI). The Small Cell Forum has a similar initiative and has defined NFAPI (network femto API) as an open API for these purposes. One key focus area will to ensure that management and control traffic routed across the open fronthaul are protected to try and eliminate the risk of "man in the middle" attacks.

Another key interface is the X2 interface between eNode B's (see diagram below). X2 is also 3GPP defined but is an optional interface and some incumbent vendors have used proprietary messages over this interface thereby ensuring that multi-vendor networks are more difficult to deploy. This is a significant operational issue in deploying 5G in non-standalone mode (NSA is currently the predominant deployment model in the UK). The X2 interface is critical to 4G LTE networks as it supports network optimisation, load balancing within the network and helps to manage interference: if the X2 interface is not open, there is an in-built dependency on the existing 4G LTE vendors.

Open RAN and the Telecoms Security Bill

3GPP Interfaces



Potential Security Issues: 3GPP Standards Evolution to Open RAN

The work on developing a global standard for 5G is to be split into three different releases – Release 15, 16 and 17. Each release provides a set of functionalities that are stable at a certain point in time and can be implemented and new functionality and updates are then added to future releases.

Release 15 (which was finalized in 2019) paved the way for base stations to be logically split into a centralised unit and a distributed unit (CU/DU) with an interface (F1) between them. The CUs and DUs can be physically separated depending on the deployment and, provided the operator configures the network appropriately, the DU does not have any access to customer communications as it may be deployed at the very edge of the network (which would otherwise give rise to an increased security risk).

Another development of the O-RAN Alliance is to split the radio unit and the distributed unit (this is known as open fronthaul) so that each can be provided by different vendors. Whilst this gives increased diversity of choice for network operators it does also open up an additional attack vector. The key focus area for Open RAN standards bodies such as the O-RAN Alliance and the Telecom Infra Project is to ensure that there is a "security by design" approach and this is reflected in the working groups such as O-RAN Working Group 1 (Use Cases and Overall Architecture). This "security by design" approach will, we suspect, feature heavily in the Telecoms Security Bill, once it is enacted, and the Codes of Practice that will be issued under secondary legislation.

Open RAN and the Telecoms Security Bill

Telecoms Security Bill

- The draft Telecoms Security Bill which was introduced into Parliament on Tuesday introduces enhanced obligations on operators requiring them to take appropriate and proportionate measures for:
- Preparedness (i.e. identifying the risks of security compromises occurring; reducing the risks of security compromises occurring and preparing for the occurrence of security compromises);
- Prevention of adverse effects on the network or service or otherwise arising from security compromises; and
- Remedying and mitigating adverse effects that arise.

Additional features of the draft Bill include:

- a wide range of weaknesses or vulnerabilities will constitute security compromises even if confidentiality of signals or data on that network or service are not themselves compromised;
- further details will be set out in codes of practice giving guidance on measures that should be taken to comply with the TSRs;
- OFCOM's powers will extend to giving assessment notices to providers to impose duties to undertake or allow a range of actions to be undertaken including testing and inspection of networks, services, premises, equipment, documents and information .

Impact on the industry

Much will depend on what changes are made to the Bill as it makes its way through the UK Parliament. However, operators are clearly going to have significant misgivings about how practical the new security regime will be to implement and will want to ensure that their legal obligations are consistent with the standards work of 3GPP, the O-RAN Alliance and other standards bodies. Ultimately though, there is going to be increased scrutiny on the security aspects of industry developments such as Open RAN at a time when operators are continuing apace with 5G roll-out. The network solutions vendor community are also going to have to ensure that security principles continue to be at the forefront of their development and testing processes and that they continue to comply with industry standards such as the 3GPP SA3 Security Assurance Methodology and the GSMA Network Equipment Security Assurance Scheme.

Contact Details

Paul.graham@fieldfisher.com

Christopher.Eastham@fieldfisher.com