5G Network Vulnerabilities for Untrusted Networks (December to May 2024)

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) FutureG Advanced Component Development and Prototypes Program. The information in this report is based on open-source material published or made available between 1 December and 31 May 2024.

5G Network Vulnerabilities for Untrusted Networks

Vulnerabilities Listed in NIST NVD

NIST CVE-2023-32846/32845/32844/32843/32842/32841: 5G Modem possible system crash due to malformed RRC messages

CVSS Severity V4.x: N/A; CVSS Severity V3.x: High 7.5; V2.0: N/A

https://nvd.nist.gov/vuln/detail/CVE-2023-32846

In the 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service (DoS) when receiving malformed radio resource control (RRC) messages, with no additional execution privileges needed. User interaction is not needed for exploitation.

Assessment: This vulnerability is specific to MediaTek devices. It affects MediaTek Smartphone, Tablet, AIoT, Smart display, Smart platform, OTT, Wi-Fi, TV, Computer Vision, and Audio chipsets.

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 Untrusted Networks or are of potential general interest.

RAFT: A Real-Time Framework for Root Cause Analysis in 5G and Beyond Vulnerability Detection

6 January 2024

https://ieeexplore.ieee.org/abstract/document/10454824

Abstract: The reliability of 5G systems and their applications in a complex, dynamic, and heterogeneous environment requires rigorous testing and real-time detection for system vulnerabilities and unintended emergent behaviors. In this paper, fuzz testing is performed on 5G systems by randomly injecting and permuting control commands into the system under test (SUT) of the 5G RRC authentication and authorization

Contents:

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

process, emulating Man-In-The-Middle (MITM) attacks to trigger potential vulnerabilities and unintended behaviors. The fuzzed system behaviors contain information that could indicate the system's health status, potential vulnerabilities, and, more importantly, it enables the causation analysis in the SUT to detect the location and type of attacks or abnormal inputs from the profiling of the impacted behaviors. We then propose a Real-time Framework for Root Cause Analyses (RAFT) in NextG Vulnerability Detection based on analyzing the random fragments of the log file generated during the communication process. By processing the random fragments of the logging profiles captured during fuzz testing with the continuous bag-of-words (CBOW) Model, we extract the information of states and states transitions and perform causal analysis to identify the root cause for vulnerability detection in the 5G system. The novelty of our framework lies in the creation and analysis of the information extraction that does not require capturing the entire log file, instead only it only requires the log file fragments to achieve high accuracy. This approach enables real-time detection and deployment to real-life scenarios where access to the entire logging profile is difficult to obtain or unavailable. The presented framework RAFT directly adapts to various machine learning (ML) models that allow the adaptation to hardware with various computation complexity from internet-of-things (IoT) to RAN servers. The experimental results show a significant performance gain and are thoroughly evaluated by the accuracy and area under the curve (AUC) results. In particular, we show the proposed framework can attain a high AUC value ($0.92\leq\text{AUC} < 0.96$) by accessing only a 70% fragment of the original log file while maintaining a higher accuracy. In addition, we find RAFT reduces the time complexity by more than 5% as the fragment size reduces to 70% of the original log file. The causation analysis nature of RAFT summarizes vulnerability information into essential root causes that can be easily transmitted within the network in real-time and turned into guidance for back-end engineers. The unique advantages of RAFT, including accurate causation with information fragments, reliable performance without large training datasets, and less computation complexity guarantee a wide range of use cases and deployment environments of RAFT.

Assessment: In this paper authors have proposed a RAFT in 5G and Beyond vulnerability detection. The proposed framework is based on fuzz testing generated experimental results that provide ground truth to examine and analyze the characteristics of the vulnerabilities and unintended emergent behaviors of the 5G authentication and authorization process. The RAFT algorithm creates and analyzes extracted information that utilizes log files fragments instead of requiring entire log files as compared to existing algorithms cited in the paper which are accurate. Another advantage of RAFT is it can be integrated with pre-existing ML models. Authors claim RAFT detects the root cause of the SUT behaviors in real-time and provides insight into system behaviors under various MITM attacks. However, the MITM attack is emulated, but emulation details are not fully shared. Additionally, there is no experimental verification of the attack included in the paper to provide validation, that would have established the utility of Fuzzing model approach for 5G testing much stronger.

This paper presents a promising approach for 5G security testing and is of general interest

A Formal Security Analysis of the Fast Authentication Procedure based on the Security Context in 5G Networks

10 January 2024

https://link.springer.com/article/10.1007/s00500-023-09486-x

Abstract: The security context, generally stored in the universal subscriber identity module card or the baseband chip, is the critical information applied by the subscriber to access the 5G network during the fast authentication procedure. Once exposed or illegally used, the security context can be exploited to derive various keys for authentication and encryption. Despite its importance, challenges and questions still remain in the previous relevant research. To fill this gap, by adopting the security protocol verification tool ProVerif, we provide a comprehensive formal model of the fast authentication procedure based on the security context to analyze whether security goals can be met. Unfortunately, we uncover two vulnerabilities, including one never reported before. Our analysis shows these vulnerabilities stem from fundamental design flaws in the cellular network protocol and thus apply to the 4G network. These vulnerabilities could be exploited to launch several attacks, including impersonation and eavesdropping. We have validated these attacks using five mobile phones from five different baseband manufacturers through experimentation

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

in three mobile carriers. We found an insecure implementation of one of these phones that exposed it to replay attacks. We further discuss the security threats posed by the impersonation attack, such as location spoofing and one-tap authentication bypass, which is verified on 10 popular apps. We finally propose several countermeasures to eliminate these security issues. Actually, we have reported the novel vulnerability to the GSM Association and received a confirmation in the form of a coordinated vulnerability disclosure (CVD) number CVD-2022-0057.

Assessment: In 5G, subscribers are protected by many security mechanisms, one of the most important is the AKA protocol/procedure that has been made cryptographically stronger than what was in 4G. The AKA procedure utilizes the pre-key shared by the USIM (Universal Subscriber Identity Module) card and the network to enable them to mutually authenticate each other and establish the session keys for secure communications. However, the authors of this paper discovered two major security vulnerabilities – "Impersonation" and "Eavesdropping" by using the security protocol verification tool ProVerif in the "security context" parameter that is generally stored in the USIM or baseband chip, used by the subscriber to access the 5G Network during the fast authentication procedure.

This paper includes a comprehensive formal model for the fast authentication procedure using the security context in 5G Networks and identifies two vulnerabilities as stated earlier, one of which is new. It resents two attack models to show how these vulnerabilities are exploited by impersonation attack by verifying them in mobile phones belonging to three different 5G carriers. In addition, the paper includes two attacks that exploit the identified vulnerabilities and verify them in three carriers. Authors analyze root causes and propose several effective counter measures to prevent these attacks.

This paper is of general interest for security analysis regarding authentication.

An Efficient Vulnerability Detection Method for 5G NAS Protocol Based on Combinatorial Testing

14 February 2024

https://link.springer.com/chapter/10.1007/978-3-031-53555-0_7

Abstract: With the rapid development and wide application of 5G networks, the security of 5G networks has become a widely concerned issue. Protocol security is the foundation of 5G network security. To protect 5G protocol security, we propose an efficient vulnerability detection method for 5G Non-Access Stratum (NAS) protocol. In this work, we use a combinatorial testing algorithm to generate testing cases that can detect the vulnerability caused by multi-parameter interaction. Furthermore, we define compliance and semantic constraints to restrict the scale of input space and maximize the effectiveness of the testing cases. Finally, we implement a prototype system based on this method and then conduct practical vulnerability detection on 5G UE simulation environments UERANSIM and srsUE. Through experiments, we find five security vulnerabilities having both security and privacy implications and prove our method has better performance in terms of protocol state coverage and the scale of testing cases.

Assessment: This paper proposes an efficient vulnerability detection method for NAS protocol, which is a control plane protocol (i.e., carries signaling messages between UE, RAN, and Network Functions in Mobile Core based on combinatorial testing). Combinatorial testing requires compliance and semantic constraints that are related to field values and lead to defining a vulnerability detection method for NAS protocol.

This paper is of general interest.

A Formal Analysis of 5G EAP-TLS 1.3

14 February 2024

https://link.springer.com/chapter/10.1007/978-3-031-53555-0_14

Abstract: As the fifth-generation mobile network communication technology, 5G supports a wider range of application scenarios with faster speed and lower latency, so the importance of its security cannot be underestimated. Authentication protocols play a crucial role in security as the first safeguard of 5G networks. We provide a formal model of the 5G EAP-TLS 1.3 authentication protocol and perform an automated security

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

analysis using ProVerif, a symbol-based formal verification tool, and our results show that there are some potential flaws in the current protocol design that will cause the protocol to violate the security goals that need to be guaranteed in the standard. To the best of our knowledge, this is the first formal verification study on the 5G EAP-TLS 1.3 protocol.

Assessment: In mobile communication networks, the security of users' data depends on the guarantees provided by the authentication protocols. For 5G networks, the 5G-EAP-TLS protocol has been proposed for this objective. While it has been updated a few times for protocol related vulnerabilities, new vulnerabilities are still being discovered. This paper provides a formal model of 5G-EAP-TLS protocol and conducts a thorough analysis using ProVerif model checker. ProVerif is a symbol-based formal verification tool, and it discovered a few design flaws in the protocol that may jeopardize the security goals that result in severe security vulnerabilities when implemented in real systems. To our knowledge, this is the first study on the formal verification of 5G-EAP-TLS protocol.

This paper is of general interest in the area of formal analysis of the TLS protocol.

Security in 5G Network Slices: Concerns and Opportunities

1 March 2024

https://ieeexplore.ieee.org/abstract/document/10494839

Abstract: Network slicing has emerged as a cornerstone technology within the 5G ecosystem, enabling efficient resource allocation, service customization, and support for various applications. Its ability to deliver Network-as-a-Service (NaaS) brings a new paradigm of adaptable and efficient network provisioning. However, with the diversification of services and the increasing complexity of network infrastructures, a simultaneous rise in security vulnerabilities becomes evident. These flaws go beyond the limitations of conventional network security and affect various aspects of network slice (NS) implementation and management. The limitations of traditional security, such as static policies, single point of failure, and challenges in effectively securing network-slicing deployments, underscore the need to explore security measures tailored to the dynamic nature of 5G networks. To ensure the robust security of 5G networks, it is essential to consider various security concerns such as isolation, authentication, and authorization. Furthermore, dynamic orchestration and inter-slice communication security challenges must be proactively tackled. The security concerns related to 5G networks must be addressed comprehensively to ensure the safe and secure operation of the network. Our survey paper goes into these complex security issues, providing an in-depth and systematic review of the various contexts in which they emerge. We have identified the five most vulnerable areas in Network Slicing: Slice-Lifecycle, Communication type slice uses, Technologies used to provide service, Management threats, and End Devices utilized in service. Apart from threats in these vulnerable areas, we also discussed a few generous attacks that can be launched to disrupt network-slicing services. Furthermore, this study is a valuable resource for evaluating the current state of research efforts in this domain, contributing to the ongoing enhancement of security measures and the overall robustness of network-slicing technology. In doing so, we aim to ensure the secure and sustainable evolution of 5G networks as they become increasingly integral to our digital infrastructure.

Assessment: Security of 5G Network Slicing has been studied extensively in the literature because of inherent complexity of the architecture and diversity of applications supported with their stringent performance requirements. This paper is a survey paper and appeared in April 2024 issue of IEEE Access journal, so it is most recent and includes several new vulnerabilities that have been reported in IEEE/ACM and other conferences and journals publications recently.

This paper is of general interest in the area 5G Network Slicing security.

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

5G-SPECTOR: An O-RAN Compliant Layer-3 Cellular Attack Detection Service

1 March 2024

https://www.ndss-symposium.org/wp-content/uploads/2024-527-paper.pdf

Abstract: Over the past several years, the mobile security community has discovered a wide variety of exploits against link and session-establishment protocols. These exploits can be implemented on software-defined radios (SDRs) that disrupt, spoof, or flood layer-3 (L3) messages to compromise security and privacy that still apply to the latest 5G mobile network standard. Interestingly, unlike the prior generations of closed (proprietary) mobile network infrastructures, 5G networks are migrating toward a more intelligent and open-standards-based fully interoperable mobile architecture, called Open RAN or O-RAN. The implications of transitioning mobile infrastructures to a software-defined architectural abstraction are quite significant to the INFOSEC community, as it allows us to extend the mobile data plane and control plane with security-focused protocol auditing services and exploit detection. Based on this design, we present 5G-SPECTOR, the first comprehensive framework for detecting the wide spectrum of L3 protocol exploits on O-RAN. It features a novel security audit stream called MOBIFLOW that transfers fine-grained cellular network telemetry, and a pro- grammable control-plane xApp called MOBIEXPERT. We present an extensible prototype of 5G-SPECTOR that can detect seven types of cellular attacks in real-time. We also demonstrate its scalability to 11 unknown attacks as well as 31 real-world cellular traces, with effective performance (high accuracy, no false alarms) and low (<2% CPU, <100 MB memory) overhead.

Assessment: To detect cellular network threats in real-time, which is a necessity to control and prevent the harm from reaching to the 5G infrastructure, runtime monitors have been developed and deployed. These UE-based monitors rely on reading low level cellular information using baseband APIs provided by the vendors that have been further extended and deployed in the RANs such as heuristic based fake base station detectors and anomalous traffic classifiers. One of the features of the SPECTOR is a runtime monitor that acts as a first defense at the 5G O-RAN control plane that offers programmability and extensibility.

O-RAN security is an active area of research at the present time pursuing analysis of attack surfaces, potential threats, and mitigation of control-plane threats caused by malicious xApps, rApps, and ML models. In this context SPECTOR is focused on securing O-RAN from external cellular threats using MOBIEXPERT xApp on the control plane to enable cellular network operators to program Intrusion Detection System (IDS) signatures for a wide range of external cellular exploits. SPECTOR has been prototyped and tested with seven different L3 attacks and 31 cellular network traces in practice.

This paper describes an intrusion detection tool for attacks on O-RAN based 5G networks and is of general interest.

Penetration Testing of 5G Core Network Web Technologies

4 March 2024

https://arxiv.org/abs/2403.01871

Abstract: Thanks to technologies such as virtual network function the Fifth Generation (5G) of mobile networks dynamically allocate resources to different types of users in an on-demand fashion. Virtualization extends up to the 5G core, where software-defined networks and network slicing implement a customizable environment. These technologies can be controlled via application programming interfaces and web technologies, inheriting their security risks and settings. An attacker exploiting vulnerable implementations of the 5G core may gain privileged control of the network assets and disrupt its availability. However, there is currently no security assessment of the web security of the 5G core network. In this paper, we present the first security assessment of the 5G core from a web security perspective. We use the STRIDE threat modeling approach to define a complete list of possible threat vectors and associated attacks. Thanks to a suite of security testing tools, we cover all of these threats and test the security of the 5G core. In particular, we test the three most relevant open-source 5G core implementations (i.e., Open5GS, Free5Gc, and OpenAirInterface). Our analysis shows all these cores are vulnerable to at least two of our identified attack vectors, demanding increased security measures in the development of future 5G core networks.

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

Assessment: In this paper authors present for the first time a web-based threat model for web security of the 5G core networks. To study 5G core web security, the STRIDE tool is leveraged for threat modeling. STRIDE allows deriving all the threat vectors systematically that affect the 5G code. Additionally, STRIDE is capable of creating threats related to spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. All these threats have been studied using three well-known 5G core implementations such as Open5GS, Free5gc, and OpenAirInterface using well known and established security tools such as Nmap, WhatWeb, Niko, and others. This paper includes security results for well-known attacks such as: (i) Database permission leakage, (ii) SQL injection, (iii) NoSQL injection, (iv) Dictionary attack, and (v) DoS and DDoS, (vi) Clickjacking and several others for all three cores.

This paper describes an intrusion detection tool for attacks on O-RAN based 5G networks and is of general interest.

Det-RAN: Data Driven Cross-Layer Real-Time Attack Detection in 5G Open RANs

19 May 2024

https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/1792/Det_RAN_Pre_print.pdf?sequence=1&isAllowed=y

Abstract: Fifth generation (5G) and beyond cellular networks are vulnerable to security threats, primarily due to the lack of integrity protection in the RRC layer. In order to address this problem, we propose a real- time anomaly detection framework that leverages the concept of distributed applications in 5G O-RAN networks. Specifically, we identify Physical Layer (PHY) features that can generate a reliable fingerprint, infer in a novel way the time of arrival of uplink packets lacking integrity protection, and handle cross-layer features. By identifying legitimate message sources and detecting suspicious activities through an Artificial Intelligence (AI) design, we demonstrate O-RAN-based applications that run at the edge can be designed to provide additional security to the network. Our solution is first validated in extensive emulation environments achieving over 85% accuracy in predicting potential attacks on unseen test scenarios. We then integrate our approach into a real-world prototype with a large channel emulator to assess its real-time performance and costs. Our solution meets the low-latency, real-time constraints of 2 ms, making it well-suited for real-world deployments.

Assessment: In this work authors show O-RAN can be leveraged for designing novel AI solutions at the edge of the network that can swiftly detect the presence of attackers, significantly contributing to enhancing the security of 5G networks. The proposed Det-RAN framework in the paper is designed to process cross-layer features and proactively detect the attacks generated with RRC messages, while achieving strict real-time constraints in 5G networks.

It is well known in the 5G security community that despite 3GPP 5G standards having significantly enhanced the protection of subscribers, vulnerabilities in the procedures still exist. It has been repeatedly shown an attacker can map the 5G -TMSI (Temporary Mobile Subscriber Identity) with RNTI (Radio Network Temporary Identifier) and impersonate the victim, triggering various attacks (e.g., DoS, MitM due to the absence of message integrity protection at the lower layers of the network protocol). It has been shown the potential for UE identity spoofing is a major concern as the RNTI and 5G-TMSI can be matched during the connection establishment process and could be exploited to identify the victim.

This paper describes AI based attack detection methods for O-RAN networks that is of general interest.

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

Active Foreign Commercial 5G Standalone Networks

Table 1 lists foreign network operators that claim to have launched 5G SA commercial mobile services as of 31 May 2024[a]. As of this publication, 39 operators in 22 countries, excluding the United States, claim to have launched commercial 5G SA services.

Table 2. 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 SA core network runs on TPG's 700 MHz spectrum holdings. Note 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 that 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]
Finland	Telia Company[21] Elissa	November 2021 June 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] Elisa launched Finland's first 5G SA network in summer 2021, with an expansion to 5G SA phone subscriptions in February of 2024.[23]
Germany	Deutsche Telekom[24] Vodafone [25]	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.

[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 Programs Office in partnership with Idaho National Laboratory

Country	Operator	5G SA Launch	Remarks
Hungary	Yettel	21 November 2023	Yettel Launched 5G SA services, with 700 base stations nationwide.[26]
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.[27, 28] Jio acquired spectrum in the 700 MHz, 800 MHz, 1800 MHz, 3300 MHz, and 26 GHz bands in auctions in mid-2022.[29]
Ireland	Three	21 December 2023	Three will begin implementing 5G SA services on an initial trial basis.[30]
Italy	OpNet (formerly Linkem)[31]	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.[32] However, the company plans to introduce 5G SA wireless services in the future using Ericsson's dual-mode 5G Core technology.[33]
Japan	SoftBank Corp.[34] NTT Docomo[35] 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.[36] 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).[37]
Kuwait	STC Kuwait[38]	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.[39]
Philippines	Smart Communications[40] 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.[41] Globe Telecom announced the launch of commercial 5G SA services in December 2022.[42]
Portugal	NOS	30 November 2023	NOS now operates Portugal's first 5G SA network with 4200 base stations.[43]
Saudi Arabia	Zain KSA[44] STC Saudi Arabia [45,46]	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.[47] STC's 5GC supports both 5GNSA and 5G SA services.
Singapore	M1 Limited[48] StarHub Mobile[49] Singtel[50]	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.
South Africa	Rain[51]	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[52], although it applied for spectrum in the 800 and 3500 MHz bands as well.
South Korea	KT[53]	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.[54]
Spain	Vodafone[55] Orange Movistar/Telefonica	December 2021 February 2023 5 July 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.[56] Movistar as a part of Telefonica now offers 5G SA services in 11 cities with speeds up to 1600Mbps in the 700MHz band.[57]

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

Country	Operator	5G SA Launch	Remarks
Taiwan	Taiwan Mobile Co.[58]	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.[59]
Thailand	AIS[60]	July 2020	AIS launched 5G SA services in July 2020,[61] and by August 5G SA had reportedly been extended to all 77 provinces in the country.[62] AIS 5G operates in the 700 MHz, 2600 MHz, and 26 GHz bands. [63]
United Arab Emirates (UAE)	Etisalat	5 April 2023	Etisalat launched 5G SA commercial services in April 2023.[64]
United Kingdom	Virgin Media O2	22 February 2024	Virgin Media O2 now offers 5G services in 14 cities including Manchester, Liverpool, London, Lincoln, Birmingham, Sheffield, Glasgow, Newcastle, Leeds, York, Belfast, Cardiff, Nottingham, and Slough.[65]

5G Acronyms

Table 3. 5G SA 2024 Acronyms

Acronym	Definition	Acronym	Definition
(U)SIM	(Universal) Subscriber Identity Module	MME	Mobility Management Entity
5G	5th Generation	NAS	Non-Access Stratum
AGPLv3	Affero General Public License	NIDD	Network Intrusion Detection Dataset
AKA	Authentication and Key Agreement	NR	New Radio
AMF	Access and Mobility Management Function	O-RAN	Open Radio Area Network
API	Application Programming Interface	RIC	RAN Intelligent Controller
CVE	Common Vulnerabilities and Exposures	RMR	RIC Message Router
EAP	Extensible Authentication Protocol	RRC	Radio Resource Control
GHz	GigaHertz	SA	StandAlone
GSM	Global System for Mobiles	SCEF	Service Capability Exposure Function
HSS	Home Subscriber Server	SCS/AS	Sub Carrier Spacing
IEEE	Institute of Electrical and Electronics Engineers	SEPP	Security Edge Protection Proxy
IoT	Internet of Things	SIGPIPE	Signal Pipe
IP	Internet Protocol	TLS	Transport Layer Security
LTE	Long Term Evolution	UDR	User Data Repository
MHz	Megahertz	UE	User Equipment
MITM	Man in the Middle	Wi-Fi	Wireless Fidelity

This newsletter is a product of the DoD OUSD FutureG Programs 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.thefastmode.com/technology-solutions/35000-elisa-launches-finlands-first-5g-sa-phone-subscriptions | 1 February 2024| Accessed on 9 May 2024 | 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://www.ericsson.com/en/press-releases/6/2022/3/ericsson-rogers-launch-canadas-first-commercial-5g-standalone-

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

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] [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]

[17] [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]

[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] [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]

[23] [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]

[24] [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]

[25] [RCR Wireless News | Juan Pedro Tomás | "Vodafone's 5G SA network already reaches 10 million people

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

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]

[26] [Telecomputer | "Yettel Hungary Rolls out 5G SA Network" | https://www.telecompaper.com/news/yettel-hungary-rolls-out-5g-sa-network--1483137 | 21 November 2023 | Accessed on 21 November 2023 | The source is publicly available information and does not contain classification markings]

[27] [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]

[28] [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]

[29] [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]

[30] [Data Center Dynamics | "Three Ireland launches 5G Standalone Network | https://www.datacenterdynamics.com/en/news/three-ireland-launches-5g-standalone-network/ | 9 January 2024 | Accessed on 9 May 2024 | The source is publicly available information and does not contain classification markings]

[31] [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]

[32] [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]

[33] [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]

[34] [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]

[35] [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]

[36] [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]

[37] [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]

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

[38] [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]

[39] [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]

[40] [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]

[41] [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]

[42] [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]

[43] [Data Center Dynamics | "Portugal's NOS launches 5G Standalone Network" | https://www.datacenterdynamics.com/en/news/portugals-nos-launches-5g-standalone-network/ | 30 November 2024 | Accessed on 9 May 2024 | The source is publicly available information and does not contain classification markings]

[44] [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]

[45] [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]

[46] [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]

[47] 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]

[48] [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]

[49] [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]

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

[50] [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]

[51] [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]

[52] [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]

[53] [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]

[54] [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]

[55] [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]

[56] [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]

[57] [RCR Wireless | "Movistar Initially launched 5G SA in 11 Cities Across the Country" | https://www.rcrwireless.com/20230705/carriers/movistar-launches-5g-sa-technology-spain | 5 July 2023 | Accessed on 10 May 2024 | The source is publicly available information and does not contain classification markings]

[58] [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]

[59] [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]

[60] [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]

[61] [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]

[62] [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]

[63] [RCR Wireless News | Catherine Sbeglia Nin | "AIS launched 5G standalone services in July 2020" | https://

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

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]

[64] [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]

[65] [Data Center Dynamics | "Virgin Media O2 launches 5G Standalone Network in UK" | https://www.datacenterdynamics.com/en/news/virgin-media-o2-launches-5g-standalone-network-in-uk/ | 23 February 2024 | Accessed on 9 May 2024 | The source is publicly available information and does not contain classification markings]

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