Written evidence submitted by TRL Technology

The Security of 5G

Authors: W Bennett and P Yates, TRL Technology Ltd

Caveat: This submission is based on publicly available source material.

About TRL Technology

TRL Technology is an agile UK-based company which designs, develops and delivers advanced electronic systems for the protection of people, infrastructure and assets when and where it matters. TRL Technology is also a recognised UK sovereign supplier of high-grade encryption solutions electronic-countermeasure solutions.

We create scalable solutions by investing in innovation and delivering excellence. Working in partnership with civil and defence organisations, we defend against evolving and emerging threats worldwide.

As part of the leading US defence supplier L3Harris, we are resourced to anticipate and support our customers' evolving needs, staying one step ahead of the threat in a changing environment.

Our flexibility comes largely from the fact that we have retained the ethos of a smaller company, where relationship building is paramount. The long-term customer, industry and in-country partnerships we develop pay huge dividends in terms of trust, responsiveness and our understanding of key issues.

Executive Summary

The impact of 5G technology will be widespread and far reaching into the prosperity of the United Kingdom. It will be structurally coupled with many critical and essential services, in such a way that their viability will be threatened if the underlying 5G network was compromised deliberately or by circumstances. The current instantiation of 5G is via technology that the UK has very little influence on, and reliant on a globalised supply chain that is itself, vulnerable and of unverifiable fidelity and provenance. We feel that the time is right to look again how 5G is deployed via the following principles:

- Sovereign Capability – the ability to manoeuvre without constraints.
- Security – Reliable and trusted Confidentiality, Integrity, Authentication and Availability of any solution.
- High Assurance – The confidence of provenance of deployed hardware and software.
- Prosperity Agenda – The best value for the UK in respect to jobs and commerce.
- Flexibility – the ability to take advantage of a delaminated architecture.

TRL Technology feel that there are a range of current and alternative approaches that meet the principles outlined above and would welcome further engagement.

Introduction

This submission explores the questions posed by the Parliamentary Defence Sub Committee on the Security of 5G. It sets out our ideas on how some of the challenges posed by the Committee, could be addressed. We welcome the chance to contribute to this important dialogue. We would welcome further discussion with the relevant stakeholders and organisations in order to investigate and validate the ideas presented.

We feel that the importance of 5G to the future prosperity of the UK, its allies and partners, along with recent changes in technology mean that the time is right to review the security of 5th generation mobile communications.

5G mobile wireless networking promises to deliver high-speed, low-latency, real-time services to billions of connected devices and will play an important role in our future, making 5G technology essential and integral to our daily life, security and economy. However, 5G architecture is more than just a higher speed wireless interface; it is a complete suite of hardware and software capability that in its ultimate instantiation, could be a complete network in its own right.

New core-network features of 5G, will make the network easier to customise, but at the same time introduce novel security challenges.

There are a limited number of 5G vendors, with market-leading Chinese company Huawei being viewed as presenting a “perceived risk” (HCSEC Oversight Board, 2019) and being excluded from sensitive aspects of the 5G network in the UK, which is now encouraging diversification of the UK's telco supply chain. While this is an important treatment of the potential risk, we feel that there are additional measures that could be taken to reduce that risk even further.

In addition, the industry is taking advantage of the rapid development of technologies such as virtualisation, commodity hardware and open source software to move away from monolithic architectures with the attendant hazards of vendor lock-in and inflexibility.

With our established reputation in cyber security and wireless systems, TRL Technology has an opportunity to provide guidance and the secure UK sovereign solutions which will ensure that users of these networks can have the required and necessary trust in them.

Our response is based on the following principles:

- Sovereign Capability – the ability to manoeuvre without constraints.
- Security – Reliable and trusted Confidentiality, Integrity, Authentication and Availability of any solution.
- High Assurance – The confidence of provenance of deployed hardware and software.
- Prosperity Agenda – The best value for the UK in respect to jobs and commerce.
- Flexibility – the ability to take advantage of a delaminated architecture

Our response

Our response is referenced to the questions posed from the Committee.

1. What are the risks to the UK’s 5G infrastructure? How can these be mitigated?

The general risks to the UK 5G infrastructure can be summarised as:

- Over dependence on a small set of overseas vendors, one of which (Huawei) are considered as presenting a “perceived risk”. This leads to vendor lock-in and lack of flexibility in sensitive areas such as selection of suitable encryption techniques, and interworking with other networks. Additionally, once dominant, the opportunity to herd users of technologies such as Wi-Fi, 4G and other communications technologies onto 5G would produce an unhealthy monopoly with the associated risks.
- The provenance of hardware (computer chips, electronic components) and software is difficult to establish without intrusive and costly techniques. This means that doubt is raised over the security and integrity of the deployed solution, with respect to hostile surveillance and potential disruption of traffic. TRL Technology routinely work to develop secure & managed supply chains as part of our provision of encryption solutions to HMG and MOD, and believe this approach can also be applied to specific elements of the 5G value and supply chain.
- Use of IP and similar enterprise derived protocols for core capability rather than “traditional” methods of signalling, routing and addressing. This means that the attack surface is a vast and complex system and vulnerable to a wide variety of cyber security weaknesses and attack methods.

The potential for 5G to carry important services as telemetry of Utilities (Water, Gas, and Electricity) and its ubiquity means that it should be viewed as Critical National Infrastructure. Additionally HMG almost exclusively uses commercial services for its routine and mission critical communications. The potential attractive pricing of 5G derived services, means that more and more CNI and Critical Communications will be carried over these means – with increased exposure to disruption and hostile surveillance.

Any mitigation measures should exhibit the following attributes:

- Low Overhead – Should present a low management burden
- Reduced Attack Surface – limit the opportunities for hostile action.
- No Undesirable Emergent Properties – understood behaviours
- Resilient To Malicious Modification – tamper resistant
- Stable – no race conditions or oscillations in behaviours
- Resilient: Failure\attack\attrition-tolerant control mechanisms.
- Secure: infrastructure meta-data may require protection
- High-Availability: reliable services

As a minimum, technical mitigation measures should include:

- Distributed monitoring and compliance solution
- Flexible reliable Micro-Services Architecture (MSA)
- A Trusted App store eco-system
- ‘Safe & Secure’ silo for Critical National Infrastructure (CNI)
- Root of Trust provision
- Evergreen patching

- Robust Orchestration
- Trusted Network Functions Virtualisation (NFV)
- Hardened Control layer

Cryptographic engineering techniques can be used as a basis to many of the above measures.

2. What is the role of government in 5G cyber security?

Government has a vital role to play in 5G Cyber Security. It should be responsible for setting the security requirements and the environment in which operators and vendors operate. It must ensure the UK has the maximum freedom of manoeuvre and trust in the operation and use of its CNI. We see that Ofcom and the NCSC as key in this approach. HMG should take a proactive stance in international standards bodies to ensure that future standards and protocols are benign and not capable of malicious use. HMG should encourage research and development with the UK industrial sector into secure 5G applications, components and alternatives to existing capabilities. With the rapid development of new communications technology (e.g. 6G Networks, Wi-Fi 6, virtualisation), it is critical that the UK is in the best position to exploit and benefit from this innovation.

3. To what degree is it possible to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components?

The nature of networks make it difficult but not impossible to segment by Vendor. Although standards do exist to facilitate interworking between vendors, the requirement for interworking and service equivalence mean that this is often costly in time and effort. Additionally, vendors will drive standards to benefit their own approach and make it difficult for new entrants to challenge their dominance. This is particularly prevalent when dealing with monolithic architectures.

One approach might be to delaminate the architecture using a technique similar to that proposed by DARPA (DARPA, 2020) in the US. This describes an opening up of the architecture to allow decoupling of hardware and software that allows the introduction of alternative functions from trusted suppliers. This could allow technology based on Open Standards (e.g. Open RAN) built on trusted UK sovereign hardware (e.g. software defined radios) to be introduced readily and cheaply.

4. What credible alternatives are available to Huawei systems?

Alternatives do exist to Huawei and ZTE – namely Samsung (South Korea), Ericsson (Sweden) and Nokia (Finland). These are seen as more attractive, but some questions remain on dependency, provenance of supply chain, interworking and architectural approach. Another approach would be to look at the opportunities presented by the Open Standards work done to support initiatives such as Open RAN (O-RAN Alliance e.V, 2019). This body looks at the use of commercial Software Defined Radio Hardware running an open standards based Radio Access Node Software Stack.

Vodafone are running proof of concept trials (Mobile Europe, 2019) to see if Open RAN could assist with deployment of broadband services in rural areas in the UK and overseas. With virtualisation and the use of commodity hardware, other open architecture solutions (OpenAirInterface, 2020) can now be proposed as alternatives to increasing large parts of the 5G architectural landscape.

Open RAN could be instantiated on hardware of known provenance (trusted chip sets and RF components), to create highly assured nodes that could form a solution for sensitive sites or geographies, or to provide an overlay for high assured services for a sub set of users.

5. To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?

A political dimension is inevitable in decisions of this magnitude. There are always trade-offs between price (affordability), timeliness, and technical capability. Also consequences can ripple out from the initial decision point that become political. However, in a post COVID-19 world it may be prudent to re-examine the decisions made to ensure that they are still valid, and are appropriate for the new geo-political landscape. In particular the reliance on fragile supply chains and the volatility of supply under times of crisis should be considered. There will be a need to look at shrinking supply chains, "Right shoring" and building in surge capability rather than "leaning out" spare capacity.

6. How will the UK Government's decision impact the UK's geopolitical position?

Former Foreign Secretary Jeremy Hunt has stated (Corera, 2020), "The issue is what happens if we get to the situation where no Western companies are really able to compete with Huawei going forward," he told the BBC. "Like it or not, in a decade's time people will look back and say, 'was this really wise to take this decision in 2020 that has led to this dependency?"

7. How will the UK's allies, particularly those in Five Eyes, respond to this decision?

We have seen other FYEY countries respond with an outright ban on using Huawei equipment, and the promotion of alternative technology or vendors. The UK seems to be in a unique position of a heavily restricted deployment by geography, functionality and network share. The FVEY community share several capabilities (F-35 Fighter and the Type 26 warship to name two) that share sensitive information. In certain operational scenarios, this might make interoperability a challenge due to presence of an untrusted sub system within the overall information system. This might lead to limiting of operational information sharing or the reduction in the quality of that information.

8. How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

The use of commercial systems is increasingly common within defence away from the immediate "fighting edge", although it is creeping in to many combat systems. 5G will form a major part of the commercial connectivity available and it will be increasingly difficult to disentangle from its influence – especially as service providers converge around a common core based on 5G architecture. This will mean that untrusted networks from high risk vendors will have to be accommodated at cost, if no alternatives can be found. This might negate the perceived cost savings from deployment of high risk vendor equipment.

9. How important it is for the UK, separately or with allies, to maintain industrial capability in this field?

To enable true operational freedom without reliance on high risk vendors it is critical that the UK and its allies maintain the ability to produce and operate their own equipment and services. This is especially important when if the potential value of the transformational nature of 5G derived services are to be realised.

The promise of Industry 4.0, AI and Cloud technology are dependent on a suitable network infrastructure. The benefits of these initiatives have the power to transform not just commercial enterprise, but also how Defence and Security carries out its business.

The UK has many sovereign companies that could produce some or all of the 5G capability. This would have the effect of generating prosperity in jobs and services around the development, deployment and export of trusted and assured 5G technology. This could be made more attractive by a joint FVEY proposition that would open up the markets of those countries and beyond to NATO and other partners. This could be an attractive proposition to the UK in a post COVID-19 and post BREXIT age, linking the UK prosperity agenda to valid national security concerns.

- END

15 April 2020

References

HCSEC Oversight Board, 2019. *Annual Report 2019,* London: HMG.

Corera, G., 2020. *Huawei 5G verdict is a decision 'with few good options'.* [Online]
Available at: https://www.bbc.co.uk/news/technology-51263799
[Accessed 14 April 2020].

DARPA, 2020. *Improving 5G Network Security.* [Online]
Available at: https://www.darpa.mil/news-events/2020-02-05
[Accessed 14 April 2020].

HCSEC Oversight Board, 2019. *Annual Report 2019,* London: HMG.

Mobile Europe, 2019. *Vodafone UK to deploy OpenRAN for rural coverage and greater capacity in cities.* [Online]
Available at: https://www.mobileeurope.co.uk/press-wire/vodafone-uk-to-develop-openran-for-rural-coverage-and-greater-capacity-in-cities
[Accessed 14 April 2020].

OpenAirInterface, 2020. *Software-defined 5G System.* [Online]
Available at: https://www.openairinterface.org/?page_id=466
[Accessed 15 April 2020].

O-RAN Alliance e.V, 2019. *Leading the industry towards open, interoperable interfaces and RAN virtualization.* [Online]
Available at: https://www.o-ran.org/
[Accessed 15 April 2020].