Long Term Evolution (LTE) / Fifth Generation (5G) mobile networks for military use

Douglas Stapleton, Andrew McLarty, Merlin Nichols
Department of Defence
Project Land 2072 Prime System Integration
Canberra, Australia
douglas.stapleton@defence.gov.au

***Abstract*—This paper [1] examines the key issues in adopting current LTE and future 5G networks to military usage. The bandwidth requirements on the modern battlefield are exploding, and heading beyond traditional voice communications to encompass video, imagery and data. One of the more attractive and promising means of resolving the tactical bandwidth requirements for current and future operations is the consideration of 4G LTE and 5G mobile networks. In fact, 4G LTE networks are already in military service in many countries whereas; 5G networks are gaining credibility as high speed data transmission mediums. The two key features of 5G, being its near-zero latency and data rates of 1–10 Gbps, will change the possibilities for battlefield communications.**

Traditional battlefield communications have been constrained to a twofold view of the world; a high speed tactical backbone suitable for intra-headquarters usage and much lower capacity mobile tactical communications for the deployed land force. Future communications systems will inevitably require low latency and high bandwidth, such as is envisioned for 5G. This will enable a re-think of military communications networks towards one generic style node without today's distinction between high speed backbone and low capacity tactical communications.

Keywords-4G; LTE; 5G; battlefield communications

I. BACKGROUND

As David Kilcullen noted in his paper *The Australian Army in the Urban, Networked Littoral*, the Army will operate in the future in an environment that is increasingly networked:

"As the Australian Army leaves Afghanistan, the urban littoral will rise in importance simply because Australia's primary operational environment (POE) is overwhelmingly littoral and increasingly urbanised. But we no longer face the littoral of which Ralph Peters or Charles Krulak wrote in the 1990s – in the pre-mobile phone era, before significant penetration of the Internet into the developing world. Today we face an urban, networked littoral. The explosion of electronic connectivity changes both the environment and the threats we may encounter within it."

Defence forces around the globe are experiencing difficulties in meeting the data requirements of their deployed forces. Demand for voice, data and video services are filling data capacities as quickly as capacity is increasing. Current military bespoke technologies are not keeping pace with commercial developments. Modernisation of commercial technologies has seen increases in data bandwidth availability exceeding an order of magnitude each decade. Defence capabilities have not kept pace with these developments.

The use of cellular mobile phone technologies is entrenched in the Australian Defence Force for the strategic or fixed environments. This paper focusses on the communications system to support the future data requirements of the field deployed forces.

Australia is heavily dependent on satellite technology for field deployed high capacity communications bearers to link forces to formation headquarters and higher command elements.

Existing Land communication systems have evolved around the organisational structure of the Australian Army which, with its requirement for high mobility, makes it difficult to provide adequate bandwidth to the deployed force. In recent years tactical operations have experienced a significant demand for improved services and applications down to lower levels of the deployed force. The two requirements are now in conflict with current tactical equipment struggling to meet the increasing requirements for bandwidth.

One of the more attractive and promising means of resolving tactical bandwidth requirements for current and future operations is 4G LTE or 5G networks.

In fact, 4G LTE networks are in service in many countries around the world with 5G networks already gaining credibility as high speed data transmission mediums. These developments effectively bring LTE/5G technologies onto the Defence planning horizon.

II. PROBLEM STATEMENT

The bandwidth requirements on the modern battlefield are exploding, and heading beyond traditional voice communications to encompass video, imagery and data. For example, Army vehicles will become increasingly networked for logistic and tactical information. This will build up a second machine oriented set of end points in the new Battlespace network.

[1] *The views in this paper are those of the authors and do not represent the views of JP2072 or the Department of Defence.*

These statements are supported on a Networked Battlespace Concept as articulated in The Army Objective Force 2030 (AOF 2030) Handbook [1] and aligned with the Australian Defence Force (ADF) Network Centric (NCW) Roadmap:

"8.31 The AOF 2030 Communications and the Network (C&N) system will connect people and technology, providing a free flow of data across the battlespace and thus enabling knowledge. The C&N system will be pervasive across the AOF 2030, with all sensors and systems closely integrated and forming a seamless network of actors which rapidly share data. This data will be utilised to compile information from which intelligence can be derived and knowledge gained."

To summarize the requirement, the future battlefield network must further enable Command and Control (C2), secure voice, secure data, secure video streaming (including full motion video (FMV)), dynamic targeting, logistics requests, individual location reporting, fused Common Operating Picture (COP) and Battlefield Damage Assessment (BDA) [2].

There is, however, an increasing reliance on sensor data and special applications such as Battle Management Systems and other applications. This will force a rethink in how these applications are made available to the ordinary soldier and thus flatten the network hierarchy. For example, general situational awareness (SA) at the tactical edge can be enhanced by better map displays, etc.

The future model will need to take account of developments where many military devices will be networked together along with sensors and individual soldiers. This may ultimately see an individual soldier as a 'node' with their own 'Personal Area Network' to connect the local devices providing tactical logistics, health and positional data.

The connectivity required at each node may soon revolve around one nodal pattern that will then link the node to the next node in the chain. Bearers will be used to link the node to the next node on the battlefield; line of sight radio, satellite etc. In this pattern, the users and their devices will connect to the node infrastructure, which will then use the Network Planning Management System (NPMS) to link out through bearers provided to that node. This will end the deployed/mobile design distinction at the high level design pattern along historical lines which was constrained to high-speed bearers at the headquarters level only.

There is broad availability of LTE smart phones in the market, replacing the clunky and expensive handsets associated with legacy military networks. The advantage of more modern technology also includes greater parts availability, competitive pricing, and interoperability. There is of course the balancing argument between ruggedised and thus more environmentally survivable end units compared to a replacement strategy for commercial handsets on failure, for example. LTE then delivers higher speeds and lower latency than competing technologies, such as the recently terminated Joint Tactical Radio System (JTRS). The all-IP network is standards based, allowing the military to take advantage of a large ecosystem of vendors for the radio and core networks [3].

What is the future of specifically developed military solutions in the personal communications era? There will always be a place for robust, hardened, communications that will withstand EW and nuclear threats, untethered to fixed infrastructure and able to be taken off road. However, a key example of the difficulties is shown by the career of the Joint Tactical Radio System, (JTRS), which lasted from 1997 until 2012 when the program was terminated after an expenditure of approximately USD 15 billion. Fundamentally, the commercial world was able to develop superior speeds in communication products, partly because these are built to utilise fixed infrastructure. One severe disadvantage of a military developed product is the small research and development base, compared to the market driven research areas that are leveraged by the commercial offerings. Commercial-off-the-shelf (COTS) products are faster to market, maintainable with good system longevity. They adhere to LTE standards-based architecture with resultant maturity, reliability and scalability.

Figure 1. illustrates that the trend line shows how purely military developed communications infrastructure is falling behind 4G LTE and this trend will be exacerbated by the introduction of 5G network capability [3].

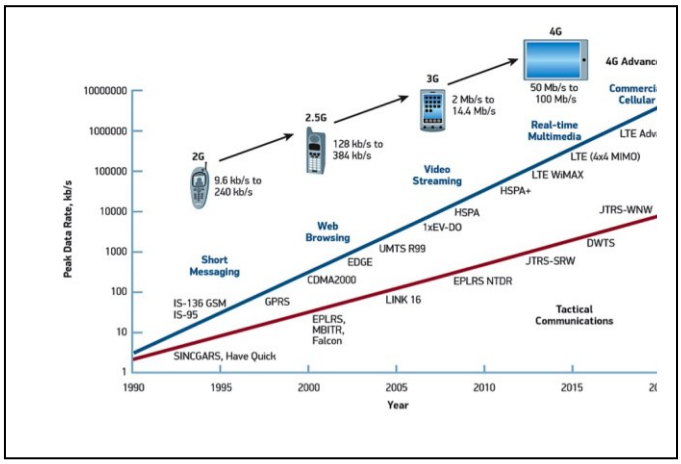

Figure 1. Commercial LTE technology outpacing proprietary alternatives

III. FUTURE LAND NETWORK DESIGN CONSIDERATIONS

What are the major drivers around communications technology over the next 3 to 7 years?

In fixed telecommunications infrastructure, the current 4G LTE networks are still developing with current projects indicating 5G networks should begin to appear around 2020. Australia has already seen Telstra[2] and Optus[3] introduce 4.5G capabilities. These announcements effectively bring 5G technologies onto the planning horizon for the future Land Network and ready for consideration as one of the more attractive medium to long term options.

Near zero latency and high data rates in LTE/5G will make the current distinctions between the high speed backbone at the

[2] https://www.cnet.com/au/news/telstra-5g-2018-1gbps-4g-upgrade/

[3] http://eftm.com.au/2017/02/optus-announces-5g-network-plans-launches-gigabit-4-5g-mobile-network-36819

headquarters' level and lower speed tactical systems applicable to soldiers, a moot point; assuming that size, weight and power constraints allow the technology to roll down to the tactical level of operations.

The next question is, when the commercial world is on the verge of deploying high speed capable LTE/5G networks, how can these COTS based systems be adapted to military usage?

1. Noting the military requirement for deployed and mobile networks to be capable of being independent of commercial infrastructure, there may be circumstances where the surrounding network availability becomes useful in a military context. Usage of 5G in Australia will become part of society's infrastructure and can be used to support the bulk of the military traffic patterns; that is when the Army elements are located near fixed infrastructure and can natively take advantage of the commercial networks (via secure gateways). On deployment, the host nation of the conflict may have 4G/5G communication facilities available. In fact these facilities may become increasingly important to both sides of a conflict leading to a "Geneva Convention" type protection for in-theatre communications assets; although from a military perspective they can only be regarded as supplemental assets not a replacement for the Army's own organic communications capability. Even in an Area of Operations, the larger headquarters are often set back from the conflict; perhaps even in another country where it is reasonable to pay for use of the host nation's communication infrastructure or accessible satellite communications. Cost may be a substantial factor in the balance between use of in-country facilities and the cost of bringing in deployed equipment. The assessment of acceptable risk levels may differ between the operational to strategic level compared to the tactical level.

2. Range extension can take 5G connectivity with the army on deployment and manoeuvres. That range extension can come from a variety of sources, such as satellite; UAV above the troops with switching equipment on-board , portable 5G nodes that are deployed in the wake of the Army as it moves forward; i.e. dropped on the ground for a short operational life span (allowing for backward connection and then into the meshed network).

3. Protection of military data across the commercial networks through highly secure encryption that matches the data's classification and longevity.

IV. 5G

The Australian Communications Management Authority paper on *5G and mobile network developments - Emerging issues* makes the point that; "Australia has benefited from progressive investments and upgrades in mobile network capabilities and service deployments" [4]. Successive generations of mobile technologies have been deployed in Australia approximately every ten years. 5G represents the next expected evolution in mobile technologies, with the first commercial deployments in Australia expected from 2020. There are two defining requirements for 5G that separate it from previous developments. They are its near-zero latency and data rates of 1–10 Gbps.

These two features support an 'anytime, anywhere, anyone and anything' capability of 5G, which is expected to play a role in supporting a wider deployment of the Internet of Things (IoT) in Australia.

Specific requirements for 5G (source: GSMA Intelligence) provide these commercial, end-user expectations:

- Data rates 1–10 Gbps connection to an end point in the field
- Near zero latency: 1 millisecond end-to-end round trip
- 1,000 times more bandwidth per unit area
- 10 to 100 times more connected devices
- Perception of 99.999 per cent availability and 100 per cent coverage
- 90 per cent reduction in network energy usage
- Up to 10-year battery life for low power, machine-type devices (reflecting a designed low power usage, actual results are device dependent)"

5G rests on four key pillars – new air-interface, flexible spectrum allocation, network function virtualization (NFV) and software-defined networking (SDN). NFV and SDN work in conjunction to enable new network management concepts such as network slicing, ultra-high reliability and native multi-tenancy. These pillars work together to optimize end-to-end latency and provide a seamless user experience. NFV is a network architecture concept that enables the separation of hardware from software or 'function', and has become a reality for the mobile industry due to the increased performance of COTS IT platforms. SDN is an extension of NFV wherein software can perform dynamic reconfiguration of an operator's network topology to adjust to load and demand, e.g. by directing additional network capacity to where it is needed to maintain the quality of user experience at peak data consumption times.

V. Proposed Node Concept

Future deployed land communications can be modelled on one network node concept based on 5G connectivity being available to all end users and their devices.

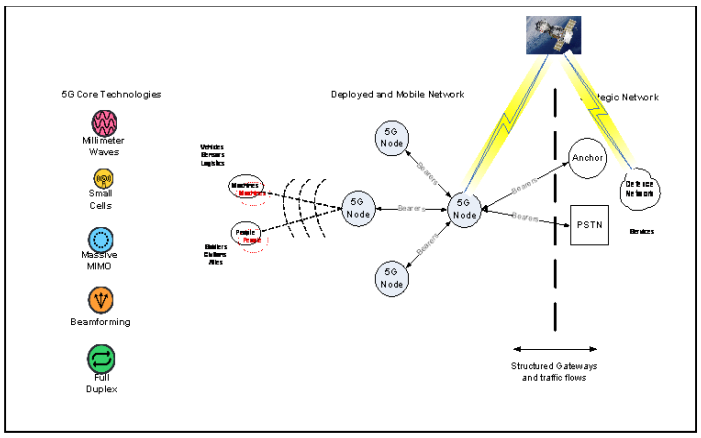

Figure 2. Proposed 5G Node Concept

On the left hand side of Figure 2. the core 5G technologies are illustrated from the IEEE Spectrum article on *Everything You Need to Know About 5G*[4]. Millimeter waves, massive MIMO, full duplex, beam forming, and small cells are just a few of the technologies that will enable ultra-fast 5G networks. These technologies have been individually demonstrated to a level of maturity that enables them to be considered, as a group, to underpin the design claims for 5G networks.

Figure 2. illustrates that regardless of location, all end user devices or machine endpoints will use 5G to connect to their local node. When the node is located near civilian infrastructure, the node could make use of commercial connectivity via a secure gateway with specific encryption to protect the military nature of communications; acknowledging the additional risks for cyber and signature.

There is a security aspect, apart from encryption, to the concept of sharing bearers across commercial 5G infrastructure. Each 5G node within a military deployment will relate to other 5G nodes in that same military deployment. The military force may effectively become its own 5G network provider. However, to transition across commercial bearers will necessitate transitioning across a secure gateway at defined points in the network topology.

This brings about a fundamental change in the way that reliable voice is delivered by the network, to provide a better, more stable and secure outcome. Older military networks were originally oriented towards voice traffic, to which a data capability was added. The new 5G networks are fundamentally high speed data networks over which voice is carried as but one application. This is currently done on the 4G LTE networks through VoLTE (Voice over LTE). From 4G networks onwards, the voice features allow for "precedence" for emergency first responders. This allows for the pre-emption of voice communication. This capability may contribute towards the military quality of service and prioritisation requirements allowing for commanders to pre-empt voice communications in time of crisis.

VI. Security Threats

Whilst it is noted that military systems have been built to exist in a more hostile and challenging environment both from a physical and electronic perspective, future commercial technologies including LTE and 5G are being developed conscious of a more hostile RF spectrum based on having to address self-interference and high network density.

A. Electronic Warfare

Electronic Warfare (EW) is the component of information operations which exploits the use of the RF spectrum to gain an advantage over an adversary. The US Army defines Electronic Warfare as:

"Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES)" [5].

The manual goes on to define:

1) "Electronic Attack

EA is the use of jamming, electronic deception, or directed energy to degrade, exploit, or destroy the adversary's use of the EMS. EA can attack the adversary anywhere—from his tactical formations, back to his national infrastructure.

2) Electronic Protection

EP is the protection of the friendly use of the EMS. EP covers the gamut of personnel, equipment, and facilities. EP is part of survivability. As an example, self and area protection systems can interfere with the adversary's target acquisition and engagement systems to prevent destruction of friendly systems and forces" [5].

In this paper, concern is mostly of an adversaries EA capability and the EP mechanisms which could be used to counter these effects. This paper investigates some of the challenges facing the adoption of 4G LTE or 5G solutions to meet the needs of future deployed land force.

3) Electronic Warfare Considerations

Domination of the electromagnetic spectrum is a crucial component of most modern military operations. There are few battlefield elements that do not rely on communications and information systems [6]. RF jamming creates a localised 'Denial of Service' (DoS) of the targeted Radio Access Technologies (RAT). Barrage jamming has the same effect on the LTE or 5G signals as other radio systems. Attacks which focus on specific elements of the LTE signal have been proven to be more effective. Some of these attacks require time synchronisation with the target signal which significantly adds to the complexity of performing the exploit.

The LTE downlink signal uses a multiple carrier signal called Orthogonal Frequency Division Multiple Access (OFDMA). Each OFDMA sub-carrier carries a separate stream of information. LTE protocols are vulnerable to radio jamming; Lichtman et al. [7] investigated the effectiveness of a number of jamming techniques. Analysis revealed that attacks were far more effective if they were synchronised with the elements of the downlink or uplink signal. The paper concluded that LTE is extremely vulnerable to adversarial jamming.

Rover et al. [8] investigated several attacks targeting Radio Access Networks (RAN) identifying some potential mitigating factors and suggested topics for future research. These can be summarised as the use of frequency spreading techniques, signal randomisation and encryption techniques for consideration in future standards, which may also be applicable to retro fit in a private military or emergency service network.

Rogue base stations cross the boundary between cyber and EW as they are reliant on a jamming attack to initiate the User Equipment (UE) moving from their base station to the rogue system. Future developments need to provide mutual authentication between network devices to prevent such attacks.

[4] http://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g

B. IP Based Vulnerabilities - Exploits

The draft 5G Security Architecture [9], provides a definition of the security problem for 5G networks from the perspective of the commercial entities involved in delivering a public system. A view on whether governments or specifically military and emergency service elements are having any influence on the development of the 5G standards does not appear to be publicly available.

The development of the Transmission Control Protocol and Internet Protocol (TCP/IP) stack was done with little consideration of security and operation in a hostile environment. There is a long history of exploits made available by targeting the shortcoming in various implementations of Internet Protocol (IP) Version 4. Reference [10] provides an analysis of IP V4 .

Adoption of IP v6 does not prevent these problems whilst some IPv4 issues are resolved, IPv6 introduces an additional set of issues to be mitigated.

If possible the land communications network should be limited to the use of IPv6 with IPv4 disabled throughout the network to reduce the potential attack surface.

C. Technology Exploits

1) International Mobile Subscriber Identity (IMSI) protection

International Mobile Subscriber Identity (IMSI) protection was provided in the 3G standards; however attacks which make a UE revert to 2G (GSM) make it vulnerable. The IMSI is passed at call connection to enable a UE to be granted resources from the base station.

2) Rogue Base Stations

IMSI catchers, stingrays or GSM interceptors as they're also called, force a phone to connect to them by emitting a stronger signal than the legitimate towers around them. Once connected, pings from the phone can help the rogue tower identify a phone in the vicinity and track the phone's location and movement while passing the phone signals on to a legitimate tower so the user still receives service [11].

These devices once they have captured a UE can perform a number of attacks. One approach is a simple DoS by capturing the UE but not providing any resources. A similar attack informs the UE to shut down its RAT as no service is available. Another class of attack involves downgrading the encryption protocol to none or an easily cracked algorithm to permit eavesdropping on the transmissions which the rogue station passes on to a carrier's node [12].

3) Multiple WiFi protocols

As most new UEs are equipped with the capability to use multiple RAT and wireless local area networking (WiFi) protocols. The availability of these interfaces increase the attack surface available to exploit. As UE are configured to be either a subscriber on a network or perform as an Access Point (AP) they are vulnerable to attacks targeting both.

Proper configuration of security settings and disabling unused services will assist in limiting or the prevention of these attacks.

4) Network Function Virtualisation and Software Defined Networking

NFV and SDN are two key concepts for the delivery of future complex networks. We have seen the emergence of virtualisation technologies such as VMware and Microsoft Hyper-V taking over the hosting of hundreds of thousands of servers in data centres around the world in the recent years.

VMware NSX is the network virtualisation and security platform for vSphere and other hypervisors such as OpenStack [13].

> *"The solution de-couples the network functions from the physical devices, in a way that is analogous to de-coupling virtual machines (VMs) from physical servers. In order to de-couple the new virtual network from the traditional physical network, NSX natively re-creates the traditional network constructs in virtual space — these constructs include ports, switches, routers, firewalls, etc"* [13].

SDN has rapidly developed and is now being deployed in production environments. SDN facilitates the separation of the control and packet forwarding capabilities of the network. Reference [14] recommends six technical considerations for SDN and NFV:

a. Mandate encryption and authentication in [North Bound Interface][5] NBI, [South Bound Interface] SBI and [East-West Bound Interface] EWBI.

b. Identify and monitor exposed functionalities of SDN controllers.

c. Control and monitor running application resources.

d. Holistic Support for Security policies.

e. Access control, Credentials, System updates

f. Sandboxing, Application Isolation.

The report also provides three recommendations for organisations:

a. Develop incident response capabilities and information sharing practices among telecom operators.

b. Keep systems up to date.

c. Use adequate security methods.

These recommendations provide a sound basis for the development of the security policies for a future land network.

5) Multiple technologies 2G, 3G, 4G, and 5G coexistence

Multiple technologies 2G, 3G, 4G, and 5G coexistence enable some of the attacks already mentioned such as ISMI catchers, above.

It is suggested that careful consideration of which technologies will be enabled to ensure that the attack surface is minimised.

[5] This is the terminology to describe the interfaces between layers of the SDN

Reference [15] identified the convergence of network technologies as being a contributor to the increasing risk presented by 5G networks. These threats are proposed from a consideration of vulnerabilities presented by current 2G, 3G and 4G legacy systems. 5G networks are considered the most attractive targets for future attackers. He proposed the following topics for consideration:

6) Mobile Malware Attacks Targeting EU

Some recent examples of malware attacks against Google's Android operating system and Apple's OSX operating system.

New malicious code exploiting OSX called "Komplex", appears to be targeting the aerospace industry discovered by researchers from Palo Alto [16]. Komplex is a Mac Trojan which is capable of downloading and installing additional files and deleting existing files.

Malware known as Dok targets computers running OSX. It has targeted users in Europe through spam emails. The malware uses "nag screens" that ask the user to install an update, but which really is seeking the user's admin password. Dok affects all versions of OSX. Apple has revoked a legitimate developer certificate that allowed the malware to eavesdrop on secure HTTPS traffic [17].

Spyware known as Pegasus, which was detected last year targeting iOS devices, now has a variant that targets Android devices, according to Google and security company Lookout. Pegasus was being used to spy on human rights activists and journalists around the world. The Android variant, which Google has named Chrysaor (Pegasus's brother in Greek mythology), can log keystrokes, take screenshots, and read messages in various applications. It uses the device's microphone and camera to spy on target. Chrysaor can also remove itself from the device [18].

7) 5G Mobile Botnets

With the deployment of 5G comes the convergence of the IoT, Internet and the global mobile telephone network. The term botnet is derived from the words robot and network. A bot in this case is a device infected by malware, which then becomes part of a network, or net, of infected devices controlled by a single attacker or attack group [19]. Any IP enabled device on a network could be exploited to act as bot to be used to contribute to a denial of service (DOS) attack. These attacks are generally targeted at the host operating system of the UE but could also be directed toward equipment comprising the network core.

D. Access Networks

1) UE Location Tracking

The primary component of these breaches is Signal System 7 (SS7) protocol. As this protocol originated in the Public Switched Telephone network where all parties were trusted. No security measures were implemented [20]. It has been demonstrated that SS7 attacks are still applicable to eavesdropping on SMS messaging.

Attackers recently exploited vulnerabilities in the SS7 protocol to steal money from bank accounts protected with two-factor authentication. The SS7 protocol allows mobile phone networks to talk to each other. The attacks, which began in January 2017, exploited flaws in SS7 to intercept text messages with mobile transaction authentication numbers (mTANs) or single-use passwords sent by banks as part of two-factor authentication schemes for funds transfers [21].

2) HeNB Femtocell Attacks

The Home eNodeB (HeNB) is the 3GPP's term for a LTE femtocell or Small Cell. A HeNB performs the same function as an eNodeB, but is optimized for deployment for smaller coverage than macro eNodeB, such as indoor premises and public hotspots [22]. As HeNB will be similar to the current series of home routers they will be subject to similar issues:

a. Physical Attacks on HeNB

b. Attacks on HeNB Credentials

c. Configuration Attacks

d. Protocol Attacks

3) User Data and Identity Privacy Attacks

Rogue eNodeB and Wi-Fi node access points permit eavesdropping on user data and tracking UE in the network. Future developments of the standards will hopefully remove some of these issues by forcing the protocols to be more secure.

E. Mobile Operator's Core Network

Greater processing power, increased bandwidth and increasing number of UE provide the platform to deliver Distributed Denial of Service (DDoS) attacks of increased magnitude. The Core Network will need to implement measures to minimise the effects of DDoS attacks targeting its components.

Lack of authentication between the eNodeB and the up-stream network will mean that the network will be vulnerable to IP-based attacks, the severity of which will be compounded by the lack of encryption on the data and signalling traffic.

F. External IP Networks

Being IP based, 4G LTE and 5G networks will be susceptible to compromise from connected networks which have been compromised. Normal network security measures including firewalls, intrusion prevention and network segmentation will help to mitigate this issue.

VII. CONCLUSION

The future is beginning to look like a high-speed low-latency data network supporting applications across the battlespace. Voice will be but one application on the data network, unlike heritage networks which have been primarily voice radio networks with limited bandwidth available for data, as an addition. 5G becomes a broader specialised network, with a simpler node pattern concept. Future military organisations may become operators of their own 5G networks that will reach out to utilise commercial 4G/5G networks as the opportunities arise.

Future deployable communications systems will require defensive capabilities against cyber-attacks due to them being purely IP based systems. A network architecture containing proper placement of border protection, intrusion prevention and

network segmentation will be the first layer of defence. The system design needs to provide a robust identity and authorisation system to ensure that the system only hosts authorised entities. Proper use of authentication and encryption between devices will help to eliminate attacks perpetrated by devices masquerading as network elements.

Development of the standards for 5G are addressing system generated interference and providing technology which will assist defence forces in the deployment of 4G and in the future 5G in a secure and robust manner. Little research is being conducted to address the use of this technology in an environment with an aggressive EW adversary.

VIII. RECOMMENDATION

As 5G standards are still under development numerous researchers referenced in this paper have suggested changes that could be made to current or future standards to mitigate a significant number of the threats mentioned.

Future developments need to provide mutual authentication on both signalling and data channels between network devices to prevent rogue devices masquerading as network nodes.

Proper configuration of security settings and disabling unused services will assist in limiting or the prevention of attacks exploiting characteristics of the available RAT.

Use reference [14] recommendations for SDN and NFV in the development of the security policy for the future network.

Normal network security measures including firewalls, intrusion prevention and network segmentation will help to mitigate IP based attacks originating both internally and externally.

Mitigation measures for attacks targeting RAT can be summarised as; the use of frequency spreading techniques, signal randomisation and encryption techniques for consideration in future standards

In terms of network research for the broader Defence community of interest, it is recommended that Defence endorse future research on methods of protecting LTE and 5G from smart jamming attacks.

References

[1] Department of Defence, The Army Objective Force, 2 ed., Puckapunyal: Australian Army Headquarters, 2011.

[2] K. Brown, "Enhancing Battlefield Communications through 4G LTE+ Cellular Technology," *Journal of Battlefield Technology ,* vol. 18, no. 3, November 2015.

[3] H. Jensen and J. Sharp, "LTE Infrastructure for today's military networks," Radisys Corporation, 2013. [Online]. Available: http://picmg.mil-embedded.com/articles/lte-infrastructure-todays-military-networks/. [Accessed 17 Mar 2017].

[4] Australian Government, "5G and mobile network developments- Emerging issues", ACMA - 2016," researchacma, February 2016. [Online]. Available: http://www.acma.gov.au/theACMA/~/media/47F68EC7164A4BBD88D29D1420ADA3A4.ashx. [Accessed 17 March 2017].

[5] Headquarters, Department of Army, Field Manual - Information Operations (FM 100-6), 27 August 1996 ed., Washington, DC, Department of Army.

[6] C. Benson, M. Frater and M. Ryan, Tactical Electronic Warfare, Canbarra: Argos Press, 2007, p. 12.

[7] M. Lichtman, J. Reed, T. Clancy and M. Norton, "Vulnerability of LTE to Hostile Interference," IEEE, Blacksburg, 2013.

[8] R. Jover, J. Lackey and A. Raghavan, "Enhancing the security of LTE networks," *EURASIP Journal on Information Security,* vol. 2014:7, pp. 1-14, 2014.

[9] 5G Ensure, "Deliverable D2.4 Security Architecture (draft)," 5G PPP, 2016.

[10] IETF, "Security Assessment of the Internet Protocol Version 4," Internet Engineering Task Force (IETF), UK, 2011.

[11] K. Zetter, "Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls," CryptoPhone, 2014. [Online]. Available: https://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers/. [Accessed 6 May 2017].

[12] H. Lin, "Forcing a Targeted LTE Cellphone into an Eavesdropping Network," Amsterdam, 2016.

[13] SDX Central, "What is VMware NSX," 2017. [Online]. Available: https://www.sdxcentral.com/products/nsx/. [Accessed 6 May 2017].

[14] A. Martin, L. Marinos, E. Rekleitis, G. Spanoudakis and N. Petroulakis, "Threat Landscape and Good Practice Guide for Software Defined Networks/5G," European Union Agency For Network And Information Security, Heraklion Crete, 2016.

[15] J. Rodreguez, Security for 5G Communications in 5G Mobile Networks, J. Rodreguez, Ed., Chichester: John Wiley & Sons Ltd, 2015, pp. 207 - 219.

[16] J. Vrijenhoek, "New 'Komplex' Trojan Malware Targeting Macs [Updated]," 2016. [Online]. Available: https://www.intego.com/mac-security-blog/new-komplex-trojan-malware-targeting-macs. [Accessed 6 May 2017].

[17] SANS Institute, "Dok Mac Malware Signed With Valid Certificate," *SANS NewsBites,* vol. 19, no. 035, p. 1, 1 May 2017.

[18] SANS Institute, "Pegasus Spyware Variant Chrysaor Affects Android," *SANS NewsBites,* vol. 19, no. 028, p. 1, 6 April 2017.

[19] M. Rouse, "botnet - Definition," 2017. [Online]. Available: http://searchsecurity.techtarget.com/definition/botnet. [Accessed 6 May 2017].

[20] K. Nohl, "SS7 Attack Update and Phone Phreaking," Berlin, 2016.

[21] SANS Institute, "SS7 Flaws Exploited in Online Bank Account Heists," *SANS NewsBites,* vol. 19, no. 036, p. 2, 5 May 2017.

[22] Alcatel-Lucent, "Home eNodeB (HeNB)," 2017. [Online]. Available: https://infoproducts.alcatel-lucent.com/html/DN09131794/htm/docs/mme_feature_overview/c159895329/c159895329.html. [Accessed 3 May 2017].