Contents:

Pg. 1

Summary
Vulnerabilities for Operate Through
NIST NVD Listed

Pg. 2-6

Literature Review of 5G Vulnerabilities

Pg. 6-8

Active Foreign Commercial 5G Networks

Pg. 8

Literature Review of Other Pertinent 5G-Related Items of Interest

Pg. 9-13

Sources

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

5G Network Vulnerabilities for Operate Through Quarterly Update (Q4-2023)

Summary

This report summarizes information on vulnerabilities associated with the 5G network that potentially could be employed or leveraged by an untrusted network operator. The report is in support of the Under Secretary of Defense for Research and Engineering (OUSD R&E) 5G Operate Through Program. The information in this report is based on open-source material published or made available between 1 June and 31 August 2023.

5G Network Vulnerabilities for Operate Through

The vulnerabilities in this section were obtained from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). Vulnerabilities that are of direct interest for the Operate Through program, as well as 5G-related vulnerabilities of potential general interest, are included.

Vulnerabilities Listed in NIST NVD

NIST CVE-2023-26072: An issue was discovered in Samsung Mobile Chip Set

CVSS Severity V3.x: Critical; V2.0 (Not available)

https://nvd.nist.gov/vuln/detail/CVE-2023-26072

An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list.

NIST CVE-2023-26073: An issue was discovered in Samsung Mobile Chip Set

CVSS Severity V3.x: Critical; V2.0 (Not available)

https://nvd.nist.gov/vuln/detail/CVE-2023-26073

An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list.

NIST CVE-2023-26074: An issue was discovered in Samsung Mobile Chip Set

CVSS Severity V3.x: Critical; V2.0 (Not available)

https://nvd.nist.gov/vuln/detail/CVE-2023-26074

An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions.

NIST CVE-2023-26075: An issue was discovered in Samsung Mobile Chip Set

CVSS Severity V3.x: Critical; V2.0 (Not available)

https://nvd.nist.gov/vuln/detail/CVE-2023-26075

An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List.

NIST CVE-2023-26076: An issue was discovered in Samsung Mobile Chip Set

CVSS Severity V3.x: Critical; V2.0 (Not available)

https://nvd.nist.gov/vuln/detail/CVE-2023-26076

An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options.

Literature Review of 5G Vulnerabilities for Operate Through

The following section summarizes open-source literature focused on 5G-related vulnerabilities that either directly pertain to 5G Operate Through or are of potential general interest.

Attacks and Threats Verification Based on 4G/5G Security Architecture

17 June 2023

https://link.springer.com/chapter/10.1007/978-3-031-35836-4_26

Abstract: 5G networks are in high demand and are expected to transform many industries, including finance, healthcare, transportation, and entertainment, shaping the future of communication. Although the 3rd Generation Partnership Project has developed several cybersecurity protocols, vulnerabilities in these agreements still exist. These vulnerabilities can lead to security attacks on mobile devices during the registration process of the base station or wireless access, such as Data Leaking attacks, Denial-of-Service attacks, and Downgrade attacks. This study aims to analyze and experiment with relevant attack cases, identify existing information security vulnerabilities in the mobile network, and test the 4G/5G network security protocol for vulnerabilities through active attacks to demonstrate their impact on mobile devices. By doing so, this project aims to contribute towards the development of stronger and more secure mobile communication technology.

Assessment: This article aims to analyze and experiment with attacks such as Data Leaking attacks, Denial-of-Service attacks, and Downgrade attacks. This paper is a survey paper that focusses on testing the security vulnerabilities in the 4G/5G mobile network security protocols that will arise in a 5G – Non-Stand Alone (NSA) deployments.

Security and Privacy Vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective

13 December 2022

https://www.sciencedirect.com/science/article/pii/S1389128622005497

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

Abstract: Spectrum scarcity has been a major concern for achieving the desired quality of experience (QoE) in next-generation (5G/6G and beyond) networks supporting a massive volume of mobile and IoT devices with low-latency and seamless connectivity. Hence, spectrum sharing systems have been considered as a major enabler for next-generation wireless networks in meeting QoE demands. Specifically, the 3rd generation partnership project (3GPP) has standardized coexistence of 4G LTE License Assisted Access (LAA) network with WiFi in the unlicensed 5 GHz bands, and the 5G New Radio Unlicensed (NR-U) with WiFi 6/6E in 6 GHz bands. While most current coexistence solutions and standards focus on performance improvement and QoE optimization, the emerging security challenges of such network environments have been ignored in the literature. The security framework of standalone networks (either 5G or WiFi) assumes the ownership of entire network resources from spectrum to core functions. Hence, all accesses to the network shall be authenticated and authorized within the intra-network security system and is deemed illegal otherwise. However, coexistence network environments can lead to unprecedented security vulnerabilities and breaches as the standalone networks shall tolerate unknown and out-of-network accesses, specifically in the medium access. In this paper, for the first time in literature, we review some of the critical and emerging security vulnerabilities in the 5G/WiFi coexistence network environment which have not been observed previously in standalone networks. Specifically, independent medium access control (MAC) protocols and the resulting hidden node issues can result in exploitation such as service blocking, deployment of rogue base-stations, and eavesdropping attacks. We study potential vulnerabilities in the perspective of physical layer authentication, network access security, and cross-layer authentication mechanisms. This study opens a new direction of research in the analysis and design of a security framework that can address the unique challenges of coexistence networks.

Assessment: The 3 GPP has standardized coexistence of the 5G New Radio Unlicensed (NR-U) with Wi-Fi 6/6E in 6GHz band leading to higher utilization of the spectrum. However, such an arrangement has been shown to have security vulnerabilities and breaches that can be tolerated by standalone networks but are a serious threat to spectrum sharing networks as surveyed in this paper leading to hidden node related security attacks.

5G RRC Protocol and Stack Vulnerabilities Detection via Listen-and-Learn

17 March 2023

https://ieeexplore.ieee.org/abstract/document/10059624

Abstract: The paper proposes a protocol-independent Listen-and-Learn (LAL) based fuzzing system, which provides a systematic solution for vulnerabilities and unintended emergent behavior detection with sufficient automation and scalability, for 5G and nextG protocols and large-scale open programmable stacks. We use the relay model as our base and capture and interpret packets without prior knowledge of protocols implementation. Radio Resource Control (RRC) is selected proof of concept of the proposed system. Our fuzzing architecture incorporates two abstractions of different dimension, fuzzing-command-level and bit-level, and the proposed LAL fuzzing framework focuses on command-level fuzzing covering potential attacks by autonomously generating a comprehensive fuzzing case set. Our analysis of 39 RRC states successfully illustrates 129 vulnerabilities resulting in RRC connection establishment failure from 205 command-level fuzzing cases and reveals insights into exploitable vulnerabilities in each channel of RRC procedure. Furthermore, to assess risks and prevent potential vulnerability, we use the Long Short-Term Memory (LSTM) based model to perform a deep analysis of transaction states in sequenced commands. With the LSTM based model, we efficiently predict more than 95 percent connection failure at an average duration of 0.059 seconds after the fuzzing attack and provide sufficient time for proactive defense before RRC connection completion or failure, with an average of 3.49 seconds. The rapid vulnerability prediction capability also enables proactive defenses to potential attacks. The proposed fuzzing system offers sufficient automation, scalability, and usability to improve 5G security assurance and could be used for existing and newly released protocols and stacks validation and real-time system vulnerability detection and prediction.

Assessment: Using RRC as a proof of concept, this paper presents a LAL-based fuzzing system that can identify vulnerabilities and undesirable behavior patterns and detect them for 5G systems with 95 percent

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

accuracy. It is a modeling study using an LTSM-based machine learning model. It is not clear what is the operational scenario under which fuzzing data is collected and if it all was a 5G system. If the readers are interested in fuzzing system, it can be a good read.

Formal-Guided Fuzz Testing: Targeting Security Assurance from Specification to Implementation for 5G and Beyond

20 July 2023

https://arxiv.org/abs/2307.11247

Abstract: Softwarization and virtualization in 5G and beyond necessitate thorough testing to ensure the security of critical infrastructure and networks, requiring the identification of vulnerabilities and unintended emergent behaviors from protocol designs to their software stack implementation. To provide an efficient and comprehensive solution, we propose a novel and first-of-its-kind approach that connects the strengths and coverage of formal and fuzzing methods to efficiently detect vulnerabilities across protocol logic and implementation stacks in a hierarchical manner. We design and implement formal verification to detect attack traces in critical protocols, which are used to guide subsequent fuzz testing and incorporate feedback from fuzz testing to broaden the scope of formal verification. This innovative approach significantly improves efficiency and enables the auto-discovery of vulnerabilities and unintended emergent behaviors from the 3GPP protocols to software stacks. Following this approach, we discover one identifier leakage model, one DoS attack model, and two eavesdrop attack models due to the absence of rudimentary MITM protection within the protocol, despite the existence of a Transport Layer Security (TLS) solution to this issue for over a decade. More remarkably, guided by the identified formal analysis and attack models, we exploit 61 vulnerabilities using fuzz testing demonstrated on srsRAN platforms. These identified vulnerabilities contribute to fortifying protocol-level assumptions and refining the search space. Compared to state-of-the-art fuzz testing, our united formal and fuzzing methodology enables auto-assurance by systematically discovering vulnerabilities. It significantly reduces computational complexity, transforming the non-practical exponential growth in computational cost into linear growth.

Assessment: In this paper, authors propose a novel and first-of-its-kind approach that connects the strengths and coverage of formal and fuzzing methods to efficiently detect vulnerabilities across protocol logic and implementation stacks in a hierarchical manner. Authors design and implement formal verification to detect attack traces in critical protocols, which are used to guide subsequent fuzz testing and incorporate feedback from fuzz testing to broaden the scope of formal verification. This innovative approach significantly improves efficiency and enables the auto-discovery of vulnerabilities and unintended emergent behaviors from the 3GPP protocols to software stacks. In the paper, authors demonstrate this approach to the 5G Non-Stand-Alone (NSA) security processes leading to a robust and self-reinforcing solution to the scalability challenges that often arise when detecting vulnerabilities and unintended emergent behaviors in intricate, large-scale 5G systems and their deployments in critical infrastructures and verticals.

[This paper is written by the authors of the previous paper cited in this document and uses identical method/algorithm to 5G-Non-Stand-Alone system, i.e., 5G/LTE system. The earlier paper was focused on 5G only. Because analysis gets a little bit complex due to inter-working modeling of two systems, the paper contains additional results.

The Vulnerability and Enhancement of AKA Protocol for Mobile Authentication in LTE/5G Networks

22 March 2023

https://www.sciencedirect.com/science/article/pii/S1389128623001305

Abstract: The Long-Term Evolution (LTE)/5G network connects much of the world's population to provide subscriber's voice calls and mobile data delivery, with security provided by the Authentication

and Key Agreement (AKA) defined by 3GPP, which makes the LTE/5G network more secure than all its predecessors. Primarily due to the access limitations of LTE systems, the vulnerabilities of AKA protocol and potential attacks have not received much investigation, which is essential to LTE users with a tremendous number of cellular services. In this study, we focus on two questions: (i) what are the vulnerabilities that can be exploited to carry out attacks in practice? and (ii) how to design an enhanced AKA protocol against such attacks? We examine the detailed procedures of Evolved Packet System (EPS)-AKA protocol by 3GPP and have identified three types of attacks with respect to catching, location tracking, and jamming. We have designed and implemented attacks with commercial equipment to evaluate their threats in practice. In addition, we propose an enhanced AKA protocol that essentially relies on asymmetric encryption rather than symmetric in the AKA protocol and additional digital signatures to countermeasure these attacks. Finally, we verified our solution through formal verification to prove that our solution can mitigate the newly found vulnerabilities.

Assessment: Authentication and Key Management are fundamental to the security of Cellular Communication Networks because they provide: (1) Mutual authentication between users and networks; and (2) Ability to derive cryptographic keys as needed for secure control and user plane messages. This paper discusses the vulnerabilities and enhancements of EPS-AKA (Evolved Packet System – And Key Agreement) which is 4G/LTE specific. The 4G EPS-AKA has been shown to have a few well-known vulnerabilities such as: (a) UE Identity is sent over radio networks without encryption; (b) TMSI and GUTI are flawed because they are not refreshed as frequently as needed; (c) GUTI allocation is shown to be predictable being of fixed size; and (d) Authentication Vector (AV) proposed by Home Network is not part of authentication decision.

In response to these well-known vulnerabilities in 4G authentication, 5G has defined three plus authentication methods – (i) 5G - AKA, (ii) EAP – AKA, (iii) EAP – AKA' (Similar to AKA but encryption key changed from 128 bits to 256 bits), and (iv) EAP – TLS [Extensible Authentication Protocol] over TLS). For details about 5G authentication and other security features, please see 3GPP TS 33.501.

It is a 4G security paper but can be included as it will motivate readers to read about 5G authentication, which is one of the most critical security enhancement to 5G.

Modeling 5G Threat Scenarios for Critical Infrastructure Protection

19 July 2023

https://ieeexplore.ieee.org/abstract/document/10182173

Abstract: Fifth-generation cellular networks (5G) are currently being deployed by mobile operators around the globe. 5G is an enabler for many use cases and improves security and privacy over 4G and previous network generations. However, as recent security research has revealed, the 5G standard still has technical security weaknesses for attackers to exploit. In addition, the migration from 4G to 5G systems takes place by first deploying 5G solutions in a non-standalone (NSA) manner, where the first step of the 5G deployment is restricted to the new radio aspects of 5G. At the same time, the control of user equipment is still based on 4G protocols; that is, the core network is still the legacy 4G evolved packet core (EPC) network. As a result, many security vulnerabilities of 4G networks are still present in current 5G deployments. To stimulate the discussion about the security risks in current 5G networks, particularly regarding critical infrastructures, we model possible threats according to the STRIDE threat classification model. We derive a risk matrix based on the likelihood and impact of eleven threat scenarios (TS) that affect the radio access and the network core. We estimate that malware or software vulnerabilities on the 5G base station constitute the most impactful threat scenario, though not the most probable. In contrast, a scenario where compromised cryptographic keys threaten communications between network functions is both highly probable and highly impactful. To improve the 5G security posture, we discuss possible mitigations and security controls. Our analysis is generalizable and does not depend on the specifics of any particular 5G network vendor or operator.

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

Assessment: This paper highlights the security vulnerabilities that have been shown to arise in 5G-NSA (Non-Stand Alone) deployments due to interworking of 4G and 5G protocols and systems. However, most of these vulnerabilities in 5G-SA (Stand Alone) deployments are not visible due to planned implementation of 5G Security Standard (3GPP TS 33.501) in a Service Based Architecture spanning control and data plane communications.

Active Foreign Commercial 5G Standalone Networks

Table 1 lists foreign network operators that claim to have launched 5G Standalone (SA) commercial mobile services as of 31 August 2023[a]. As of this publication, 39 operators in 22 countries, excluding the United States, claim to have launched commercial 5G SA services.

Table 1. Foreign 5G SA Commercial Networks

Country	Operator	5G SA Launch	Remarks
Australia	Telstra[1] Optus[2] TPG Telecom[3]	May 2020 November 2021 November 2021	Telstra claimed to be the first Australian provider to enable 5G SA services to its customers. Telstra's spectrum operates in Low (700-900 MHz), Mid (1800-3600 MHz), and High (26-28 GHz) bands.[4] Optus is providing 5G SA services in the 3500 MHz, 2300 MHz, and 2100 MHz spectrum bands; TPG's standalone core network runs on TPG's 700 MHz spectrum holdings. Note that TPG now incorporates Vodafone Australia.[5]
Austria	Hutchison Drei Austria	September 2022[6]	Drei bought 5G licenses to operate in the 700 MHz and 1.5 GHz bands and employs equipment from Qualcomm and ZTE.[7]
Bahrain	STC Bahrain	May 2022	STC Bahrain launched the country's first 5G SA network using Huawei equipment. The network supports enhanced mobile broadband (eMBB), URLLC, and Massive Machine-Type Communications (mMTC) services.[8]
Brazil	TIM Brasil Claro Brasil Vivo	July 2022 July 2022 July 2022	All three of Brazil's wireless providers activated 5G SA commercial services in July 2022 in the capital of Brasilia in the 3500 MHz band (TIM soft-launched its 5G SA services in April to select users).[9] [10] 5G services in the 26 GHz band, primarily aimed at hotspot coverage for industrial applications or point to point solutions, are also planned.[11]
Bulgaria	A1 Bulgaria	October 2022	A1 Bulgaria completed the rollout of its 5G SA network, which employs Nokia-made RAN and Ericsson dual-mode 5G Core backbone network.[12]
Canada	Rogers Communications[13] Bell Canada	March 2022 July 2022	Rogers' 5G SA network is Canada's first. The company's 5G services operate in the 600, 1700, and 2500 MHz bands.[14] The company expanded its spectrum to the 3500 MHz band in June 2022.[15] Bell Canada launched its 5G SA network in July 2022 in the 3500 MHz band, initially providing services in southern Ontario before expanding to nationwide coverage.[16]
China	China Mobile[17] China Telecom China Unicom CTM	November 2020[18] November 2020[19] November 2020 November 2022	As of early 2021, these three operators had deployed over 700,000 5G SA base stations; China Mobile commissioned 5G SA services in all prefectures and cities across China; and China Telecom and China Unicom jointly built the world's largest shared 5G SA network, covering 300 cities. Companhia de Telecomunicacoes de Macau (CTM) launched 5G SA services in November 2022.[20]

[a] This list does not include commercial 5G SA fixed wireless access (FWA) or private networks, or operators engaged in testing or trials.

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

Country	Operator	5G SA Launch	Remarks
Finland	Telia Company[21]	November 2021	Telia was the first commercially available 5G SA network in the Nordic and Baltic regions. The company offers 5G services in the 700 and 3500 MHz bands and has also acquired spectrum in the 26 GHz band. The company is working on rolling out 5G services to all its markets across the Nordic and Baltic countries.[22]
Germany	Deutsche Telekom[23] Vodafone[24]	April 2022 March 2022	As of early 2022, Deutsche Telekom's network had 5,000 antennas operating in the 3600 MHz spectrum, providing coverage to over 200 urban centers and cities. Vodafone had over 4,000 antennas supporting 5G SA services, operating in the 3600, 1800, and 700 MHz spectra and is projected to reach nationwide coverage by 2025.
India	Reliance Jio	October 2022	Reliance Jio launched 5G SA services in select Indian cities in October 2022, with the goal of achieving national coverage by December 2023.[25, 26] Jio acquired spectrum in the 700 MHz, 800 MHz, 1800 MHz, 3300 MHz, and 26 GHz bands in auctions in mid-2022.[27]
Italy	OpNet (formerly Linkem)[28]	October 2021	Linkem's 5G SA network is Italy's first and operates in the 3500 MHz band. Linkem changed its name to OpNet following the sale of its retail operations to Tiscali in 2022. Note that OpNet/Linkem currently only operates 5G SA Fixed Wireless Access (FWA) in the 3.5 and 26 GHz bands and was inadvertently included in this list of 5G SA commercial operators.[29] However, the company plans to introduce 5G SA wireless services in the future using Ericsson's dual-mode 5G Core technology.[30]
Japan	SoftBank Corp.[31] NTT Docomo[32] au by KDDI	October 2021 August 2022 February 2022	Supporting SoftBank Air Terminals, SoftBank provides coverage in the 3.9-4.0 GHz and 29.1-29.5 GHz ranges.[33] NTT Docomo launched the world's first commercial 5G SA network allowing smartphones to simultaneously utilize both mid-band (sub-6 GHz) and mmWave frequencies, providing 5G NR Dual Connectivity (NR-DC) to users. au by KDDI launched 5G SA services in Kanagawa in February 2022, employing a virtualized RAN (vRAN).[34]
Kuwait	STC Kuwait[35]	May 2021	STC's 5G services were launched in the 3500 Mhz band and the company expanded its services into the 2100 MHz band, as well.[36]
Philippines	Smart Communications[37] Globe Telecom	October 2021 December 2022	Smart launched the first 5G SA network in the Philippines in Makati City. Based on available information, the company's 5G services appear to mainly be in the 700 and 3500 MHz bands, although 5G carrier aggregation tests have also been carried out using the 2600 and 3500 MHz bands.[38] Globe Telecom announced the launch of commercial 5G SA services in December 2022.[39]
Saudi Arabia	Zain KSA[40] STC Saudi Arabia[41, 42]	February 2022 August 2021	At launch, Zain's network comprised 5,000 towers and covered 51 cities. The provider operates 5G in the 2600 and 3500 MHz bands.[43] STC's 5GC supports both 5GNSA and 5G SA services.
Singapore	M1 Limited[44] StarHub Mobile[45] Singtel[46]	July 2021 July 2021 September 2021	M1 and StarHub Mobile engaged in a joint venture to build their 5G SA network; both the M1/StarHub and the Singtel networks were commissioned in the 3500 MHz spectrum.

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

Country	Operator	5G SA Launch	Remarks
South Africa	Rain[47]	July 2020	Rain launched the first 5G SA network in Africa in partnership with Huawei. Rain secured bandwidth in the 700 MHz and 2600 MHz bands,[48] although it applied for spectrum in the 800 and 3500 MHz bands as well.[49]
South Korea	KT[50]	July 2021	KT is the first provider in South Korea to launch 5G SA services. In 2018, KT secured 5G spectrum in the 3500-3600 MHz and 26.5-27.3 GHz bands.[51]
Spain	Vodafone[52] Orange	December 2021 February 2023	Vodafone's initial 5G SA commercial rollout in Spain was for the businesses in the Almeria Science and Technology Park. Orange launched 5G SA commercial services in February 2023 as "5G+" with roughly 90% coverage in Madrid, Barcelona, Valencia, and Seville, with additional locations to be added later in the year.[53]
Taiwan	Taiwan Mobile Co[54].	October 2021	Taiwan Mobile 5G services operate in the 700 MHz and 700 MHz + 3500 MHz/28 GHz (low+high) bands. The company also operates 4G/5G EUTRA-NR EN-DC in the 700 MHz, 1800 MHz, 2100 MHz, 3500 MHz, and 28 GHz bands.[55]
Thailand	AIS[56]	July 2020	AIS launched 5G SA services in July 2020,[57] and by August 5G SA had reportedly been extended to all 77 provinces in the country.[58] AIS 5G operates in the 700 MHz, 2600 MHz, and 26 GHz bands.[59]
United Arab Emirates (UAE)	Etisalat	5 April 2023	Etisalat launched 5G SA commercial services in April 2023.[60]

Literature Review of Other Pertinent 5G-Related Items of Interest

China, 5G, and Alliance Security Beyond the 2021/2022 NATO Summits

22 July 2022

https://www.gmfus.org/news/china-5g-and-alliance-security-beyond-202122-nato-summits

Abstract: This summary presents the key points drawn from a roundtable organized by GMF and held under the Chatham House rule, which brought together experts from Europe and the United States to explore how broad questions around China, 5G, resilience, and critical infrastructure were being addressed in the context of NATO. The roundtable was held in 2021, but the conclusions and analysis were updated following the invasion of Ukraine and NATO's 2022 Madrid summit.

Assessment: These papers are included here for the information of the reader to check out, if the contents interest them. No review is included here because these publications did not undergo any formal technical pre-publication review process.

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

Sources

[1] [Telstra | Nikos Katinakis | "We're the first to enable standalone 5G in Australia" | https://exchange.telstra.com.au/were-the-first-to-enable-standalone-5g-in-australia/ | 1 May 2020 | Accessed on 16 October 2022 | The source is publicly available information and does not contain classification markings]

[2] [Optus | "Optus switches on Standalone 5G network for limited trial" | https://www.optus.com.au/about/media-centre/media-releases/2021/11/optus-switches-on-standalone-5g-network-for-limited-trial | 30 November 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[3] [CRN | Nico Arboleda | "TPG Telecom launches 5G standalone network" | https://www.crn.com.au/news/tpg-telecom-launches-5g-standalone-network-572694 | 16 November 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[4] [Telstra | "5G and EME" | https://telstra.com.au/consumer-advice/eme/5g-and-eme | Accessed on 16 October 2022 | The source is publicly available information and does not contain classification markings]

[5] [Telecoms.com | Jamie Davies | "Vodafone Australia finally completes merger with TPG" | https://telecoms.com/505494/vodafone-australia-finally-completes-merger-with-tpg/ | 13 July 2020 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[6] [Comms Update | "Drei launches 5G SA for homes and businesses" | https://www.commsupdate.com/articles/2022/10/03/drei-launches-5g-sa-for-homes-and-businesses/ | 3 October 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[7] [RCR Wireless News | Juan Pedro Tomás | "Three Austria launches 5G Standalone network" | https://www.rcrwireless.com/20220930/5g/three-austria-launches-5g-standalone-network | 30 September 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[8] [IEEE Communications Society | Alan Weissberger | "STC launches first 5G standalone (SA) core network in Bahrain via Huawei" | https://techblog.comsoc.org/2022/05/23/stc-launches-first-5g-standalone-sa-core-network-in-bahrain/ | Accessed on 8 June 2022 | The source is publicly available information and does not contain classification markings]

[9] [TeleSemana.com | Andrea Catalano | "TIM Brasil implementó su red core 5G SA mientras la casa matriz está en zozobra" | https://www.telesemana.com/blog/2022/04/07/tim-brasil-implemento-su-red-core-5g-sa-mientras-la-casa-matriz-esta-en-zozobra/ | 7 April 2022 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[10] [COMMS Update | "Vivo, TIM, Claro all switch on 5G in Brasilia" | https://www.commsupdate.com/articles/2022/07/07/vivo-tim-claro-all-switch-on-5g-in-brasilia/ | 7 July 2022 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[11] [TeleSemana.com | Andrea Catalano | "TIM Brasil define cómo desplegará sus redes a partir del espectro adquirido de 5G y anticipa parte de su estrategia commercial" | https://www.telesemana.com/blog/2021/12/09/tim-brasil-define-como-desplegara-sus-redes-a-partir-del-espectro-adquirido-de-5g-y-anticipa-parte-de-su-estrategia-comercial/ | 9 December 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[12] [Comms Update | A1 Bulgaria completes integration of SA 5G network | https://www.commsupdate.com/articles/2022/10/17/a1-bulgaria-completes-integration-of-sa-5g-network/ | 17 October 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[13] [Ericsson | "Ericsson, Rogers launch Canada's first commercial 5G standalone network" | https://

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

www.ericsson.com/en/press-releases/6/2022/3/ericsson-rogers-launch-canadas-first-commercial-5g-standalone-network | 28 March 2022 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[14] [Comms Update | "Rogers doubles 5G cities/towns to 130; launches Dynamic Spectrum Sharing" | https://www.commsupdate.com/articles/2020/10/14/rogers-doubles-5g-citiestowns-to-130-launches-dynamic-spectrum-sharing/ | 14 October 2020 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[15] [T-Net | "Rogers to Launch Premium 3500 MHz 5G Spectrum in Nanaimo, a First in Canada" | https://www.bctechnology.com/news/2022/6/17/Rogers-to-Launch-Premium-3500-MHz-5G-Spectrum-in-Nanaimo-a-First-in-Canada.cfm | 17 June 2022 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[16] [Comms Update | "Bell launches '5G+' 3500MHz service in Ontario; prepares to deploy 5G SA core network" | https://www.commsupdate.com/articles/2022/07/29/bell-launches-5g-3500mhz-service-in-ontario-prepares-to-deploy-5g-sa-core-network/ | 29 July 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[17] [RCR Wireless News | Juan Pedro Tomás | "Chinese telcos expected to deploy 1 million 5G SA stations in 2021" | https://www.rcrwireless.com/20210205/business/chinese-telcos-expected-deploy-1-million-5g-sa-base-stations-this-year | 5 February 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[18] [China Mobile | "China Mobile Hong Kong Launches Hong Kong's First 5G Standalone Network" https://eshop.hk.chinamobile.com/en/about_us/media_centre/NewsPDF/20201126pr.html | 30 November 2020 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[19] [IEEE ComSoc Blog | Alan Weissberger | "China Telecom launches 5G standalone cloud native network with Tianyi Cloud" | https://techblog.comsoc.org/2020/11/16/china-telecom-progressing-5g-standalone-network/ | 16 November 2020 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[20] [Comms Update | "5G to launch in Macau next week" | https://www.commsupdate.com/articles/2022/11/08/5g-to-launch-in-macau-next-week/ | 8 November 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[21] [Telia Company | "Telia Company launches 5G SA core network in Finland – the first commercially available 5G SA network in the Nordic and Baltic region" | https://www.teliacompany.com/en/news/press-releases/2021/11/telia-company-launches-5g-sa-core-network-in-finland--the-first-commercially-available-5g-sa-network-in-the-nordic-and-baltic-region/ | 10 November 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[22] [Telia Company | "Telia's 5G network measures data speeds of 4 gigabit per second – almost a world record" | https://www.teliacompany.com/en/news/news-articles/2021/telias-5g-network-measures-data-speeds-of-4-gigabit-per-second--almost-a-world-record/ | 26 April 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[23] [Fierce Wireless | Monica Alleven | "Deutsche Telekom touts 5G SA rollout in Germany"| https://www.fiercewireless.com/5g/deutsche-telekom-touts-5g-sa-rollout-germany | 5 April 2022 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[24] [RCR Wireless News | Juan Pedro Tomás | "Vodafone's 5G SA network already reaches 10 million people in Germany" | https://www.rcrwireless.com/20220315/carriers/vodafone-5g-sa-network-already-reaches-10-million-people-germany | 15 March 2022 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

[25] [IndiaTV | Poorva Joshi | "Jio 5G rollout in metro cities by Diwali, to cover entire country by December 2023: Mukesh Ambani" | https://www.indiatvnews.com/business/news/jio-5g-rollout-reliance-metro-cities-delhi-mumbai-kolkata-chennai-diwali-to-cover-entire-country-by-december-2023-mukesh-ambani-akash-latest-updates-2022-08-29-803748 | 29 August 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[26] [Reliance Jio | "Experience life like never before" | https://www.jio.com/5g | 2022 | Accessed on 4 January 2023 | source is publicly available information and does not contain classification markings]

[27] [Times of India | "Reliance Jio's 5G footprint after spectrum auction: Here are the details" | 2 August 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[28] [Comms Update | "FWA operator Linkem launches Italy's first 5G SA network" | https://www.commsupdate.com/articles/2021/10/01/fwa-operator-linkem-launches-italys-first-5g-sa-network/ | 1 October 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[29] [Comms Update | "Linkem Group becomes OpNet" | https://www.commsupdate.com/articles/2022/10/04/linkem-group-becomes-opnet/ | 4 October 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[30] [Comms Update | "OpNet opens Italian 5G SA core network with Ericsson" | https://www.commsupdate.com/articles/2022/11/25/opnet-opens-italian-5g-sa-core-network-with-ericsson/ | 25 November 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[31] [SoftBank | "SoftBank Corp. First Carrier in Japan to Provide 5G Standalone Commercial Services" | https://www.softbank.jp/en/corp/news/press/sbkk/2021/20211019_01/ | 19 October 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[32] [Qualcomm | "Qualcomm and NTT DOCOMO Unleash Next Generation 5G Speeds and Coverage Through World's First High-Speed 5G Standalone Service" | https://www.qualcomm.com/news/releases/2022/09/qualcomm-and-ntt-docomo-unleash-next-generation-5g-speeds-and-co | 7 September 2022 | Accessed on 16 October 2022 | The source is publicly available information and does not contain classification markings]

[33] [Comms Update | "SoftBank adds mmWave to 5G services" | https://www.commsupdate.com/articles/2021/03/22/softbank-adds-mmwave-to-5g-services/ | 22 March 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[34] [RCR Wireless News | Catherine Sbeglia Nin | "KDDI worked with partners Samsung and Fujitsu to turn on the Open RAN site in Japan" | https://www.rcrwireless.com/20220218/open_ran/kddi-claims-worlds-first-5g-standalone-open-ran-site-supported-by-vran | 18 February 2022 | Accessed on 4 January 2023 | The source is publicly available information and does not contain classification markings]

[35] [Developing Telecoms | Shailaja Pai | "STC Kuwait rolls out commercial 5G standalone infrastructure" | https://developingtelecoms.com/telecom-technology/wireless-networks/11104-stc-kuwait-rolls-out-commercial-5g-standalone-infrastructure.html | 10 May 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[36] [Comms Update | "STC Kuwait launches commercial 5G standalone infrastructure; boosts 2100MHz 5G coverage" | https://www.commsupdate.com/articles/2021/05/07/stc-kuwait-launches-commercial-5g-standalone-infrastructure-boosts-2100mhz-5g-coverage/ | 7 May 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[37] [Developing Telecoms | Shailaja Pai | "Smart fires up first 5G SA network in Makati, Philippines" | https://

developingtelecoms.com/telecom-business/operator-news/12024-smart-fires-up-first-5g-sa-network-in-makati-philippines.html | 5 October 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[38] [Smart | "Smart gears up for leading high performance 5G Capacity and Coverage Features" | https://smart.com.ph/About/newsroom/press-releases/2020/12/23/smart-gears-up-for-leading-high-performance-5g-capacity-and-coverage-features | 23 December 2020 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[39] [Comms Update | "Globe completes PHP9.5bn sale of towers to Frontier; announces 5G SA launch" | https://www.commsupdate.com/articles/2022/12/12/globe-completes-php9-5bn-sale-of-towers-to-frontier-announces-5g-sa-launch/ | 12 December 2022 | Accessed on 24 April 2023 | The source is publicly available information and does not contain classification markings]

[40] [Developing Telecoms | Shailaja Pai | "Zain launches Saudi Arabia's first 5G standalone network" | https://developingtelecoms.com/telecom-business/operator-news/12805-zain-launches-saudi-arabia-s-first-5g-standalone-network.html | 3 February 2022 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[41] [IEEE Communications Society | Alan Weissberger | "STC launches first 5G standalone (SA) core network in Bahrain via Huawei" | https://techblog.comsoc.org/2022/05/23/stc-launches-first-5g-standalone-sa-core-network-in-bahrain/ | Accessed on 8 June 2022 | The source is publicly available information and does not contain classification markings]

[42] [Developing Telecoms | STC and Ericsson Expand 5G Standalone in Saudi Arabia | https://developingtelecoms.com/telecom-technology/wireless-networks/11681-stc-and-ericsson-expand-5g-standalone-in-saudi-arabia.html | 11 August 2021 | Accessed on 8 June 2022 | The source is publicly available information and does not contain classification markings]

[43] [Comms Update | "Zain KSA rolls out 5G services" | https://www.commsupdate.com/articles/2019/06/27/zain-ksa-rolls-out-5g-services/ | 27 June 2019 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

[44] [RCR Wireless News | Juan Pedro Tomás | "M1 launches 5G Standalone network in Singapore" | https://www.rcrwireless.com/20210728/business/m1-launches-5g-standalone-network-singapore | 28 July 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[45] [RCR Wireless News | Juan Pedro Tomás | "M1 launches 5G Standalone network in Singapore" | https://www.rcrwireless.com/20210728/business/m1-launches-5g-standalone-network-singapore | 28 July 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[46] [Ericsson | "Singtel enters 5G standalone era powered by Ericsson" | https://www.ericsson.com/en/press-releases/2/2021/9/singtel-enters-5g-standalone-era-powered-by-ericsson | 22 September 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[47] [RCR Wireless News | Juan Pedro Tomás | "Rain launches standalone 5G network in South Africa" | https://www.rcrwireless.com/20200720/business/rain-launches-standalone-5g-network-south-africa | 20 July 2020 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[48] [Mobile World Live | Anne Morris | "South Africa completes first phase of delayed auction" | https://www.mobileworldlive.com/featured-content/top-three/south-africa-completes-first-phase-of-delayed-auction | 9 March 2022 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

This newsletter is a product of the DoD OUSD FutureG & 5G Office in partnership with Idaho National Laboratory

49 [Rain | "Application Form for 700MHz, 800MHz, 2.6GHz and 3.5GHz Spectrum Award Process" | https://www.icasa.org.za/uploads/files/IMT-ITA-Application-15-01-2021-Final-Draft-Part-1.pdf | 28 December 2020 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

50 [ZDNet | Cho Mu-Hyun | "KT becomes first South Korean telco to launch 5G standalone service" | https://www.zdnet.com/article/kt-becomes-first-south-korean-telco-to-launch-5g-standalone-service/ | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

51 [Everything RF | "5G Frequency Spectrum in South Korea" | https://www.everythingrf.com/community/5g-frequency-spectrum-in-south-korea | 22 July 2020 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

52 [5GWorldPro.com | "Vodafone Spain deploys 5G Standalone in Almeria" | https://www.5gworldpro.com/blog/2021/12/10/vodafone-spain-deploys-5g-standalone-in-almeria/ | 10 December 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

53 [Total Telecom | Harry Baldock | "5G+: Orange launches 5G standalone in Spain" | https://totaltele.com/5g-orange-launches-5g-standalone-in-spain/ | 13 February 2023 | Accessed on 19 February 2023 | The source is publicly available information and does not contain classification markings]

54 [Nokia | "Nokia deploys 5G standalone core network for Taiwan Mobile" | https://www.nokia.com/about-us/news/releases/2021/10/22/nokia-deploys-5g-standalone-core-network-for-taiwan-mobile/ | 22 October 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

55 [Taiwan Mobile | "Taiwan Mobile's 5G Advantage" | https://english.taiwanmobile.com/product/5G_advantage.html | 2022 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

56 [The Fast Mode | Ray Sharma | "Thai Operator AIS, Samsung Launch 5G VoNR over 5G SA network" | https://www.thefastmode.com/services-and-innovations/21155-thai-operator-ais-samsung-launch-5g-vonr-over-5g-sa-network | December 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

57 [AIS | "AIS 5G underlines leadership as first in the world to launch SA Teams up with Samsung to showcase Samsung Galaxy S21 Series 5G AIS 5G SA: most bandwidth for best speeds and lowest latency in Thailand" | https://investor.ais.co.th/news.html/id/2339032/group/newsroom_press | 11 June 2021 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

58 [Bangkok Post | "AIS 5G service reaches every province" | https://www.bangkokpost.com/business/1972579/ais-5g-service-reaches-every-province | 22 August 2020 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

59 [RCR Wireless News | Catherine Sbeglia Nin | "AIS launched 5G standalone services in July 2020" | https://www.rcrwireless.com/20210723/5g/ais-and-vivo-conduct-5g-standalone-network-tests-in-thailand | 23 July 2021 | Accessed on 28 April 2022 | The source is publicly available information and does not contain classification markings]

60 [5G European Observatory | "Etisalat launches MENA region's first standalone 5G network" | https://5gobservatory.eu/etisalat-launches-mena-regions-first-standalone-5g-network/ | 5 April 2023 | Accessed on 24 April 2023 | The source is publicly available information and does not contain classification markings]