CLEARED
For Open Publication
Jan 03, 2023
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

5G Core Operate Through Quarterly Update (Q3-2022)

Summary

This report summarizes information on vulnerabilities associated with the 5G network, which could be leveraged by an untrusted network operator, 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 March and 31 May 2022.

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) for this reporting period. 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-2021-44081: A buffer overflow vulnerability exists in the Access and Mobility Management Function (AMF) of open5gs 2.1.4

CVSS[a] Severity V3.1: High; V2.0 Medium

https://nvd.nist.gov/vuln/detail/CVE-2021-44081

- Assessment: Not directly relevant – attack on the 5G core (5GC) network implementation of Open5GS open-source code.
- A buffer overflow vulnerability exists in the AMF of open5gs 2.1.4. When the length of the Mobile Subscriber Identification Number (MSIN) in the Subscription Permanent Identifier (SUPI) exceeds 24 characters, it leads to AMF denial of service.

NIST CVE-2021-44108: A null pointer dereference in src/amf/namf-handler.c in Open5GS 2.3.6

CVSS Severity V3.1: High; V2.0 Medium

https://nvd.nist.gov/vuln/detail/CVE-2021-44108

- Assessment: Not directly relevant - attack on the 5GC network implementation of Open5GS open-source code.
- A null pointer dereference in src/amf/namf-handler.c in Open5GS 2.3.6 and earlier allows remote attackers to perform Denial of Service (DoS) via a crafted Service-Based Interface (SBI) request to the AMF.

[a] Common Vulnerability Scoring System

Contents:

Pg. 1
Summary
Vulnerabilities for Operate Through
NIST NVD Listed

Pg. 2–5
Literature Review

Pg. 5–6
Active Foreign Commercial 5G Standalone Networks

Pg. 7
Projected Growth on 5G Global Connections

Pg. 8–11
Sources

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

22-50105_01

NIST CVE-2021-44109: A buffer overflow in lib/sbi/message.c in Open5GS 2.3.6

CVSS Severity V3.1: High; V2.0 Medium

https://nvd.nist.gov/vuln/detail/CVE-2021-44109

- Assessment: Not directly relevant – attack on the 5GC network implementation of Open5GS open-source code.
- A buffer overflow in lib/sbi/message.c in Open5GS 2.3.6 and earlier allows remote attackers to perform DoS via a crafted SBI request.

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.

Spoofed Networks: Exploitation of GNSS Security Vulnerability in 4G and 5G Mobile Networks

https://ieeexplore.ieee.org/document/9639276

Assessment: This is a third-party attack which utilizes vulnerabilities found in Qualcomm Global Navigation Satellite System (GNSS) chipsets to force a 4G device to attach to a spoofed network. The authors planned to explore the same attack for 5G devices but were not able to do so. Since an untrusted operator already has access to the 5G device, this attack scenario, even if proven for 5G, is not applicable to the Operate Through program.

Abstract: 5G New Radio (NR) represents a shift in mobile telephony whereby the network architecture runs containerized software on commodity hardware. In preparation, numerous 4G software stacks have been developed to test the containerization of core network functions and the interfaces with radio access network (RAN) protocols. In this work, one such stack, developed by the OpenAirInterface Software Alliance (OSA), is used to create a low-cost, simplified mobile network. Commercial off-the-shelf (COTS) UE is then connected to the network to demonstrate how a major buffer overflow vulnerability present in certain GNSS chipsets can be leveraged to enable a spoofed network attack. Finally, the theoretical attack method is extended to 5G NR networks.

A Study on a New Type of DDoS Attack Against 5G Ultra-Reliable and Low-Latency Communications

https://ieeexplore.ieee.org/document/9200956

Assessment: This is a very specific third-party attack to degrade throughput of UEs using enhanced Mobile Broadband (eMBB) by triggering activities in UEs using the Ultra-Reliable Low-Latency Communications (URLLC) use case. Not directly applicable.

Abstract: 5G NR allows eMBB and URLLC to coexist in the physical layer for better resource utilization. To enable coexistence while satisfying the QoS requirement of URLLC, 3GPP introduces the cancellation mechanism that allows a URLLC UE to preempt the transmission of eMBB UEs. In this paper, the authors show that the 3GPP design to provide stringent QoS guarantee for URLLC may become a threat to interfere with both eMBB and URLLC via highly synchronized low-volume Distributed Denial of Service (DDoS). They examine potential vulnerability for both eMBB and URLLC UEs in the uplink from the 3GPP standards. An attack model is investigated and evaluated through system-level simulations. The authors found that synchronization among compromised URLLC UEs could be leveraged by the attacker to amplify the overall impact on both eMBB throughput and URLLC latency, even when the number of compromised UEs is small.

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

On the Efficacy of New Privacy Attacks against 5G AKA

https://www.semanticscholar.org/paper/On-the-Efficacy-of-New-Privacy-Attacks-against-5G-Khan-Martin/667603cdee2bc73c9919726a33ead76e9359dc0e

Assessment: This paper argues that two attacks published in another previous paper are not valid.

Abstract: The Authentication and Key Agreement (AKA) protocol is the primary mechanism in mobile telephony for establishment of a secure channel between mobile subscribers and their service providers. In addition to the requisite security guarantees, provisioning subscription privacy is an essential requirement for AKA. A recent paper by Borgaonkar et al. has uncovered a new vulnerability in one of the associated mechanisms of the AKA protocol. Based upon this vulnerability, Borgaonkar et al. have presented two privacy attacks: the activity monitoring attack and location confidentiality attack. In their paper, the authors analyze these attacks for their effectiveness, practicability, and potency against 5G. Our analysis reveals that the activity monitoring attack is not as effective against 5G as it is against the previous generations (3G/4G). The analysis also brings to light the fact that the location confidentiality attack is a direct extension of an existing privacy vulnerability that affects all generations (including 5G) of mobile telephony. In the paper, the authors also establish that any countermeasure introduced to fix this vulnerability will also render these two new attacks ineffective.

A Systematic Analysis Method for 5G Non-Access Stratum Signaling Security

https://www.researchgate.net/publication/335468013_A_Systematic_Analysis_Method_for_5G_Non-Access_Stratum_Signalling_Security

Assessment: These are third-party attacks with malicious UE and fake gNodeb.

Abstract: This report is based on formal analysis that identified 10 new 5G protocol vulnerabilities and an improved PKI security mechanism targeted at eliminating these vulnerabilities. Firstly, the 5G system, state transition properties, and security properties were abstracted from 3GPP specifications. To mimic an attacker's behavior, a Dolev-Yao adversary model was constructed in the 5G model by empowering it with NAS signaling security testing knowledge and reasonable security capabilities in the wireless channel. Then, the authors used the TAMARIN prover to verify all the abstracted properties one by one and discovered some protocol vulnerabilities based on the counterexamples found. The authors further verified these vulnerabilities on the testbed and identified 10 new 5G protocol vulnerabilities. Moreover, they analyzed the root cause of these vulnerabilities and concluded that all of them were caused by the unconditional trust between UE and gNodeB. Therefore, the authors proposed an improved PKI mechanism based on the existing asymmetric encryption of 5G. Besides the existing public-private key pair of the home network, they introduce a new pair of asymmetric keys in the gNodeB to encrypt and sign the signaling message sent to the UE. The gNodeB can be connected only when the verification succeeds and then the RRC connection can be initiated. This mechanism can effectively avoid all the vulnerabilities found in this paper.

5G Protocol Vulnerabilities and Exploits

http://rogerpiquerasjover.net/5G_ShmooCon_FINAL.pdf

Assessment: This is a general summary of 5G security improvements and suggests digital certificates to close the vulnerabilities with pre-authentication of 5G messages. Not applicable to attacks from an untrusted operator.

Abstract: This is a presentation given by Roger Jover on 5G security at the 2020 Shmoocon that provides a brief history of mobile network security, then delves into a number of attack methods against 4G and 5G networks.

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

4G to 5G: New Attacks

https://www.slideshare.net/3G4GLtd/4g-to-5g-new-attacks

Assessment: Although the title includes 4G and 5G, this document demonstrates attacks possible with the 4G/LTE protocol and hence 5G Non-Standalone (NSA) configuration that does not have any security improvements introduced in 5G Standalone (SA). The UE capability attacks demonstrated for LTE are based on the Man in the Middle (MitM) scenario, which is third-party attack and not directly applicable to the Untrusted Network configuration. However, they are already included in the Battery Draining and UE Capability attacks originated by an Untrusted Operator that INL is planning to assess.

Abstract: This is a presentation by Altaf Shaik (Technische Universität Berlin, Germany) and Ravishankar Borgaonkar (SINTEF Digital, Norway) at HITB GSEC 2019, Singapore, 29 August 2019 that discusses a variety of vulnerabilities, techniques, and tools, including MNMap, Bidding Down, and Battery Drain attacks.

AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks

https://arxiv.org/pdf/2106.05039.pdf

Assessment: Third-party MitM attack resulting in DoS and uplink IMSI extractor.

Abstract: This paper introduces AdaptOver—a MITM attack system designed for cellular networks, specifically for LTE and 5G 5GNSA. AdaptOver allows an adversary to decode, overshadow (replace) and inject arbitrary messages over the air in either direction between the network and the mobile device. Using overshadowing, AdaptOver can cause a persistent (at least 12 hours) DoS or a privacy leak by triggering a UE to transmit its persistent identifier (International Mobile Subscriber Identifier – IMSI) in plain text. These attacks can be launched against all users within a cell or specifically target a victim based on its phone number.

7 Prime 5G Cyber-attack Targets

https://electronics360.globalspec.com/article/17963/7-prime-5g-cyberattack-targets

Assessment: The applicable areas mentioned in this high-level discussion have already been covered in previous documentation, but it is retained here for reference.

Abstract: A high-level overview of seven general types of attacks, including Device Identification, Bidding Down, Spectrum Sharing, Unsecured Endpoints, Poor System Configuration, and Counterfeit/Untrusted/ Legacy Network Components.

Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

https://www.ndss-symposium.org/ndss-paper/privacy-attacks-to-the-4g-and-5g-cellular-paging-protocols-using-side-channel-information/

Assessment: Although the title includes 4G and 5G, this article discusses only the LTE protocol and describes how the location of a LTE device can be derived by identifying its temporary identification used by the network, the Temporary Mobile Subscription Identity (TMSI) and also the persistent identification, i.e., the IMSI itself.

Abstract: In this paper, the authors show that the fixed nature of paging occasions can be exploited by an adversary in the vicinity of a victim to associate the victim's soft-identity (e.g., phone number, Twitter handle) with its paging occasion, with only a modest cost, through an attack dubbed $mathsf{ToRPEDO}$. Consequently, $mathsf{ToRPEDO}$ can enable an adversary to verify a victim's coarse-grained location information, inject fabricated paging messages, and mount denial-of-service attacks. The authors also demonstrate that, in 4G and 5G, it is plausible for an adversary to retrieve a victim device's persistent identity (i.e., IMSI) with a brute-force $mathsf{IMSI-Cracking}$ attack while using $mathsf{ToRPEDO}$ as an attack sub-step.

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

A Systematic Analysis of 5G Networks with a Focus on 5G Core Security

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9709835

Assessment: This paper provides an overview of the major security-related features in 5G networks based on information from several 3GPP technical specifications. It discusses the common Application Program Interface (API) framework (CAPIF) that 3GPP first delivered in Release 15 and then enhanced in Releases 16 and 17 (in the 3GPP TS 23.222 document). Exposing the 5G Core capabilities to API invokers (within or outside trust domains) is critical to the verticals that use 5G as the underlying infrastructure, and also exposes the 5G Core to outside attackers. Not directly applicable.

Abstract: In this paper, the authors review some of 5G's features, including the Service Based Architecture (SBA) and key NFs, the new security features in UE and RAN, the new trust model and security mechanisms (e.g., the 5G AKA protocol), and the newly introduced CAPIF. Along with the review of new features, they provide our observations on the potential security concerns accompanied with the relevant research results in the literature.

Active Foreign Commercial 5G Standalone Networks

Table 2 lists foreign network operators that claim to have launched 5G Standalone (5GSA) commercial mobile services as of 31 May 2022.[b]

Table 2. Foreign 5GSA Commercial Networks

Country	Operator	5GSA Launch	Remarks
Australia	Optus[1] TPG Telecom[2]	November 2021 November 2021	Optus provides 5G services via the 3500 MHz, 2300 MHz, and 2100 MHz spectrum bands.TPG's 5GSA core network runs on TPG's 700 MHz spectrum holdings. Note that TPG now incorporates Vodafone Australia.[3]
Bahrain	STC Bahrain	May 2022	STC Bahrain launched the country's first 5GSA network using Huawei equipment. The network supports eMBB, URLLC, and massive Machine-Type Communications (mMTC) services.[4]
Brazil	TIM Brasil[5]	April 2022	As of April 2022, TIM Brasil had soft-launched its 5GSA core network, the first in South America, for a limited group of users in the 2300 MHz band. 5G services will also be offered in the 3500 MHz band once that spectrum is released for use. 5G services in the 26 GHz band, primarily aimed at hotspot coverage for industrial applications or point to point solutions, are also planned.[6]
Canada	Rogers Communications[7]	March 2022	Rogers' 5GSA network is Canada's first. The company's 5G services operate in the 600, 1700, and 2500 MHz bands.[8]
China	China Mobile[9] China Telecom China Unicom	November 2020[10] November 2020[11] November 2020	As of early 2021, these three operators had deployed over 700,000 5GSA base stations; China Mobile commissioned 5GSA services in all prefectures and cities across China; and China Telecom and China Unicom jointly built the world's largest shared 5GSA network covering 300 cities.
Finland	Telia Company[12]	November 2021	Telia was the first commercially available 5GSA network in the Nordic and Baltic regions. The company offers 5G services in the 700 and 3500 MHz and has also acquired spectrum in the 26 GHz band. The company is working on rolling out 5G services to all of its markets across the Nordic and Baltic countries.[13]
Germany	Deutsche Telekom[14] Vodafone[15]	April 2022 March 2022	Telia was the first commercially available 5GSA network in the Nordic and Baltic regions. The company offers 5G services in the 700 and 3500 MHz and has also acquired spectrum in the 26 GHz band. The company is working on rolling out 5G services to all of its markets across the Nordic and Baltic countries.

[b] This list does not include commercial 5GSA fixed wireless or private networks, or operators engaged in testing or trials.

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

Country	Operator	5GSA Launch	Remarks
Italy	Linkem[16]	October 2021	Linkem's 5GSA network is Italy's first and operates in the 3500 MHz band.
Japan	SoftBank Corp.[17]	October 2021	Supporting SoftBank Air Terminals, SoftBank provides coverage in the 3.9-4.0 GHz and 29.1-29.5 GHz ranges.[18]
Kuwait	STC Kuwait[19]	May 2021	STC's 5GSA services were launched in the 3500 Mhz band and the company expanded its services into the 2100 MHz band, as well.[20]
Philippines	Smart Communications[21]	October 2021	Smart launched the first 5GSA 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.[22]
Saudi Arabia	Zain KSA[23] STC Saudi Arabia[24,25]	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.[26] STC's 5GC supports both 5GNSA and 5GSA services.
Singapore	M1 Limited[27] StarHub Mobile[28] Singtel[29]	July 2021 July 2021 September 2021	M1 and StarHub Mobile engaged in a joint venture to build their 5GSA network; both the M1/StarHub and the Singtel networks were commissioned using the 3500 MHz band.
South Africa	Rain[30]	July 2020	South Africa's Rain launched the first 5GSA network in Africa in partnership with Huawei. Rain secured bandwidth in the 700 MHz and 2600 MHz bands,[31] although it applied for spectrum in the 800 and 3500 MHz bands, as well.[32]
South Korea	KT[33]	July 2021	KT is the first provider in South Korea to launch 5GSA services. In 2018, KT secured 5G spectrum in the 3500-3600 MHz and 26.5-27.3 GHz bands.[34]
Spain	Vodafone[35]	December 2021	Vodafone's initial 5GSA commercial rollout in Spain was for the businesses in the Almeria Science and Technology Park.
Taiwan	Taiwan Mobile Co.[36]	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 Evolved-Universal Terrestrial Radio Access-New Radio (EUTRA-NR) Dual Connectivity (EN-DC) in the 700 MHz, 1800 MHz, 2100 MHz, 3500 MHz, and 28 GHz bands.[37]
Thailand	AIS[38]	July 2020	AIS launched 5GSA services in July 2020,[39] and by August 5GSA had reportedly extended services to all 77 provinces in the country.[40] AIS 5G operates in the 700 MHz, 2600 MHz, and 26 GHz bands.[41]

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

Projected Growth of 5G Global Connections

Figure 1 illustrates the projected growth of 5G global connections[c] from 2021 through 2030 based on data from GSMA, divided by Combatant Command.[d]

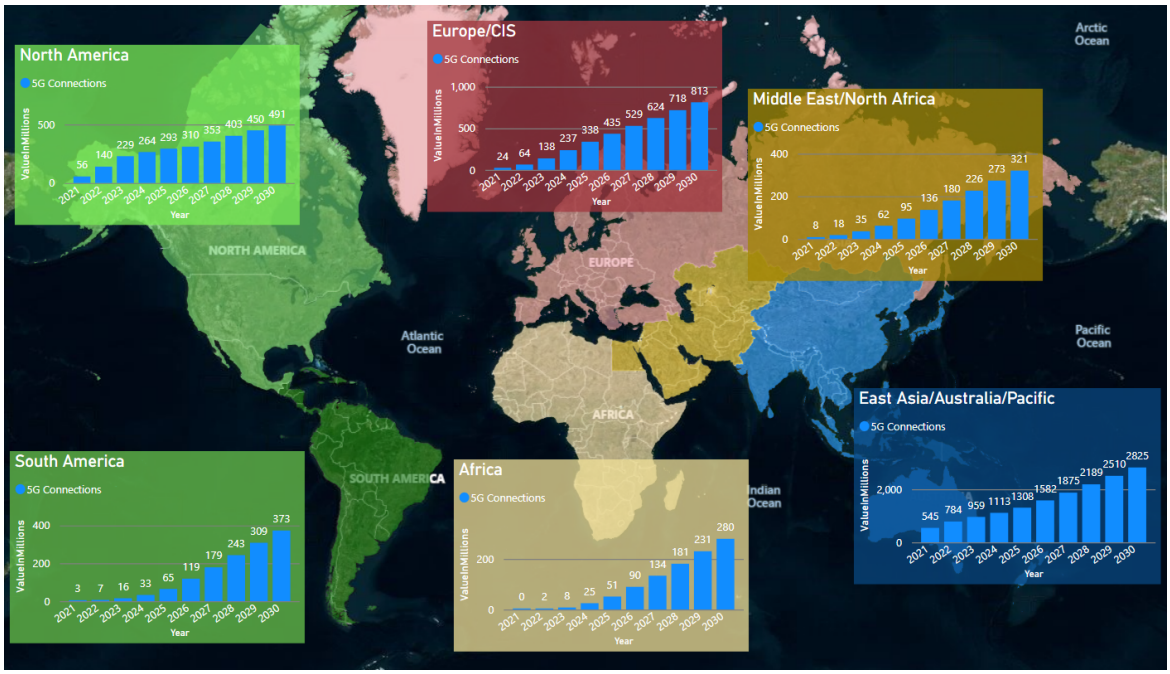

Figure 1: *Growth Projections for Global 5G Connections (GSMA)*

[c] Each connection is defined as being associated with a unique SIM. Note also that the statistics for connections include estimates for devices that use multiple SIMs.

[d] This graphic will be updated periodically to reflect any significant changes in trend projections.

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

Sources

[1] [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]

[2] [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]

[3] [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]

[4] [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]

[5] [TeleSemana.com | Andrea Catalano | "TIM Brasil implementó su red core 5GSA 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]

[6] [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]

[7] [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-network | 28 March 2022 | Accessed on 13 April 2022 | The source is publicly available information and does not contain classification markings]

[8] [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]

[9] [RCR Wireless News | Juan Pedro Tomás | "Chinese telcos expected to deploy 1 million 5GSA 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]

[10] [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]

[11] [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]

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

[12] [Telia Company | "Telia Company launches 5GSA core network in Finland – the first commercially available 5GSA 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]

[13] [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]

[14] [Fierce Wireless | Monica Alleven | "Deutsche Telekom touts 5GSA 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]

[15] [RCR Wireless News | Juan Pedro Tomás | "Vodafone's 5GSA 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]

[16] [Comms Update | "FWA operator Linkem launches Italy's first 5GSA 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]

[17] [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]

[18] [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]

[19] [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]

[20] [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]

[21] [Developing Telecoms | Shailaja Pai | "Smart fires up first 5GSA 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]

[22] [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]

[23] [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]

[24] [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]

[25] [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]

[26] [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]

[27] [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]

[28] [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]

[29][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]

[30] [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]

[31] [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]

[32] [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]

[33] [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]

[34] [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]

[35] [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]

[36] [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]

[37] [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]

[38] [The Fast Mode | Ray Sharma | "Thai Operator AIS, Samsung Launch 5G VoNR over 5GSA 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]

[39] [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 5GSA: 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]

[40] [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]

[41] [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]