DISSERTAÇÃO DE MESTRADO PROFISSIONAL

EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO

RICARDO CINCINATO FREITAS DE OLIVEIRA

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO

RICARDO CINCINATO FREITAS DE OLIVEIRA

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Ugo Silva Dias, FT/UnB _____
Orientador

Prof. Dr. Robson de Oliveira Albuquerque, FT/UnB _____
Examinador Interno

Dr. David Fernandes Cruz Moura, CTEx _____
Examinador Externo

Prof. Dr. Fábio Lúcio Lopes de Mendonça, FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

DE OLIVEIRA, RICARDO CINCINATO FREITAS
EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO [Distrito Federal] 2023.
xvi, 133 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. 5G Tático	2. Exército
3. Defesa	4. Segurança Cibernética
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

DE OLIVEIRA, RICARDO CINCINATO FREITAS (2023). *EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 133 p.

CESSÃO DE DIREITOS

AUTOR: RICARDO CINCINATO FREITAS DE OLIVEIRA
TÍTULO: EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

RICARDO CINCINATO FREITAS DE OLIVEIRA
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Eu dedico este trabalho aos meus amados pais Cincinato de Oliveira Neto (em memória) e Maria Eliedira Freitas Oliveira.

Outrossim, especialmente, eu também dedico este trabalho à minha amada esposa Lenice Teresinha Bieger de Oliveira e aos filhos gêmeos Gabriela Bieger de Oliveira e Eduardo Cincinato Bieger de Oliveira.

AGRADECIMENTOS

Agradeço ao Ilmo Sr Coordenador Paulo Henrique Pinho Sousa, da Agência Brasileira de Inteligência (Abin), à Ilma Profª Drª Márcia Abrahão Moura, Reitora da Universidade de Brasília (UnB) e ao Ilmo Prof Dr Rafael Rabelo Nunes, Coordenador do Programa de Pós Graduação de Engenharia Elétrica (PPEE), pela oportunidade de realização do curso de pós-graduação Stricto sensu em Segurança Cibernética, 1ª Turma da Abin.

Agradeço especialmente ao prezado Prof Dr Ugo Silva Dias, por toda paciência, dedicação e orientações precisas durante as minhas produções acadêmicas: artigo científico e dissertação. A evolução do meu aprendizado nas disciplinas de Comunicações Móveis e Estudos Orientados 1 e 2 serviram de bases sólidas para a produção do meu artigo científico apresentado na Conferência Internacional Multidisciplinar de Pesquisa Aplicada à Defesa e Segurança de 2022 - MICRADS´22 – realizada na Escola Naval de Suboficiais ARC de Barranquilha, em Barranquilha, Colômbia, em julho de 2022; assim como para a produção dessa dissertação nos anos de 2022 e 2023.

Agradeço a todos os valorosos docentes do PPEE por terem modificado o meu pensamento sobre a importância da ciência, a minha visão de mundo, e a minha crença na humanidade, pois eu aprendi muito com todos os senhores: Prof Dr William Ferreira Guiozza (Metodologia da Pesquisa Científica), Prof Dr Demétrio Antônio da Silva (Metodologia da Pesquisa Científica), Prof Dr Rafael Rabelo Nunes (Criptografia e Segurança de Dados), Prof Dr Georges Daniel Amvame Nze (Redes de Comunicação), Prof Dr Rafael Timóteo de Sousa Júnior (Aplicações Distribuídas), Profª Drª Edna Dias Canedo (Tópicos em Redes de Comunicação II) e Prof Dr Fábio Lúcio Lopes de Mendonça (Tópicos em Redes de Comunicação II).

Agradeço distintamente aos Doutores TC Com Lúcio Pinheiro Amaro e Maj Int Leandro Bolzan de Rezende, ambos colegas de profissão no Exército Brasileiro, pelas Cartas de Recomendação escritas por cada um, visando ao meu processo seletivo pela UnB/Abin no ano de 2020.

Agradeço aos meus superiores hierárquicos, atuais e antigos, dentro e fora do Exército Brasileiro, porque sempre confiaram em mim, bem como possibilitaram as liberações durante os horários dos expedientes e das missões extras para eu realizar esse mestrado profissional semi-presencial na UnB.

Agradeço ao camarada TC QEM José Eduardo França, da Subchefia de Comando e Controle do Ministério da Defesa (MD), por me fornecer o material didático sobre o Sistema Militar de Comando e Controle (SISMC²) e pelas informações das possibilidades de integração do 5G na Rede Corporativa do Exército (EBNet).

Agradeço ao Ilmo Sr Gustavo Viana Penido, engenheiro elétrico e funcionário da operadora de telefonia móvel Claro SP, colega da disciplina optativa 366129 – Comunicações Móveis na UnB, pela amizade e ajuda nos estudos da disciplina, além das orientações precisas sobre o sinal 5G da Claro no DF.

Agradeço ao Ilmo Sr Ricardo Fernandes de Albuquerque, engenheiro elétrico e funcionário da operadora de telefonia móvel Tim DF, pois gentilmente me forneceu os dados técnicos dos equipamentos do Sítio Móvel 5G Tim DF utilizado no Forte Caxias Quartel General do Exército (QGEx), além das fotos e custos dos equipamentos 5G embarcados na viatura *Sprinter* Furgão *Street* 415 CDI Mercedes Benz

empregado na Esplanada dos Ministérios durante a Operação Posse, em 1º de janeiro de 2023.

Agradeço aos camaradas do Centro de Instrução de Guerra Eletrônica (CIGE), Cel Com Valdecir Gregory, ex-comandante do CIGE, por ter aberto as portas da Organização Militar (OM) para os meus estudos da UnB desde 2021. E agradeço ao Cap Com Hugo dos Santos Fontes, instrutor do Curso de Planejamento de Guerra Eletrônica e Cibernética em Apoio às Operações, por ter me instruído na utilização do *software HTZ Warfare* e auxiliado na simulação das imagens da área de cobertura do sinal 5G no Setor Militar Urbano (*Clusters* coloridos), com os dados reais das ERB locais da empresa Claro DF, do SMU, por meio da página eletrônica da Agência Nacional de Telecomunicações (Anatel).

Agradeço ao camarada TC Inf Nemuel de Almeida Ramos, ex-comandante da 7ª Companhia de Inteligência (7ª Cia Intlg), situada em Brasília/DF, por ter me emprestado o *drone Mavic 2 Enterprise* utilizado no experimento de monitoramento eletrônico das áreas estratégicas no SMU, durante os meses de novembro e dezembro de 2022.

Agradeço ao camarada 1º Sgt CBMGO Nilton de Almeida Ramos, lotado no Corpo de Bombeiros Militar do Goiás (CBMGO), situado em Goiânia/GO, por ter realizado gentilmente uma instrução prática sobre o *software Litchi* e também auxiliado na confecção do Plano de Voo do *drone Mavic 2 Enterprise* da 7ª Cia Intlg.

Agradeço aos colegas mais próximos do curso do PPGEE da Abin/UnB, pela amizade sincera, incentivos nos momentos de maiores dificuldades do meu curso, pela ajuda mútua e confiança plena nas minhas sugestões nos trabalhos realizados em grupo ou em dupla: Alcides Francinaldo Souza Macedo, Alexandre Cabral Godinho, André Luiz Bandeira Molina, Cileno de Magalhães Ribeiro, João Alberto Pincovscy, Luiz Guilherme Schiefler de Arruda, Renato Luiz Alves Tavares, e Sávio Levy Rocha.

Agradeço aos demais colegas de curso do PPGEE da Abin/UnB pelos conhecimentos compartilhados durante as aulas remotas e apresentações nas atividades semanais curriculares em grupo.

Agradeço às secretárias Sra Adriana Reis da Silva e Srta Tayná Gabriela Araújo Albuquerque, pela paciência, esmero em resolver as minhas necessidades de aluno, por diversas vezes urgentes, e pela amizade fraternal que construímos ao longo desses dois anos de curso na FT/UnB.

Agradeço, distintamente, ao meu ex-chefe da Seção de Operações do Comando Militar do Planalto, o Cel Inf André Luciano Bittencourt Barbosa, que trabalhou como Diretor do Departamento de Assuntos da Câmara de Relações Exteriores e Defesa Nacional, no Gabinete de Segurança Institucional (GSI) da Presidência da República (PR), nos anos de 2020 a 2022. A sua crença no meu valor profissional tornou viável a minha inscrição no processo seletivo do Edital nº 8/2020, do PPGEE/UnB, no ano de 2020. Sem os seus incentivos, sua amizade verdadeira e suas orientações precisas, eu não teria me inscrito, muito menos, logrado o êxito esperado nesse curso de pós-graduação valoroso da Abin/UnB.

Agradeço, especialmente, à minha amada família, esposa Lenice Teresinha Bieger de Oliveira e filhos gêmeos Gabriela Bieger de Oliveira e Eduardo Cincinato Bieger de Oliveira. Vocês compreenderam todas as minhas ausências nos momentos das reuniões familiares, principalmente nas escritas científicas do artigo e dessa dissertação, pelos incentivos diários nos meus estudos e pesquisas de campo.

Por fim, sobretudo, agradeço ao nosso Deus, criador maior deste mundo maravilhoso e de todos os seres vivos, por ter me presenteado com o dom da vida e ter me incluído em uma família feliz e unida.

RESUMO

Título: EMPREGO DO 5G NA DEFESA E SEGURANÇA NACIONAL: POSSIBILIDADES, LIMITAÇÕES E UMA PROPOSTA CONCEITUAL DE ARQUITETURA PARA O EXÉRCITO BRASILEIRO.

Autor: Ricardo Cincinato Freitas de Oliveira.

Orientador: Ugo Silva Dias, Dr.

Coorientador: Georges Daniel Amvame Nze, Dr.

Programa de Pós-Graduação Profissional em Engenharia Elétrica (Mestrado) – Área de Concentração em Segurança Cibernética.

Brasília, 29 de junho de 2023.

Atualmente vivemos na Era da Informação e com o advento do Ecossistema 5G no mundo por meio das Telecomunicações Móveis Internacionais (IMT–2020 e Além), divulgada pela ITU no ano de 2015, logo as ameaças cibernéticas se tornaram mais abrangentes por causa do Poder Cibernético e da Grande Competição de Potências entre os Estados–Nação, na busca da supremacia da Informação. Este trabalho consiste em uma ampla pesquisa bibliográfica e documental realizada entre diversas fontes (primárias, secundárias e terciárias) acadêmicas internacionais e nacionais dos anos 2015 a 2023, de natureza aplicada, com abordagem qualitativa, e com objetivo exploratório, abordando alguns conceitos doutrinários internacionais e nacionais sobre Segurança Cibernética e sobre o emprego militar do Ecossistema 5G. Foi aplicado um questionário *On-line* para grupos de militares do Exército que abordava as possibilidades e limitações do emprego militar do Ecossistema 5G Brasil visando a Defesa Nacional. E foi realizada uma simulação eletrônica no *software HTZ Warfare* para definição das áreas de coberturas do sinal 5G no Setor Militar Urbano, no Distrito Federal. Tanto o Questionário *On-line*, quanto a simulação do 5G no *software HTZ Warfare* serviram de base para a proposta final de arquitetura conceitual de 5G Tático para o Exército empregar em Operações coordenadas pelo Ministério da Defesa e pelo Comando de Operações Terrestres.

Palavras-chave: 5G Tático, Exército, Defesa, Segurança Cibernética.

ABSTRACT

Title: USE OF 5G IN NATIONAL DEFENSE AND SECURITY: POSSIBILITIES, LIMITATIONS AND A CONCEPTUAL ARCHITECTURE PROPOSAL FOR THE BRAZILIAN ARMY.

Author: Ricardo Cincinato Freitas de Oliveira.

Advisor: Ugo Silva Dias, Dr.

Co-advisor: Georges Daniel Amvame Nze, Dr.

Professional Graduate Program in Electrical Engineering (Master's) – Concentration Area in Cybernetic Security.

Brasília, June 29, 2023

We currently live in the Information Age and with the advent of the 5G Ecosystem in the world through International Mobile Telecommunications (IMT–2020 and Beyond), released by ITU in 2015, cyber threats have soon become more comprehensive because of Cyber Power and the Great Competition of Powers between Nation States, in the search for Information supremacy. This work consists of a broad bibliographic and documentary research carried out among several (primary, secondary and tertiary) international and national academic sources from 2015 to 2023, of an applied nature, with a qualitative approach, and with an exploratory objective addressing some international and national doctrinal concepts on Cybersecurity and on the military employment of the 5G Ecosystem. A questionnaire was applied On-line to groups of Army military personnel that addressed the possibilities and limitations of the military use of the 5G Brazil Ecosystem aiming at National Defense. And an electronic simulation was carried out in the HTZ Warfare software to define the 5G signal coverage areas in the Urban Military Sector, in the Federal District. Both the online questionnaire and the 5G simulation in HTZ Warfare software served as the basis for the final proposal of a conceptual architecture of Tactical 5G for the Army to employ in Operations coordinated by the Ministry of Defense and the Land Operations Command.

Keywords: *Tactical 5G, Army, Defense, Cybersecurity.*

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

De acordo com [1], [2] em meados de 1960 foi desenvolvida a ARPANET, uma rede telefônica cabeada composta por nós e centrais de comutação de voz analógica capaz de realizar a comunicação estratégica dos órgãos do governo dos EUA e também suportar um possível ataque nuclear da URSS durante a Guerra Fria, tendo em vista que todas as comunicações militares utilizavam a rede de telefonia pública dos Estados Unidos da América (EUA), considerada vulnerável e limitada na época.

Essa denominação de "Rede ARPA"ocorreu por causa dos financiamentos financeiros repassados pela Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency* (ARPA)), oriunda do Departamento de Defesa (*Department of Defense* (DoD)) dos EUA [1], [2].

Em 1969, a ARPANET evoluiu rapidamente das centrais de comutação de comunicação por voz analógica com velocidade de de 56 Kbps, para centrais de comutação de comunicação por dados digitais que atingiram 45 Mbps, em 1990, com a implantação da Rede Avançada de Redes e Serviços (*Advanced Networks and Services Net* (ANSNET)), nos EUA [1], [2].

Nessa época existiram diversos projetos científicos em outros países, principalmente europeus e asiáticos, os quais pesquisaram e desenvolveram redes de computadores similares àquelas nos EUA. E foi através das pesquisas conjuntas das universidades e órgãos do governo dos países europeus e asiáticos com as universidades e os órgãos do governo dos EUA que criaram a Rede Mundial de Computadores (*World Wide Web*[1] (WWW)) no final da década de 1980 [1], [2].

Realmente, foi a partir da Globalização, meados de 1990, que a Internet discada se popularizou e se firmou como o principal forma de comunicação humana na sociedade contemporânea [1], [2], [3]. Contudo, os desafios atuais da comunicação global permanecem os mesmos desde os primórdios da Internet cabeada de 1960, apesar das melhorias já alcançadas com a Internet Banda Larga via fibra óptica e com a Internet Banda Larga sem fio atuais. São 3 fatores principais (desde os primórdios) que limitam o uso da Internet [4]: (i) restrições de múltiplo acesso; (ii) restrições de potência; e (iii) restrições do uso do Espectro Eletromagnético[2] (EEM).

Atualmente a Internet Banda Larga emprega variados equipamentos e dispositivos de Tecnologia de Informação e Comunicação (TIC) nas redes cabeadas (Coaxial, Par Trançado Não Blindado (*UnShielded Twisted Pair* (UTP)) e Fibra óptica) padrão IEEE 802.3 e também nas redes sem fios formadas pelas diversas tecnologias que utilizam faixas do EEM padronizadas pela **União Internacional das Telecomu-**

[1] Em [2] descreve que a *Web* foi criada no Centro Europeu para Física Nuclear (*European Center for Nuclear Physics* CERN)) por Tim Berners-Lee, entre os anos de 1989 e 1991, baseada nos trabalhos antecessores do Hipertexto criado por Vannevar Bush, na década de 1940 e, também, por Ted Nelson na década de 1960. Em resumo, Berners-Lee e seus companheiros criaram versões iniciais da Linguagem de Marcação de Hipertexto *HyperText Markup Language* (HTML)), do Protocolo de Transferência de Hipertexto (*HyperText Transfer Protocol* (HTTP)), um Servidor *Web* e de um Navegador (*Browser*), ou seja, criaram os 4 componentes fundamentais para operação na *World Web Wide*.

[2] Em [5], [6] o físico alemão Henrich Hertz descobriu as diversas faixas de frequências e comprimentos de ondas do Espectro Eletromagnético (EEM), no seu laboratório na Alemanha, no ano de 1887.

nicações[3] (ITU)), as quais são usadas como canais de comunicação de dados digitais (*bits*) nos padrões IEEE 802.11 (a/b/g/n/ac/ax) (*WiFi*) (2,4 – 5,8 GHz) [2], [8]; IEEE 802.15.1 (*Bluetooth*) [2], [9] (2,4 GHz da ISM (*Industrial Scientific Medicine*)); IEEE 802.15.4 (*ZigBee*) (2,4 GHz) [2], [8]; IEEE 802.16 (*WiMax*) [2], [10]; e tecnologias celulares IEEE 802.20 do 1G até 5G [11], [12], [13], [14], [15], [16], [17], [18].

De acordo com [3] existem 2 casos principais de emprego do EEM nas Comunicações sem Fio:

1. **EEM licenciado**: a ITU-R regulou o uso e a exploração comercial do EEM nas 3 Regiões Globais [19], pois as operadoras pagam verdadeiras fortunas pelos lotes das faixas de frequências das bandas subcontratadas, geralmente visando alcançar coberturas do sinal de dezenas a centenas de Km.
2. **EEM não licenciado**: quando o uso do EEM é gratuito em redes domésticas e redes pessoais com alcances locais curtos desde unidades até centenas de metros.

A cada ano cresce o número de usuários da Internet e também de aparelhos celulares no mundo conforme registra [11]. Esses dois fatores principais causaram também o aumento na demanda de dados e, consequentemente, o aumento do consumo de novas faixas do EEM ainda disponíveis para atender essa demanda crescente, segundo demonstra a Figura 1.1 – Volume de tráfego de dados para a Europa Ocidental e América do Norte entre os anos de 2010 – 2020 a seguir.

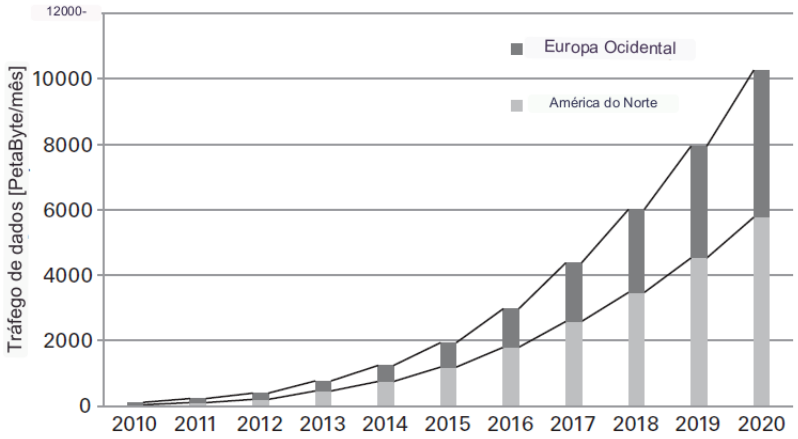

Figura 1.1: Volume de tráfego de dados para a Europa Ocidental e América do Norte entre 2010 – 2020 [11]

Das assertivas acima e da análise das informações da Figura 1.1, deduz-se que vivemos em um mundo de conectividade formada por redes cabeadas e redes sem fio com necessidades de consumo baseadas em altas taxas de tráfego de dados. Além disso, utilizamos diariamente as redes de comunicações móveis para acessar a Internet, bem como para outras aplicações em rede [1], [2]. Por exemplo: (i) trocar arquivos digitais (fotos, áudios, vídeos, textos .pdf, etc) por meio do *Bluetooth* entre dois ou mais dispositivos

[3]Em [7] ITU: é a agência das Nações Unidas (NU) especializada na gestão da TIC mundial, sediada em Genebra, na Suíça, e realiza: (i) gestão do EEM global; (ii) fomento às pesquisas científicas para as Telecomunicações Móveis Internacionais (IMT); (iii) eventos internacionais para divulgação das tecnologias de telecomunicações e padronizações em desenvolvimento; e (iv) publicação de revistas especializadas em comunicações, consultoria jurídica, finanças, pessoal, compras, auditoria interna e outros serviços para os seus membros associados.

(*tablets* e celulares) [20]; (ii) acessar videogames via *WiFi*; (iii) acessar TVs inteligentes via *WiFi*; (iv) acessar Pontos de Acesso (*Access Point*) na residência, nos estabelecimentos comerciais e nas instituições públicas via *WiFi*; (v) controlar robôs e máquinas industriais via *WiFi*; e (vi) controlar eletrodomésticos presentes nas redes *Bluetooth* e *ZigBee* da Internet das Coisas (*Internet of Things*(IoT)) [8].

O termo "**Ecossistema 5G**"foi citado de forma genérica neste trabalho para simplificar o entendimento geral dos leitores sobre as diversas instituições, atores envolvidos na implantação/implementação das tecnologias derivadas dos 3 serviços da 5ª Geração das Telecomunicações Móveis Internacionais (IMT) sem fio, os quais serão abordados e detalhados na Seção do Referencial Teórico deste trabalho, a saber: (i) **Banda Larga Móvel aprimorada** (*enhanced Mobile Broadband* (eMBB)) [11], [12], [13], [18], [21], [22]; (ii) **Comunicação Tipo Máquina massiva** (*massive Machine Type Communication* (mMTC)) [11], [12], [13], [21], [22], [18]; e **Comunicação Ultra-Confiável de Baixa Latência** (*Ultra-Reliable Low Latency Communication* (URLLC)) [11], [12], [13], [17], [18], [21], [22].

A principal definição para **Ecossistema 5G Brasil** [23]: é o Projeto 5G Brasil [24] formado por diversas instituições brasileiras em parcerias público-privadas dedicadas para desenvolver o Ecossistema 5G no Brasil [24], tais como: (i) Poderes públicos Federal, Estaduais e Municipais; (ii) Agências padronizadoras, reguladoras, governamentais e de fomento; (iii) Fabricantes de equipamentos e dispositivos de TIC; (iv) Prestadoras de Serviços de Telecomunicações; (v) Operadoras de Redes de Telecomunicações; (vi) Provedores de soluções e aplicações (da Internet); (vii) Usuários de mercados verticais; e (viii) Universidades e Institutos de Inovação, Pesquisa e Desenvolvimento. A Figura 1.2 – Associados do Projeto 5G Brasil demonstra os participantes do Ecossistema 5G Brasil a seguir.

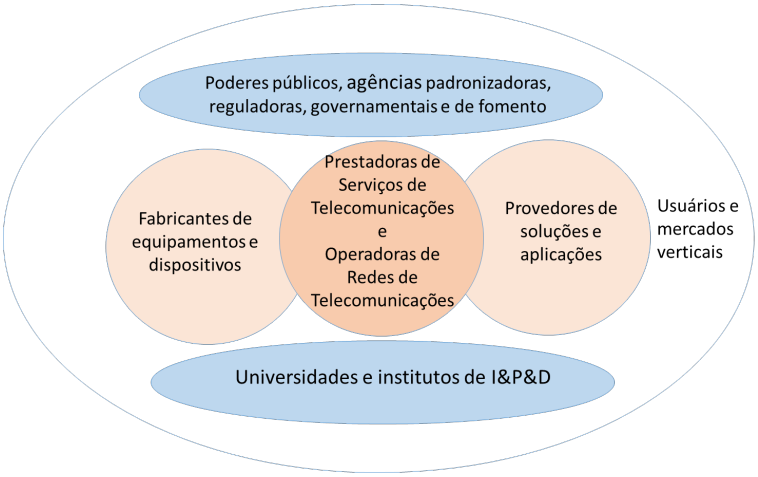

Figura 1.2: Associados do Projeto 5G Brasil [24]

Da análise da Figura 1.2 e segundo [25], observa-se que o Ecossistema 5G Brasil é formado pelas diversas associações de empresas, centros de pesquisas industriais, órgãos de classe, academias universitárias e órgãos governamentais brasileiros.

Os representantes legais do Projeto 5G Brasil assinaram um acordo de cooperação tecnológica para o desenvolvimento de tecnologias 5G com União Europeia (5G–3PPP), EUA (4G AMERICAS), Coreia do Sul (Fórum 5G da Coreia), Japão (5GMF) e China (IMT–2020) [25], [26], [27], [28] abrangendo desde a pesquisa básica e aplicada, até o desenvolvimento de produtos e soluções de sistemas de engenharia,

industrialização de produtos e soluções, aplicações práticas e compartilhamento de informações. Exemplos de instituições do Ecossistema 5G Brasil [25]: (i) Abnee; (ii) Algar Telecom; (iii) CETUC; (iv) Claro; (v) Cinexis brasil.digital; (vi) ConTIC; (vii) CPqD; (viii) Ericsson; (ix) Febratel; (x) FANAINFO; (xi) FITec; (xii) Huawei; (xiii) Inatel; (xiv) *Informa Exhibitions*; (xv) NEC; (xvi) Nokia; (xvi) Oi; (xvii) Qualcomm; (xix) Sindisat; (xx) Telebrasil; (xxi) Telefônica; (xxi) Tim; e (xxii) Trópico.

Os requisitos impostos pela ITU para o Rádio 5G Nova Geração (*5G New Radio* (5G RAN)) previstos na ***Recommendation ITU-R M.2083-0 (09/2015) IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*** [22], contém as tendências das tecnologias para as Telecomunicações Móveis Internacionais (IMT) apresentadas na Conferência Mundial de Radiocomunicações de 2015 (*World Radiocommunication Conference 2015 (WRC-15)*), em Genebra, na Suíça [22].

E a evolução dos requisitos impostos pela ITU nas **IMT–2020 e Além** para o Rádio 5G Nova Geração (*5G New Radio* (5G RAN)) também estão previstos na ***Recommendation ITU-R M.2150-1 (02/2022) Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020 (IMT-2020)*** [29], elaborada pelo Grupo de Estudo 5G (SG 5G) de Genebra, na Suíça, os quais possibilitaram o aumento considerável das velocidades de *download* (DL) e de *upload* (UP) de dados (*bits*) nas redes móveis do Ecossistema 5G sobre as gerações anteriores 4G/3G [13], [18].

Hoje o Ecossistema 5G é considerado o **Estado da Arte** [12], devido aos 3 serviços (eMBB, mMTC, e URLLC) com suas tecnologias previstas nas Rec ITU-R M.2083-0 (09/2015) (**IMT-2020 e Além**) e Rec ITU-R M.2150-1 (02/2022), conforme sintetiza a Figura 1.3 – Conceitos de Convergência do 5G (Banda Larga Móvel, Infraestrutura Fixa de IP, Interface Rádio e Arquitetura de Rede) abaixo.

Da análise das informações da Fig 1.3 abaixo, verificam-se os requisitos das comunicações móveis do 5G e suas tecnologias derivadas, tais como: (i) Redes Onipresentes; (ii) Redes Heterogêneas; (iii) Antenas MU–MIMO massivo; (iv) Ondas milimétricas; (v) Aumento exponencial da capacidade de tráfego (*bits*) do sinal sem fio (*Download* (DL) e *Upload* (UP)) sobre as antigas gerações 3G/4G; (vi) Disponibilidade de exploração de novas faixas do EEM não licenciado pela ITU; (vii) Permite comunicações com baixíssima latência, altíssima velocidade e inúmeros assinantes/usuários simultâneos em áreas externas (*outdoor*) e áreas internas (*indoor*) empregando algum dos 3 serviços (eMBB, mMTC, e URLLC); e (viii) Possibilita conectar pessoas e objetos (coisas) por meio do Protocolo da Internet versão 6 (*Internet Protocol version 6* (IPv6)) com dispositivos de Internet de Tudo (*Internet of Everything* (IoE)) [12].

Desde a divulgação oficial do Ecossistema 5G pela ITU, os demais atores desse ecossistema buscam melhorar os processos para atingirem a Indústria 4.0[4] e também atingir o conceito da Sociedade 5.0[5], por meio das redes móveis de última geração do 5G [12].

No entanto, com o advento do 5G no mundo desde 2015, as autoridades governamentais responsáveis pelas Seguranças da Informação, das Comunicações e Cibernéticas estimam que as ameaças cibernéticas

[4]Em [30] Indústria 4.0: é o conceito atual da 4ª Revolução Industrial, que surgiu em 2011, na Feira de *Hannover*, na Alemanha. Corresponde ao emprego da alta tecnologia na indústria: robótica, inteligência artificial, aprendizado de máquina, comunicação tipo máquina massiva, comunicação ultra confiável de baixa latência na automação industrial, fábrica inteligente, nanotecnologia, escaneamento 3D, telemedicina, veículo autônomo, etc.

[5]Em [31] Sociedade 5.0: é o conceito atual que surgiu no Japão, no ano de 2016, para identificar uma sociedade mais responsável com as questões humanitárias, mais conectada digitalmente, com igualdade social e bem-estar apoiados em altas tecnologias (Big Data, Internet das Coisas (IoT), e Inteligência Artificial (IA)) para a resolução de grandes problemas da sociedade: (i) Competitividade; (ii) Produtividade; (iii) Conexão; e (iv) Bem-estar social.

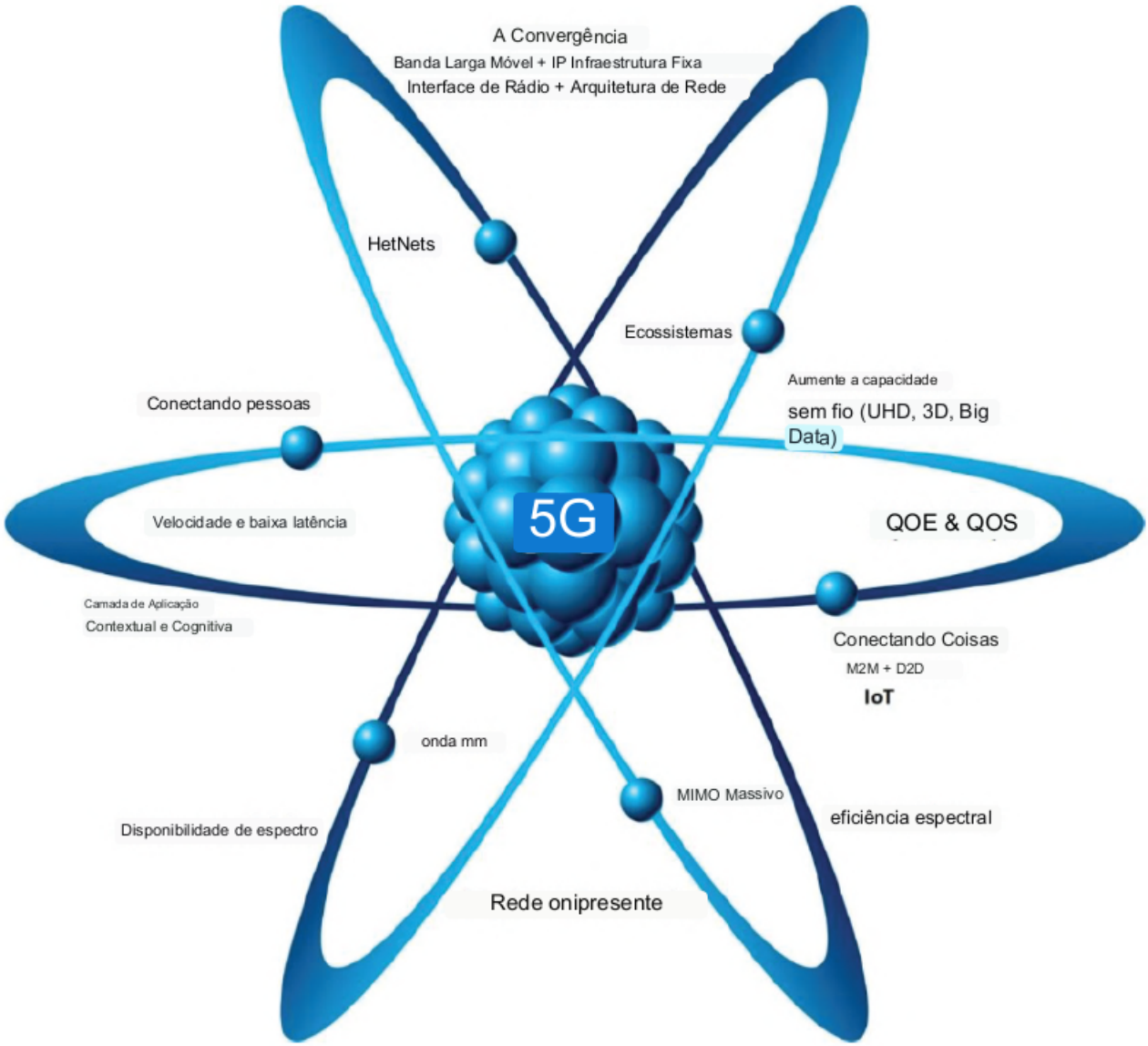

Figura 1.3: Conceitos de Convergência do 5G (Banda Larga Móvel, Infraestrutura Fixa de IP, Interface Rádio e Arquitetura de Rede) [12]

se tornaram mais próximas dos usuários das redes móveis de comunicações sem fio por causa da utilização da Internet Banda Larga na "palma da mão", podendo ser acessada em qualquer lugar, a qualquer hora, e por qualquer indivíduo ou máquina/dispositivo [12].

Baseados nos conceitos atuais de **Poder Cibernético (P Ciber)** [32], [33], [34] e **Grande Competição de Potências (GPC)** [35], [36], os estudiosos estimam que à medida que os Espaços Cibernéticos[6] permeiam as sociedades, os governos e os Estados-Nação, os mesmos podem ser usados para conquistarem e manterem seus Objetivos Nacionais Permanentes (ONP) através da supremacia da **informação**, como também, por diversas vezes, empregam a **desinformação** através de narrativas criadas para influenciar o Ambiente Operacional[7] por meio de Guerras da Informação[8] [40], [41]; Guerras Cibernéticas[9] [37], [42], [43], [44], [45], [46], [47], [48] e Guerras Omnidirecionais[10] [35], [40], para atacar, proteger, e explorar a Segurança Cibernética das Infraestruturas Estratégicas (IE), também denominadas Infraestruturas Críticas (IC) [50] dos países alvos [37], [51], [52], [53], [54], por exemplo: (i) Rússia X Geórgia (2010); (ii) Israel X Irã (2010); (iii) Rússia X Ucrânia (2014); (iv) China X EUA (2019) e (v) Rússia X Ucrânia (2022).

A Presidência da República (PR) visando manter e aprimorar a **Segurança da Informação**[11] **(Seg Info)** brasileira, a qual engloba também a Segurança das Comunicações (Seg Com) e a Segurança Cibernética (Seg Ciber), estabeleceu critérios de segurança e padronizou ações para proteção dos diversos órgãos do Governo brasileiro, instituições participantes da Administração Pública Federal (APF), Instituições Privadas e as IC brasileiras. Por isso publicou um arcabouço legal para ser seguido e fiscalizado com os seguintes documentos: (i) Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) em 2018

[6]Em [37] define o Espaço Cibernético: é o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas. Enquanto que para [38] de acordo com o Departamento de Defesa dos EUA: é um domínio global dentro do ambiente de informações que consistem das redes interdependentes de infra-estruturas de Tecnologia da Informação (TI), incluindo a Internet, redes de telecomunicações, sistemas de computador, processadores e controladores embutidos.

[7]Em [39] Ambiente Operacional: é o conjunto de condições e circunstâncias que afetam o espaço onde atuam as forças militares e que interferem na forma como são empregadas, é composto pelas 3 Dimensões: (i) Física; (ii) Humana; e (iii) Informacional.

[8]Em [40] descreve a Guerra da Informação no seul livro como uma forma do Estado e das mídias (impressas, radiofônicas, televisivas e digitais) poderem exercer a sua comunicação com a massa da população do país e usarem Informação/Desinformação como Arma. Contudo, são publicadas diferentes versões para um mesmo fato ocorrido, sendo uma versão baseada na Informação e outra versão baseada na Desinformação, mas ambas são usadas para atingirem objetivos e interesses dos seus autores. Enquanto que [41] descreve a Guerra da Informação no seu artigo científico como um conceito empregado pelo Exército Brasileiro para se referir à Doutrina das Operações da Informação, que são ações específicas para se influenciar pessoas, num determinado momento histórico, com objetivos específicos. Assim como adotado pelo DoD dos EUA, o Exército entende que o termo Guerra da Informação (*Information War*) não é sinônimo de Guerra Informacional (*Information Warfare*). Apesar de ambos serem traduzidos para o português como Guerra de Informação são fenômenos com significados diferentes para as Forças Armadas no mundo. Em resumo: a Guerra da Informação é um fenômeno complexo em 3 dimensões: (i) Física; (ii) Informacional; e (iii) Psíquica. Contudo, em todas essas 3 dimensões o objetivo é causar efeitos cognitivos e emocionais nas massas pessoais para demonstrar uma realidade.

[9]Em [37] descreve a Guerra Cibernética como: (i) ações de ataque; (ii) ações de defesa; e (iii) ações de exploração cibernéticas. Enquanto que em [] descreve a Guerra Cibernética como usos Ofensivo e Defensivo de Informação e dos sistemas de informação para negar capacidades de C² ao inimigo/adversário, visando explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar nos Níveis Operacional e/ou Tático, ou de uma Operação Militar.

[10]Em [49] define a Guerra Omnidimensional: é a guerra que não será caracterizada por dimensões ou espaços (tangíveis ou não); nem por uma ou por outra tecnologia. Será uma Guerra caracterizada pela multidimensionalidade e pela utilização de toda tecnologia disponível em todo espaço possível.

[11]*Em [55] NIST SP 800 – 12 REV. 1 – An Introduction to Information Security* descreve a **Segurança da Informação**: é a proteção da informação e dos sistemas de informação contra acesso, utilização, divulgação, perturbação, modificação ou destruição não autorizados, visando assegurar sua Confidencialidade, Integridade e Disponibilidade, sintetizadas no acrônimo **CID**. Enquanto que [56] a Norma ISO/IEC 27001 – Gestão da Segurança da Informação descreve os conceitos de **Confidencialidade (C)** para o acesso das informações permitido somente às pessoas autorizadas; **Integridade (I)** como a veracidade das informações sem alterações; e **Disponibilidade (D)** como a informação acessível em qualquer momento.

[57]; (ii) Política Nacional de Segurança da Informação (PNSI) em 2018 [58]; e (iii) Estratégia Nacional de Segurança Cibernética (E-Ciber) em 2020 [59].

A Figura 1.4 – Quadro demonstrativo da Segurança da Informação, das Comunicações e Segurança Cibernética (SIC Ciber) [60] ilustra a Estrutura (*Framework*) empregado pelo Governo brasileiro para manter e aprimorar as Seguranças da Informação, das Comunicações e Cibernética a seguir.

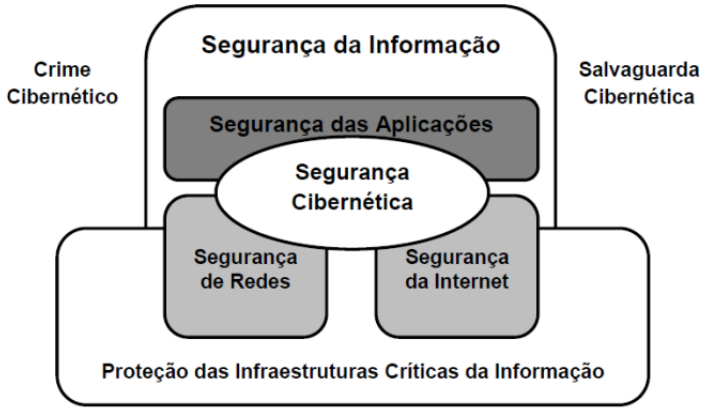

Figura 1.4: Quadro demonstrativo da Segurança da Informação, das Comunicações e Segurança Cibernética (SIC Ciber) brasileiras [60]

Das assertivas acima e da análise das informações da Figura 1.4 acima, verifica-se que a **Dimensão Informacional** do Ambiente Operacional (formado pelos 6 Domínios: Marítimo, Terrestre, Aéreo, Espacial, Cibernético, e Eletromagnético) possui vulnerabilidades passíveis de ameaças cinéticas e cibernéticas previstas nas Operações de Convergência realizadas no Amplo Espectro dos Conflitos[12], devendo serem neutralizadas essas vulnerabilidades e/ou minimizados os danos dessas ameaças com medidas deProteção Cibernética.

Abaixo a Figura 1.5 – Bússola da Proteção Cibernética descreve as ações que devem ser realizadas para se manter Segurança da Informação (Seg Info) no Estado brasileiro visando: (i) reduzir as vulnerabilidades em TI; (ii) prevenir e responder às ameaças imediatas; (iii) integrar-se em redes colaborativas; e (iv) prevenir os ativos de informação.

De acordo com o manual Doutrina Militar de Defesa Cibernética [37] o Brasil precisa ter capacidade para se defender de ameaças externas, de modo compatível com sua própria dimensão territorial e suas aspirações político-estratégicas no cenário global. Somente assim conseguirá desenvolver seus Objetivos Nacionais Permanentes (ONP), preservar seus interesses nacionais, e exercer seu direito de defesa, conforme regulam o ordenamento jurídico internacional [47] e sua própria CFRB/1988 [61].

Das assertivas acima e das análises das informações da Figura 1.4 acima e da Figura 1.5 abaixo, conclui-se que o conceito de **Ciber**[13] **Proteção** é necessário para guiar o Estado brasileiro nas ações de manutenção e aprimoramento da Seg Info nas diversas instituições governamentais da APF, das instituições não-governamentais privadas e da Estutura Militar de Defesa (Etta Mil D) formada pelo Ministério

[12]Em [39] Amplo Espectro dos Conflitos: é o conceito moderno que aborda desde a situação de Paz até as situações de Conflito Armado/Guerra, passando pelas situações de Crises, sob a responsabilidade direta de autoridade militar competente.

[13]Em [44] o termo "Ciber"é utilizado para representar tudo o que está relacionado a sistema computacional.

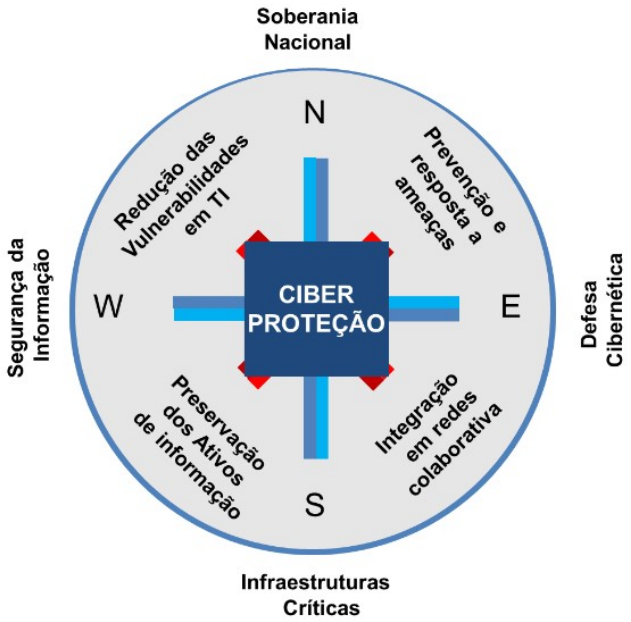

Figura 1.5: Bússola da Ciber Proteção [54]

da Defesa (MD) e pelas Forças Armadas (FA): (i) Marinha do Brasil; (ii) Exército Brasileiro (EB); e Força Aérea Brasileira (FAB).

Em [37] descreve os níveis decisórios e os atores responsáveis em cada nível da **Seg Ciber** brasileira, os quais estão sintetizados na Figura 1.6 – Níveis decisórios e atores do Setor Cibernético brasileiro a seguir.

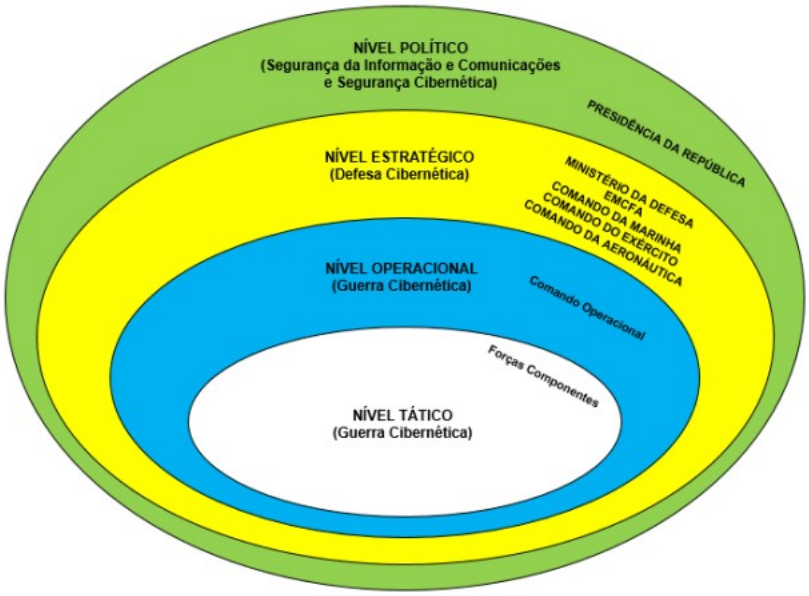

Figura 1.6: Níveis decisórios e atores do Setor Cibernético brasileiro [37]

Conforme descrevem [37], [62], [63] existem 3 tipos de ações cibernéticas nos Níveis Operacional e Tático que devem ser realizadas desde a situação de Paz e, principalmente, na situação de Guerra por um Estado-Nação [64], [65]:

1. **Ataque Cibernético**: visa destruir, degradar, corromper, negar, interromper as informações, as redes e os sistemas computacionais e de comunicações do oponente/inimigo;

2. **Exploração Cibernética**: visa buscar o dado negado em fontes seguras ou coletar dados em fontes abertas nos sistemas de TIC alvos, a fim de obter a CS do ambiente cibernético; e

3. **Proteção Cibernética**: visa neutralizar ataques e exploração cibernética contra os nossos dispositivos e redes computacionais e de comunicações.

Em resumo, segundo [51] o EB é o responsável pelo desenvolvimento do Setor Cibernético no Brasil e, consequentemente, também é o responsável pelas ações de G Ciber, tanto no nível Operacional, quanto no nível Tático, empregando-as em uma Operação militar para [37]: (i) causar danos, negar o acesso e/ou desestabilizar o Sistema de Comando e Controle (SC^2) do adversário/inimigo no contexto de um planejamento militar de nível operacional ou tático; (ii) tirar proveito das informações coletadas (dados de fontes abertas) ou das informações buscadas (dados de fontes negadas) por meio das diversas formas da Inteligência Militar (Intlg Mil); e (iii) realizar a proteção de seus ativos nos Espaço Cibernéticos próprios (pessoal, material, doutrina, *softwares e hardwares* de TIC, nos quais as informações digitais são produzidas, transitadas, processadas e armazenadas) [63].

No caso do Conselho de Segurança da ONU e de outras leis internacionais reconhecerem o emprego da **G Ciber** de um Estado–Nação como um ataque à soberania de outro Estado–Nação, observa-se que o Direito Internacional de Conflitos Armados (DICA) pode ser aplicado nas diversas formas de Guerras (Guerra Híbrida, Guerra Assimétrica, Guerra da Informação, etc), sintetizadas na denominada Guerra Omnidimensional[14] [49] na Era da Informação [40], segundo os conceitos ***Jus ad Bellum*** (Direito da Guerra) e ***Jus in Bello*** (Direito Internacional Humanitário (DIH)) de acordo com [47], principalmente no Amplo Espectro dos Conflitos [65], [66].

Agora, tanto para as ações estatais realizadas como G Ciber, quanto para ações não estatais realizadas como ataques cibernéticos ou incidentes cibernéticos, ou seja, crimes cibernéticos (espionagem eletrônica, sabotagem cibernética, e sequestro cibernético de dados digitais), seja em tempo de Paz, seja em tempo de Guerra, tais ações cibernéticas de ataque, proteção e exploração da G Ciber geralmente ocorrem no Amplo Espectro de Conflitos [66].

Outro arcabouço legal brasileiro atualmente usado para desencadear ações de Defesa nacional e de Segurança pública é formado pelos seguintes documentos: (i) Constituição da República Federativa do Brasil [61]; (ii) Livro Branco de defesa nacional [67]; (iii) Política Nacional de Defesa [68]; (iv) Estratégia Nacional de Defesa [51]; (v) Lei Complementar nº 97, de 9 de junho de 1999 [69]; e (vi) Doutrina Militar de Defesa [70].

Também podem ser utilizados outros decretos e leis federais em vigor, a fim de permitir a elaboração de novas Diretrizes e novos Planos de Emprego militar das FA nos seguintes níveis [70]: (i) Político (PR); (ii)

[14]Em [49] explica a Guerra Omnidirecional: no nível Tático as operações atuais são realizadas no Amplo Espectro dos Conflitos, conforme nomenclatura estadunidense, mas no nível Estratégico as guerras são cada vez mais Omnidimensionais, ou seja, seguem as direções das 5 Expressões do Poder Nacional (Política, Econômica, Psicossocial, Militar e Científico-tecnológica) e seguem nos tradicionais 6 Domínios dos Campos de Batalhas (Marítimo, Terrestre, Aéreo, Espacial, Cibernético e Eletromagnético). Em resumo, a Guerra Omnidirecional é uma guerra multidimensional aplicada simultaneamente nos espaços físicos e virtuais, com a utilização de todas tecnologias disponíveis, em todos os espaços possíveis.

Estratégico (MD); Operacional (Cmdo Op Atv); e (iv) Tático (F Comp). Todos esses 4 níveis decisórios (Político, Estratégico, Operacional e Tático) estão inter-relacionados, mas não existem limites precisos definidos em lei entre eles [39], conforme demonstra a Figura 1.7 – Principais documentos e os níveis de planejamento da Defesa a seguir.

Nível	Órgão	Principais Documentos
Político	- Presidência da República (PR)	- Diretriz Presidencial de Emprego de Defesa (DPED)
Estratégico	- Ministério da Defesa (MD)	- Dtz Ministerial (DMED) - Dtz do CEMCFA - Planos Estratégicos
Operacional	- Comandos Operacionais ativados	- Dtz de Planejamento Operacional - Planos Operacionais
Tático	- Forças Componentes	- Dtz de Planejamentos Táticos - Ordens de Operações - Planos Táticos

Figura 1.7: Principais documentos e os níveis de planejamento da Defesa [39].

Em [61] o Art. 142 rege que: "As FA compostas pela MB, EB e FAB são destinadas para executarem a defesa da Pátria, à garantia dos Poderes Constitucionais e, por iniciativa de qualquer destes, da lei e da ordem".

Tratando-se do modelo **Sistema 5G Tático EB**, o qual foi empregado na Operação Posse, coordenada pelo MD e COTER, em 1º de janeiro de 2023, na Esplanada dos Ministérios, para estabelecer o C4ISTAR do EB na Região Central do DF, caracteriza-se por um Sistema de Comunicações Tático dual (para uso civil e militar separado ou simultâneo), porque pode ser empregado tanto em Operações militares, quanto em atividades civis. É considerado um sistema flexível e robusto, capaz de ser conduzido por uma dupla de militares até a área de operações definida pelo Ministério da Defesa (MD) e Comando de Operações Terrestres (COTER).

E, ainda, esse modelo de Sistema 5G Tático EB pode ser transportado pela logística militar das FA (MB, EB e FAB) para qualquer localidade brasileira, tanto na Fronteira Terrestre[15] ou metrópole brasileira para realizar a Defesa nacional [51], [65].

Apesar do 5G Tático ter sido empregado diretamente na Operação Posse com caraterística de uma Operação de Não-Guerra, tipo uma Operação Interagências (quando o EB atua junto de demais órgãos federais e estaduais, tais como: PF, PRF, FN, PCDF, PMDF, BMDF, etc) para realizar a segurança presidencial durante o cerimonial da posse na Praça dos Três Poderes, e também nas atividades subsequentes nos Ministério da Justiça e Relações Exteriores, pode-se definir que essa Op Posse 2023 ficou caracterizada como Op de Defesa nacional, já que o MD interditou totalmente espaços públicos no DF, como as águas do Lago Paranoá e também os espaços terrestres e aéreos da região central na Esplanada dos Ministérios, e ainda cerceou alguns direitos e garantias individuais dos indivíduos previstos no Art. 5º da CFRB/1988, empre-

[15]Em [61] descreve a Fronteira Terrestre brasileira: no § 2º, do Art. 20 da CRFB/1988 determina que a faixa terrestre de até 150 Km de largura do limite exterior para o interior do território brasileiro é denominada unicamente como “Faixa de Fronteira”, a qual é considerada fundamental para defesa e segurança nacionais, já que sua ocupação e utilização são reguladas pela própria Carta Magna brasileira. Enquanto que em [71] descreve a Fronteira Terrestre brasileira: é de aproximadamente 15.719 km e detém uma área total de 2.357.850 Km², a qual corresponde a 27,70% do território brasileiro. Essa área deve ser vigiada e protegida diuturnamente sob responsabilidade direta das FA (MB, EB e FAB), segundo regula o Programa de Proteção Integrada de Fronteiras (PPIF), criado pelo Decreto Federal nº 8.903, de 16 de novembro de 2016.

gando fortes esquemas de seguranças das FA, visando à proteção dos presidentes brasileiro e estrangeiros presentes no DF no dia 1º de janeiro de 2023.

Por todo o exposto, parafraseando José Maria da Silva Paranhos Júnior, popularmente conhecido como o Barão do Rio Branco, patrono da diplomacia brasileira [68], conclui-se que: **"Nenhum Estado pode ser pacífico sem ser forte".** (Grifo nosso).

1.2 JUSTIFICATIVAS

Brasil é um importante ator global e líder no Continente Sulamericano devido às suas características: (i) físicas; (ii) sociais; (iii) econômicas; (iv) políticas; (v) científicas; e (vi) militares. Logo, todos os patrimônios nacionais (humano, territorial, biodiversidade, e recursos naturais estratégicos presentes em seus solos e subsolos terrestres e marítimos) devem ser salvaguardados das ameaças externas e internas, por meio de ações preventivas executadas pelos Ministérios das Relações Exteriores (MREx) e da Defesa (MD) galgadas no arcabouço legal supracitado que regula tais ações de Defesa nacional e de Segurança pública.

De acordo com a END cabe ao **Exército Brasileiro** o desenvolvimento, a segurança e a proteção do **Espaço Cibernético Brasileiro** [51], [37].

O **PLANO ESTRATÉGICO DO EXÉRCITO 2020-2023 (PEEx)** é um documento que direciona o escopo dos investimentos dessa Força Armada para o quadriênio 2020-2023, conduzindo o processo de TRANSFORMAÇÃO do Exército rumo à Era do Conhecimento [72].

Dessa forma, o PEEx em seu Objetivo Estratégico do Exército (OEE) 4 – ATUAR NO ESPAÇO CIBERNÉTICO COM LIBERDADE DE AÇÃO DO PLANO ESTRATÉGICO DO EXÉRCITO 2020 – 2023 rege que se deve [72]:

> **4.2.1.8 Adequar**[16] **a estrutura de apoio às atividades de pesquisa científica, tecnológica e de inovação para o setor cibernético do Exército. (2020-2023)** (Grifo nosso)

Finalmente, seguindo a determinação do PEEx, essa pesquisa exerce a apresentação de uma arquitetura conceitual do 5G Tático para ser empregado pelo Exército, em Operações de Defesa nacional, coordenadas pelo MD e COTER.

1.3 METODOLOGIA

Esta é uma pesquisa de natureza aplicada, com abordagem qualitativa, com objetivo exploratório, e procedimento bibliográfico sobre o emprego militar do 5G na Defesa em países estrangeiros e também no Brasil.

Devido o assunto das redes móveis de 5ª Geração estar relacionado a outros assuntos sobre tecnologias

[16] Em [72] Observação: (1) Atividade já iniciada em 2020.

de emprego dual, como a Internet e o Espectro Eletromagnético (EEM), a busca nas fontes foi realizada no universo de publicações analíticas dos anos desde 2010 até 2023, efetivada entre os anos de 2021 a 2023, durante o curso do PPGEE da UnB. Foram pesquisados os termos *"5G in Defense", "5G Dual employment", "5G Military Technologies"*, que reportaram cerca de 10 páginas eletrônicas sobre esses termos.

De acordo com [73] as Fontes da Pesquisa são classificadas em: (i) Primárias; (ii) Secundárias; e (iii) Terciárias. Além disso, na fase de catalogação das Fontes Bibliográficas na Pesquisa Científica para a elaboração da dissertação e tese, consideram-se os seguintes canais de comunicação: (i) Formais; e (ii) Informais. Pode-se considerar que existam os canais semiformais (sendo informais na forma de apresentação, mas formais na divulgação) e os superformais (formais na forma e na apresentação), conforme demonstra a Figura 1.8 – Tipos de Fontes da Informação na Pesquisa Científica a seguir.

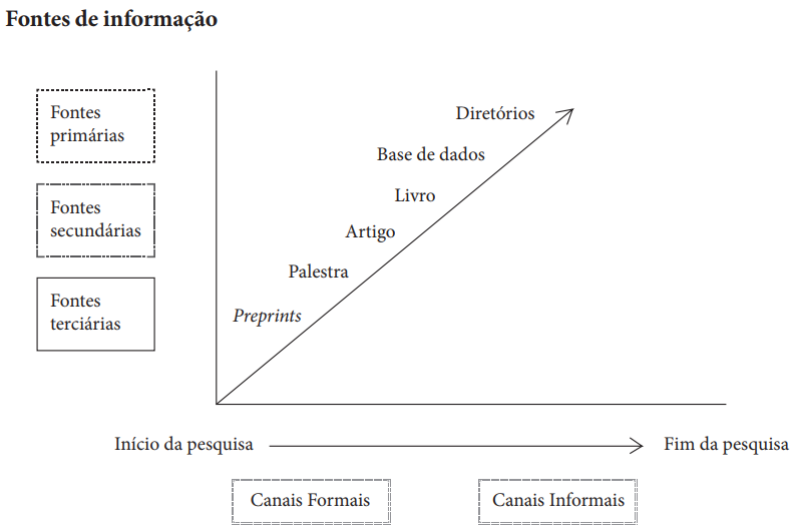

Figura 1.8: Tipos de Fontes da Informação na Pesquisa Científica [73].

Entende-se por canais formais as Fontes Bibliográficas mais conservadoras e de melhor organização e armazenamento: (i) Livros: (ii) Periódicos; (iii) Teses; (iv) Dissertações; (v) Trabalhos publicados em Anais; e (vi) Artigos Científicos. Enquanto que para os canais informais das Fontes Bibliográficas são aqueles que os pesquisadores utilizam para realizar a troca de informações com a comunidade acadêmica e também divulgar os seus trabalhos realizados: (i) Palestras; (ii) Conversas; (iii) Mensagens (e.g. correio eletrônico, *Blogs*, mensagens eletrônicas, SMS, e redes sociais); (iv) Telefonemas; e (iv) Circulação de *preprints*.

A partir das informações da Fig 1.8, estima-se que existem vantagens e desvantagens para o pesquisador em ambos canais: (i) Formais; e (ii) Informais. Normalmente no início da pesquisa são utilizadas as Fontes Terciárias e os canais formais, mas na evolução da pesquisa são acrescidas as Fontes Secundárias e Primárias e usados os canais informais segundo [73].

Foram usadas diversas Fontes de Pesquisa nesta dissertação, a saber: (i) livros e revistas físicas e digitais sobre tecnologias 5G; (ii) artigos científicos digitais publicados (Cafe; *Google Scholar, Web of Science, McPerson, Oasis.Br*; (iii) periódicos digitais (ITU, IEEE, IETS, 5G Americas, GSMA, e Microwave Jour-

nal); (iv) *websites* especializados das empresas de tecnologias participantes do Ecossistema 5G Global (Ericsson, Huawei, Samsung, Rodhe&Schwarz, Nokia, ZTE, Qualcomm, e Vodafone); (vi) *sites* governamentais nacionais e internacionais com matérias sobre o 5G (Anatel, ITU, MCom, MCTI); (vii) *sites* de universidades nacionais (UnB, Unicamp, USP, UFBA, e UFPE) e universidades internacionais (); e (viii) *sites* das FA nacionais (MB, EB, FAB) e FA estrangeiras (Alemanha, China, Coreia do Sul, EUA, França, Inglaterra, Israel, Portugal, Rússia, Suécia, Turquia, entre outras).

Esse trabalho realizou a catalogação e a revisão bibliográfica nas diversas Fontes Primárias, Secundárias e Terciárias, tanto formais, quanto informais, nacionais e internacionais, conforme descritas na Tabela 1.1 – Fontes de Pesquisa usadas nesta dissertação a seguir.

Tabela 1.1: Fontes de Pesquisas usadas nesta dissertação

Tipo da Fonte	**Qnt. Fontes**	**Descrição das Fontes**
Primárias	34	Dados criados pelo Autor da pesquisa corrente sobre estudos publicados de outros autores (e.g. Artigo científico, Palestra, Resumo, Páginas eletrônicas diversas, etc)
Secundárias	77	Dados criados por outros autores e já discutidos entre pares da pesquisa e também já publicados no meio acadêmico sobre estudos de outros autores aceitos ou refutados (e.g. Teses, Dissertações, Artigos Científicos, Revistas Científicas, Páginas eletrônicas oficiais das Universidades, Estudos de Casos, etc)
Terciárias	84	Dados criados por outros autores e já consolidados pelo senso comum acadêmico publicados em diversas fontes (e.g. Livros, Periódicos Científicos, Anais, Guias, Manuais, Páginas eletrônicas oficiais dos governos brasileiro e estrangeiros, etc)

Fonte: [74]

Totalizaram-se 195 fontes referenciadas, as quais foram selecionadas através da leitura inicial de seus resumos e conclusões e, posteriormente, da leitura completa dos seus textos. Algumas foram traduzidos dos idiomas estrangeiros para o idioma português e incluídos neste trabalho com a linguagem e visão deste autor.

1.4 PROBLEMA

O problema nesse estudo foi: **Apresentar uma proposta de arquitetura conceitual de 5G Tático para o Exército empregar na Defesa nacional**.

Esta pesquisa científica está concentrada no campo da **Segurança Cibernética (Seg Ciber)**, conforme regula o Edital nº 8/2020, do PPEE, da UnB. A Seg Ciber é um ramo da Seg Info.

Este estudo buscou levantar as diversas tecnologias derivadas do Ecossistema 5G, propostas pela ITU

em 2015, visando ao emprego militar dos 3 serviços (eMBB, mMTC e URLLC) para a Defesa nacional com o modelo do 5G Tático para estabelecer o **C4ISTAR**[17] (Comando e Controle (C²), Comunicações (Com), Computação (C), Inteligência (I), Vigilância (S), Aquisição de Alvos (TA) e Reconhecimento (R)) em futuras Operações militares coordenadas pelo MD e COTER, desencadeadas no Amplo Espectro dos Conflitos [66].

Comparando-se este estudo com os demais casos correlatos de emprego militar do 5G nas atividades de Defesa dos outros países estrangeiros pesquisados, pode-se observar que este estudo faz diversas referências de publicações da academia internacional, e que é viável a aplicação da arquitetura conceitual proposta do 5G Tático na Defesa e Segurança do Brasil, por causa dos requisitos do 5G muito bem elaborados pela ITU, visando a implementação dos 3 serviços do Ecossistema 5G (eMBB, mMTC e URLLC) no mundo durante a década de 2020 – 2030.

1.5 OBJETIVOS

Nesta seção serão descritos o Objetivo geral e os Objetivos específicos que conduziram o desenvolvimento desta dissertação.

1.5.1 Objetivo Geral

Propor uma arquitetura conceitual de 5G Tático para emprego militar sob domínio do EB, na Defesa e Segurança nacional.

1.5.2 Objetivos Específicos

Para atingir o Objetivo Geral foi necessário atingir cada Objetivo Específico a seguir:

1. Caracterizar sinteticamente os Ecossistema 5G com suas tecnologias derivadas dos 3 serviços disponíveis (eMBB/mMTC/URLLC) atualmente;
2. Apresentar sinteticamente alguns Trabalhos Correlatos sobre o emprego militar do Ecossistema 5G já publicados nas comunidades acadêmicas internacionais e nacional;
3. Apresentar os resultados e discussões do Questionário *on-line* elaborado no ambiente *Google* Formulário, versando sobre o emprego militar do 5G, encaminhado para algumas Organizações Militares (OM) selecionadas no EB;
4. Apresentar uma proposta de arquitetura conceitual de emprego militar do 5G para a Defesa e Segurança nacional, descrevendo suas possibilidades e limitações atuais; e
5. Apresentar as conclusões desta pesquisa e também as sugestões para trabalhos futuros.

[17] Em [43] **C4ISTAR** significa: *Command and Control (C²), Communications (Com), Computing (C), Intelligence (I), Surveillance (S), Target Acquisition (TA), and Reconnaissance (R).*

1.6 PRINCIPAIS CONTRIBUIÇÕES

Este trabalho contribuiu com uma abordagem primária, mas não superficial, das possibilidades e limitações do emprego militar do Ecossistema 5G sob domínio do EB.

Também contribuiu para a confecção do artigo científico denominado "**Emprego dual – civil e militar – do 5G na defesa brasileira: uma proposta para o SISFRON, sob domínio do Exército**"em [75]. Esse artigo foi apresentado em 11 de julho de 2022, na Conferência Internacional Multidisciplinar de Pesquisa Aplicada à Defesa e Segurança de 2022 – MICRADS´22, realizada na Escola Naval de Suboficiais ARC de Barranquila, em Barranquila, na Colômbia [76].

O artigo científico em tela foi publicado na Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI) edição N.º E49, 04/2022, e demonstrou algumas possibilidades do uso dual do 5G na Defesa e Segurança nacional por meio do Sistema de Monitoramento de Fronteiras (SISFRON), sob domínio do EB. O conteúdo da RISTI N.º E49, de 04/2022, pode ser acessado ou realizado o *download* gratuito por meio da página eletrônica disponível em: <http://www.risti.xyz/index.php/pt-pt/edicoes> [77].

Os resultados do Questionário *On-line* serviram de base para um Relatório independente do mestrando, o qual será encaminhado para o Escritório de Projetos do Exército (EPEx), pois versa sobre estudos das possibilidades e limitações do emprego de tecnologias derivadas do Ecossistema 5G para o EB empregar em operações para Defesa nacional.

No Brasil existem 22 instituições científicas e tecnológicas nas FA, orgânicas em cada FS, as quais podem colaborar no desenvolvimento de tecnologias duais derivadas do Ecossistema 5G Brasil [67], além de absorvê-las durante essa década de 2020 – 2030, conforme prevem [22], [12], [78], tais como:

1. **MB**: (i) Centro Tecnológico da Marinha em São Paulo (CTMSP); (ii) Diretoria de Desenvolvimento Nuclear da Marinha (DDNM); (iii) Centro Tecnológico da Marinha no Rio de Janeiro (CTMRJ); (iv) Instituto de Estudos do Mar Almirante Paulo Moreira (IEAPM); (v) Instituto de Pesquisas da Marinha (IPqM); (vi) Centro de Análise de Sistemas Navais (CASNAV); e (vii) Tecnológico da Marinha (DGDNTM);

2. **EB**: (i) Centro Tecnológico do Exército (CTEx); (ii) Centro de Capacitação Física do Exército (CCFEx); (iii) Centro de Avaliações do Exército (CAEx); (iv) Diretoria do Serviço Geográfico (DSG); e (v) Agência de Gestão e Inovação Tecnológica (AGITEC); e

3. **FAB**: (i) Instituto de Aeronáutica e Espaço (IAE); (ii) Instituto de Estudos Avançados (IEAv); (iii) Instituto Pesquisa e Ensaios em Voo (IPEV); (iv) Instituto de Aplicações Operacionais (IAOp); (v) Centro de Lançamento de Alcântara (CLA); (vi) Centro de Lançamento da Barreira do Inferno (CLBI); (vii) Instituto de Controle do Espaço Aéreo (ICEA); (viii) Instituto de Logística da Aeronáutica (ILA); (ix) Instituto de Fomento e Coordenação Industrial (IFI); e (x) Departamento de Ciência e Tecnologia Aeroespacial (DCTA).

Essas instituições realizam pesquisas científicas em diversas áreas de interesse da Defesa brasileira: (i) nuclear; (ii) cibernética; (iii) espacial; (iv) saúde; (v) criptografia/criptoanálise; (vi) comando e controle;

(vii) telecomunicações (satélites e redes); (viii) armamentos e munições; (ix) sistemas de simulação; (x) materiais estratégicos (e.g. nióbio, urânio, terras raras, grafeno, e fibra de carbono).

Estima-se que essa dissertação sirva de base para novos trabalhos acadêmicos de mestrado e doutorado na área da Defesa brasileira. Além de fomento para pesquisas de novas tecnologias relacionadas ao emprego do Ecossistema 5G junto dos projetos dos setores estratégicos das Forças Armadas (FA): (i) MB no Setor Nuclear; (ii) EB no Setor Cibernético; e (iii) FAB no Setor Espacial.

1.7 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em 5 Seções distintas descritas a seguir:

- **1 INTRODUÇÃO**: contextualiza o Problema, descreve o Problema, descreve as Justificativas, descreve os Objetivos Geral e Específicos, descreve as principais contribuições, descreve o tipo da pesquisa científica e suas fontes bibliográficas usadas, e finalmente descreve a organização do trabalho;
- **2 REFERENCIAL TEÓRICO**: descreve as tecnologias derivadas dos 3 serviços do Ecossistema 5G (eMBB/mMTC/URLLC) e também alguns Trabalhos Correlatos do emprego militar do 5G já publicados nos meios acadêmicos internacional e nacional;
- **3 PROPOSTA CONCEITUAL DE EMPREGO MILITAR DO ECOSSISTEMA 5G PARA A DEFESA E SEGURANÇA NACIONAL**: descreve uma proposta conceitual de arquitetura conceitual do 5G para emprego militar pelo EB na Defesa e Sefurança nacional;
- **4 RESULTADOS E DISCUSSÕES**: descreve os resultados do Questionário *On-line* do 5G aplicado aos participantes voluntários de algumas OM do EB e do GSI/PR; e também as possibilidades e limitações do emprego do 5G na Defesa nacional; e
- **5 CONCLUSÕES E TRABALHOS FUTUROS**: descreve as principais observações conclusivas dessa pesquisa científica; e indica sugestões de trabalhos futuros sobre as diversas tecnologias derivadas das comunicações móveis de última geração.

2 REFERENCIAL TEÓRICO

2.1 CONTEXTUALIZAÇÃO

É inegável que a tecnologia 5G está revolucionando o mundo atualmente, pois permite o uso dual – civil e militar – das tecnologias planejadas pela ITU, em 2015, implementadas globalmente, a fim de facilitar ainda mais a vida humana quando comparada às tecnologias legadas do 3G (IMT–2000) e 4G (LTE). Por exemplo:

- 5G Rádio de Acesso à Rede (5G *(Radio Access Network* (5G RAN)) por meio das Redes Definidas por Software (SDN) em multicamadas de Virtualização das Funções de Rede (NFV), sendo que cada camada independente tem potência de transmissão e área de cobertura diferente das demais outras camadas nas Redes Heterogêneas *HetNets*);
- uso do EEM do 5G brasileiro (Bandas: 700 MHz; 2,3 GHz; 3,5 GHz; e 26 GHz) possibilitarão diversas funcionalidades com seus 3 serviços (eMBB, mMTC e URLLC) típicos no emprego tático do 5G para as Comunicações Críticas;
- Melhoraria na eficiência do uso do Espectro Eletromagnético (EEM) licenciado e não-licenciado da ITU, por meio das Ondas centimétricas (10 GHz – 30 GHz) e Ondas Milimétricas (30 GHz – 100 GHz) tanto na esfera civil para fins industriais, comerciais, e sociais, como na esfera militar para fins de Defesa nacional e Segurança pública;
- Comunicações mais rápidas e mais seguras nas Redes Heterogêneas (*HetNets*) com baixas potências nas diversas microcélulas (mini, micro, pico e femto);
- Flexibilidade e Programabilidade com Fatiamento da Rede em Subredes independentes;
- Melhor eficiência energética e de custos das Estações Rádio Bases (ERB) com utilização de Antenas Ortogonais Painéis Planares (64 a 1024 elementos internos) com Máximos Usuários e Máxima Entrad–Máxima Saída (MU-MIMO) e Direcionamento de Feixe Híbrido (usa feixes Mecânicos e Eletrônicos simultâneos) (*Beamforming*);
- (iii) Fábricas/Cidades/Hospitais/Fazendas/Bases Militares Inteligentes automatizadas e robotizadas;
- Lazer com *streaming* de filmes 4K/8K em viagens em veículos ultra rápidos;
- Telemedicina/Telecirurgia remotas;
- Equipamentos de Internet das Coisas (*Internet of Things* (IoT)) e Internet de Tudo (*Internet of Everything* (IoE));
- (vii) Pistas (V2X) e Veículos (V2V) autônomos;
- Uso da Cadeia de Blocos (*Blockchain*) em sistemas criptográficos/decriptográficos;

- Treinamentos com uso das Realidades Virtual (RV) e Aumentada (RA);
- Desenvolvimento de meios de emprego militar vestíveis baseadas na Internet das Coisas de Combate (IoTC);
- Desenvolvimento de novos sistemas de **C4ISTAR** (Comando e Controle (C^2), Comunicações (Com), Computação (C), Inteligência (I), Vigilância (S), Aquisição de Alvos (TA) e Reconhecimento (R)) empregando Inteligência Artificial (IA);
- Uso de *drones* e robôs para busca, salvamento e resgate em áreas de risco de morte humana;
- Uso de Simuladores com Aprendizado de Máquina (*Machine Learning* (ML)) para treinamentos em embarcações, veículos, aeronaves e armamentos de tiro coletivo e individuais; e
- Uso de Redes Não Terrestres, também conhecida como Internet do Espaço [79], composta por Satélites de Comunicações com Órbitas de Baixa Altura (cerca de 500 a 1,5 mil Km de altitude) com cerca de 1 – 200 Gbps e 35 ms de latência, Órbita de Média Altura (cerca de 10 mil Km de altitude) com cerca de 1 – 200 Gbps e 60 ms de latência, Órbita Elipsoidal (cerca de 15 a 25 mil Km de altitude), e Órbita Geossícrona (cerca de 36 mil Km de altitude), todas redes satelitais empregam Ondas Milimétricas do EEM geralmente acima de 24 GHz [80].

Nesta Seção são abordados os principais conceitos doutrinários sobre o Ecossistema 5G a seguir.

2.2 O ECOSSISTEMA 5G

2.2.1 5G Global

Segundo [16] aproximadamente a cada 10 anos um novo padrão global das redes móveis de comunicações sem fio é desenvolvido para atender às demandas crescentes de consumo de dados [15]. Os padrões globais são definidos pela ITU para: (i) alcançar a conectividade onipresente; (ii) garantir a interoperabilidade mundial; e (iii) permitir a harmonização de vários fornecedores e economias de escala.

Em [11] podemos acompanhar a evolução das comunicações móveis desde a geração 1G (1981), 2G (1990), 3G (2001), 4G (2015) até a atual 5G (2020), conforme demonstra a Figura 2.1 – Evolução dos padrões celulares 1G ao 5G a seguir.

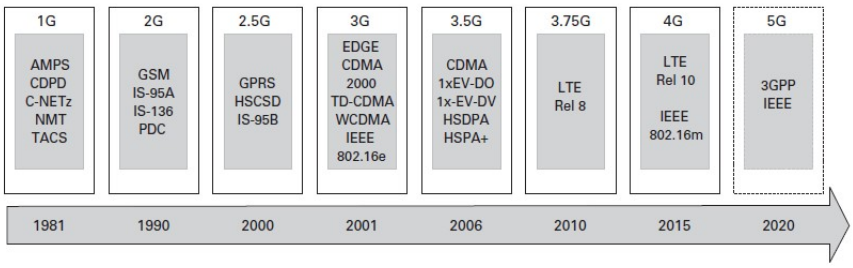

Figura 2.1: Evolução dos padrões celulares 1G ao 5G [11]

Baseado nas informações demonstradas na Figura 2.1 –Evolução dos padrões celulares acima, deduz-se que as tecnologias do **5G** são evoluções planejadas das tecnologias usadas nas gerações anteriores do 1G ao 4G [22].

A ITU apresentou a ***Recommendation ITU-R M.2083-0 (09/2015) IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond***, contendo as tendências das tecnologias para as IMT na Conferência Mundial de Radiocomunicações de 2015 (*World Radiocommunication Conference 2015 (WRC-15)*), em Genebra, na Suíça. Essa recomendação enfatiza especialmente 4 (quatro) áreas-chaves para as Telecomunicações Móveis Internacionais (*International Mobile Telecommunications*) (IMT) [22] : (i) interface(s) de rádio e sua interoperabilidade; (ii) acessar questões relacionadas à rede; (iii) questões relacionadas com o espectro; e (iv) características do tráfego.

Essa Rec ITU-R M.2083-0 (09/2015) ficou conhecida mundialmente como **IMT-2020 e Além** e lançou as bases fundamentais para a implantação do Ecossistema 5G Global conforme [22]. Contém as novas tendências das redes de comunicações móveis designadas a partir de 2015 com as seguintes propostas:

(i) conectar o mundo com uma nova infraestrutura sem fio, promovendo novos aplicativos e serviços profissionais, industriais e de lazer;

(ii) criar um novo mercado de TIC mundial com produtos e serviços especiais;

(iii) acabar com a exclusão digital por meio de redes móveis acessíveis, sustentáveis e fáceis de implantar;

(iv) criar novas formas de comunicação entre os usuários;

(v) criar novas formas de educação por meio de conteúdos digitais baseado em Nuvem, estudos e trabalhos remotos;

(vi) promover a eficiência energética em diversos setores da economia;

(vii) promover mudanças sociais através da conexão e compartilhamento de opiniões públicas rápidas;

(viii) promover nova arte e cultura em apresentações em grupo, coro virtual, co-autoria e co-produção musical; e

(ix) pessoas conectadas podem interagir e criar novas comunidades e culturas próprias.

As **IMT–2020 e Além** seguem os padrões técnicos já estabelecidos pela instituição de engenheiros da *3rd Generation Partnership Project 5G* (5G 3GPP), em tradução literal “3ª Geração de Parceria de Projeto 5G” [15], e segue realizando a padronização global do 5G, a fim de facilitar a implantação do Ecossistema 5G pelo mundo [81].

Em [81] descreve que a *Global System for Mobile Communications Association (GSMA)*, em tradução literal "Sistema Global para Associação de Comunicações Móveis (GSMA)"é uma instituição europeia tipo parceria público-privada formada por mais de 300 (trezentas) empresas globais diretamente ligadas à implantação do 5G no mundo (e.g. fabricantes de celulares e dispositivos móveis, empresas de desenvolvedoras de *software*, fornecedores de equipamentos e empresas de Internet, bem como organizações em setores industriais adjacentes) e representa mais de 800 (oitocentas) operadoras de telefonia móvel no

mundo. A GSMA realiza diversas conferências anuais e *workshops* globais, tais como: *(i) Mobile World Congress; (ii) Mobile World Congress Xangai; (iii) Mobile World Congress Americas; e o (iv) Mobile 360 Series*. Atualmente a GSMA divulgou o Ecossistema 5G Global fundamentado em 3 (três) pilares: (i) alcance; (ii) conectividade para o bem; e (iii) serviços e soluções da indústria [82].

A última atualização para as IMT–2020 e Além foi divulgada pela ITU-R na ***Recommendation ITU-R M.2150-1 (02/2022) Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020 (IMT-2020)***, elaborada pelo Grupo de Estudo 5G (SG 5G) de Genebra, na Suíça [29].

O 3GPP 5G (5GS) detalha as especificações das interfaces do rádio terrestre, incluindo as especificações 5G para seus aspectos não radioelétricos, como os elementos da rede principal (e.g. Rede EPC (*Evolved Pack Core*) e da Rede 5GC (*5G Core*), critérios de segurança, e também de *codecs* para as IMT–2020 e Além [29].

A próxima Conferência Mundial de Radiocomunicações da ITU 2023 (WRC-23) será realizada em Dubai, Emirados Árabes Unidos, no período de 20 de novembro de 2023 a 15 de dezembro de 2023 [83]. Nessa WRC-23 serão divulgadas atualizações de diversas Resoluções sobre o 5G (e.g. a 223 WRC-19, as 171/172/245/246/247/429/661/662/772 WRC-19, a 235 WRC-15, entre outras), e também serão abordados outros temas relacionados às comunicações globais, suas padronizações, estudos e novas tecnologias 6G para melhor aproveitamento e harmonização do EEM.

Das assertivas acima, conclui-se que o modelo das redes móveis sem fio presente nas recomendações técnicas da **IMT–2020 e Além** foi validado mundialmente pelo 5GS como o padrão das novas redes móveis sem fio de 5ª Geração desenvolvidas para a década de 2020–2030 [12], conforme estabelecido na *Working Radio Conference 2019 (WRC19)* da ITU-R, realizada de forma remota (*On-line*) em 9 de julho de 2020, devido ao isolamento social obrigatório imposto durante a pandemia global de COVID-19 [84].

Por fim, de acordo com [21] a evolução do 5G Puro (2015), passará pelo 5G e Além (B5G) (2025) até chegar ao 6G (2028), pois foram previstos os seguintes calendários de implantação:

- **Fase 1 do 5G**: de 2015 a 2020, apresentado na WRC-15 ficou conhecida como simplesmente 5G, com o espectro distribuído abaixo dos 6 GHz [12], [22];
- **Fase 2 do 5G**: de 2020 até 2030, provavelmente, com o espectro distribuído acima dos 6 GHz recentemente recentemente atribuído na Conferência Mundial das Radiocomunicações de 2019 (WRC-19), normalmente designada por B5G [12], [85]; e
- **Fase 2 pós-5G**: de 2028 para além de 2030, em direção ao 6G, caso tenha normalização [12], [79], [86].

2.2.2 Ecossistema 5G Global e os três casos de emprego previstos na IMT–2020 e Além

Desde o ano de 2012, estudos da ITU-R revelaram as tecnologias e serviços derivados do Ecossistema 5G Global, cujos requisitos estão previstos na **IMT–2020 e Além** lançada em 2015 [22].

As "Tecnologias Chaves"[11] ou "Tecnologias Avançadas"[16] do 5G propiciam uma gama de aplica-

ções variadas, com impactos diretos na vida das pessoas, causados por meio dos 3 serviços planejados para as denominadas Redes Futuras (*Future Nets (FN)*) [16] citados a seguir:

1. **Banda Larga Móvel aprimorada** (*enhanced Mobile Broadband* (eMBB)) [12], [13], [21], [22], [18], e outros autores a denominaram como **Banda Larga Móvel extrema** (*extreme Mobile Broadband* (xMBB)) [11], **Banda Larga Móvel ultra** (uMBB) [15] e somente como **Mobile BroadBand** (MBB²) [17];
2. **Comunicação Tipo Máquina massiva** (*massive Machine Type Communication* (mMTC)) [11], [12], [13], [21], [22], [18]; e
3. **Comunicação Ultra-Confiável de Baixa Latência** (*Ultra-Reliable Low Latency Communication* (URLLC)) [12], [13], [21], [22], [17], [18], e também denominada **Comunicação Tipo Máquina Ultra-confiável** (*Ultra-reliable Machine-Type Communication* (uMTC)).

De acordo com [11] e [15] estimam que o 5G fornecerá uma ampla variedade de aplicações de comunicações de voz e de Internet móvel para diversos dispositivos e equipamentos, conforme demonstra a Figura 2.2 – Os três casos de uso do 5G NR previstos pela IMT–2020 e Além [22] a seguir.

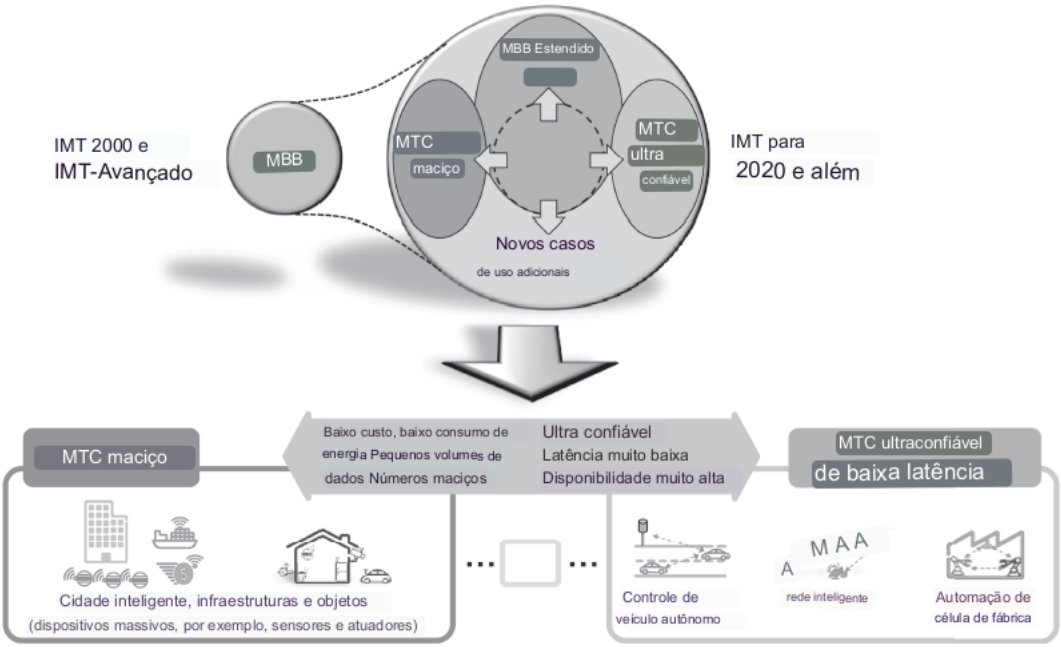

Figura 2.2: Os três casos de uso do 5G previstos pela IMT-2020 [11]

A partir da análise das informações da Figura 2.2 e dos estudos do 5G nas *Recommendation ITU-R M.2083-0 (09/2015)* [22] e *Recomendación UIT-R M.2150-1 (02/2022)* [29], está descrita uma síntese dos 3 casos e os princípios de emprego do 5G NR [18] a seguir:

1. **Banda Larga Móvel aprimorada (eMBB)** [22] – é mais preparada para realizar a comunicação entre seres humanos, porque fornece uma experiência mais uniforme na área de cobertura e degradação de desempenho suave do sinal rádio à medida que o número de usuários simultâneos aumenta [11].

Também suportará comunicação confiável para Segurança Nacional e Segurança Pública já que dispõe de ampla cobertura, baixa latência e extremas taxas de dados velozes [11]. Por exemplo:

(i) **eMBB *Hotspot* Interna** (*Indoor Hotspot eMBB*) [29] – é usada para conectar muitos usuários estacionários e/ou usuários pedestres em ambiente interno isolado, como escritórios, *shopping centers*, estádios de esportes com densidade muito alta de usuários em [18];

(ii) **eMBB Densa Urbana** (*Dense Urban eMBB*) [29] – é usada para conectar muitos usuários em ambiente urbano com alta densidade de usuários e de cargas de tráfego com foco em veículos e pedestres usuários em [18]; e

(iii) **eMBB Rural** (*Rural eMBB*) [29] – é usada para conectar muitos usuários em ambiente rural com cobertura de área ampla e contínua, para atender muitos usuários, pedestres usuários, veículos comuns e veículos de alta velocidade [18].

2. **Comunicação Tipo Máquina massiva (mMTC)** – é mais preparada para realizar a comunicação entre máquinas (M2M) ou comunicação entre dispositivos (D2D) presentes na Internet das Coisas (IoT), visando baixo consumo de energia elétrica e altas capacidades de baterias, porque fornece uma experiência mais uniforme na área de conectividade sem fio para dezenas de bilhões de dispositivos habilitados na Internet, conectividade escalável para aumentar o número de dispositivos por Km², transmissão eficiente de pequenas cargas úteis, ampla cobertura de área e penetração profunda são priorizadas sobre taxas de dados [11].

   Por exemplo: **mMTC Macro Urbana** (*Urban Macro mMTC*) [29] se deseja um macroambiente urbano com cobertura contínua com foco em um alto número de dispositivos do tipo máquina conectados em áreas inteligentes (cidades, fábricas, hospitais, prédios, escolas e casas)[18].

3. **Comunicação Ultra-Confiável de Baixa Latência (URLLC)** – é mais preparada para realizar a comunicação entre dispositivos (D2D) fornecendo enlace de comunicação em tempo real ultraconfiável, de baixíssima latência e alta disponibilidade [11]. Por exemplo: **URLLC Macro Urbana** (*Urban Macro-URLLC*) [29] se deseja um macroambiente urbano voltado para comunicação ultraconfiável, disponível e de baixíssima latência [18]. Ou seja, URLCC é destinada para serviços de rede com requisitos extremos, é para aplicativos que incluem: (i) transporte inteligente; (ii) automação industrial com robótica; (iii) veículos autônomos; (iv) entregas autônomas por *drones*; (v) telecirurgia remota; e (vi) Internet Tátil [87].

Enfim, em [88] foi analisado o uso do 5G Futuro e os impactos nas Indústrias e na Sociedade publicado no ano de 2020: (i) 93% dos casos de Comunicação Ultra Confiável de Baixa Latência (URLLC); (ii) 78% dos casos de Banda Larga Móvel aprimorada (eMBB); e (iii) 45% dos casos de Comunicação Tipo Máquina massiva (mMTC).

2.2.3 Ecossistema 5G Global e os requisitos previstos na IMT–2020 e Além

No ano de 2015 foi publicada a Resolução ITU-R 65, a qual versava sobre os "**Princípios para o processo de desenvolvimento futuro das IMT para 2020 e mais além**"e direcionava os critérios para o processo de desenvolvimento das Recomendações e Relatórios para as **IMT–2020 e Além**, incluíram-se

as recomendações para as especificações da interface aérea do novo rádio denominado 5G NR (*5G New Radio*) [16].

As **IMT–2020 e Além** divulgaram os requisitos iniciais das principais tecnologias futuras das redes de comunicações sem fio 5G NR [18]. No entanto, estudos recentes de diversos fabricantes e vendedores internacionais possibilitaram organizar os parâmetros dos **Indicadores Chaves de Desempenho** (*Key Performance Indicator* (KPI)) em termos temporais faseados com prazos [89]: (i) Curto prazo (2022) (SEVO); (ii) Médio prazo (2025) (MEVO); e (iii) Longo prazo (2030) (LEVO).

A Figura 2.3 – Requisitos das redes 5G com Evoluções de Curto (5G SEVO), Médio (5G MEVO) e Longo (5G LEVO) prazos demonstra os requisitos propostos pela ITU a seguir, enquanto que a Tabela 2.1 – Alvos dos Indicadores Chaves de Desempenho (KPI) nas evoluções de Curto, Médio, e Longo prazos do 5G NR descreve esses requisitos chaves a seguir.

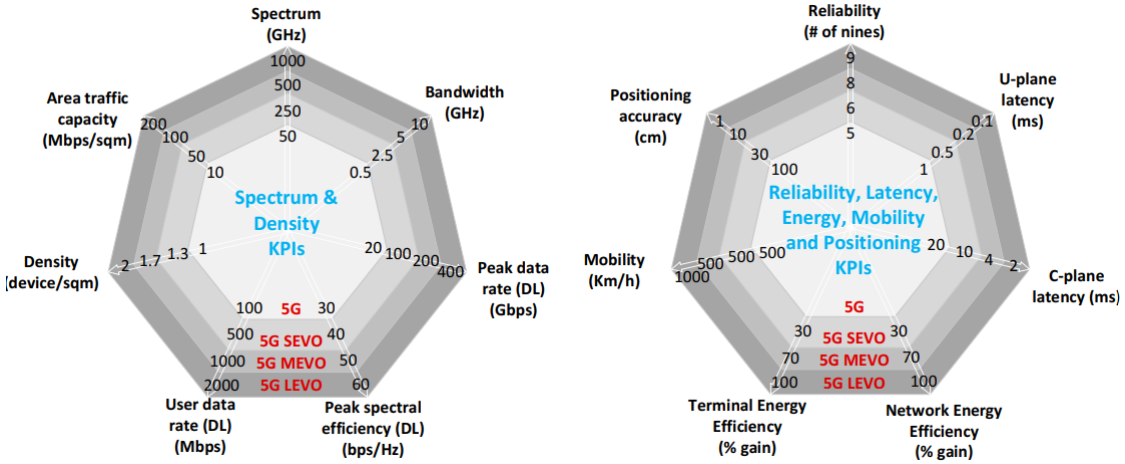

Figura 2.3: Requisitos das redes 5G com Evoluções de Curto (5G SEVO), Médio (5G MEVO) e Longo (5G LEVO) prazos [89]

A partir das análises das informações da Figura 2.3 acima e da Tabela 2.1 abaixo, pode-se inferir que esses Indicadores Chaves de Desempenho (KPI) são fundamentais para que os fabricantes e vendedores padronizem seus equipamentos do Ecossistema 5G. Esses parâmetros possibilitam a implantação global por esses motivos: (i) aumentar o alcance e acesso dessas tecnologias em diversos países simultaneamente; (ii) diminuir os custos na produção, instalação e intercomunicação de equipamentos de fabricantes distintos; e (iii) facilitar o controle e auditoria do EEM pela ITU-R nos países.

2.2.4 Ecossistema 5G Global e suas faixas do Espectro Eletromagnético

Em [12] descreve que as redes 5G trouxeram inovação com base no uso das faixas de micro-ondas de rádio frequência (RF) nas faixas desde as Ondas centimétricas (3 GHz – 30 GHz) até as Ondas milimétricas (30 GHz – 300 GHz), com seus correspondentes comprimentos de onda [13], conforme demonstra a Figura 2.4 – Faixas do EEM com Micro-ondas centimétricas e milimétricas usadas no Ecossistema 5G abaixo.

Tabela 2.1: Alvos dos Indicadores Chaves de Desempenho (KPI) nas Evoluções de Curto (5G SEVO), Médio (5G MEVO) e Longo (5G LEVO) prazos do 5G NR

Alvos KPI	**Alvos 5G**	**Alvos 5G SEVO**	**Alvos 5G MEVO**	**Alvos 5G LEVO**
Espectro	< 52.6 GHz	< 250 GHz	< 500 GHz	< 1.000 GHz
Largura de Banda	< 0.5 GHz	< 2.5 GHz	< 5 GHz	< 10 GHz
Taxa de Dados de Pico	> 20 Gbps; UL: > 10 Gbps	DL: > 100 Gbps; UL: > 50 Gbps	DL: > 200 Gbps; UL: > 100 Gbps	DL: > 400 Gbps; UL: > 200 Gbps
Taxa de Dados de Usuário	DL: > 100 Mbps; UL: > 50 Mbps	DL: > 500 Mbps; UL: > 250 Mbps	DL: > 1 Gbps; UL: > 0.5 Gbps	DL: > 2 Gbps; UL: > 1 Gbps
Densidade	> 1 device/sqm	> 1.3 device/sqm	> 1.7 device/sqm	> 2 device/sqm
Capacidade de Área de Tráfego	> 10 Mbps/sqm	> 50 Mbps/sqm	> 100 Mbps/sqm	> 200 Mbps/sqm
Confiabilidade URLLC	> 5 nonos	> 6 nonos	> 8 nonos	> 9 nonos
Plano de Latência-U URLLC	< 1 ms	< 0.5 ms	< 0.2 ms	< 0.1 ms
Plano de Latência-C URLLC	< 20 ms	< 10 ms	< 4 ms	< 2 ms
Eficiência Energética da Rede	Qualitativo	> 30% ganho	> 70% ganho	> 100% ganho
Eficiência Energética do Terminal	Qualitativo	> 30% ganho	> 70% ganho	> 100% ganho
Mobilidade	< 500 Km/h	< 500 Km/h	< 500 Km/h	< 1.000 Km/h
Precisão de posicionamento	NA (< 1 m)	< 0.3 m	< 0.10 m	< 1 cm

Fonte: Adaptado do Artigo Científico [89]

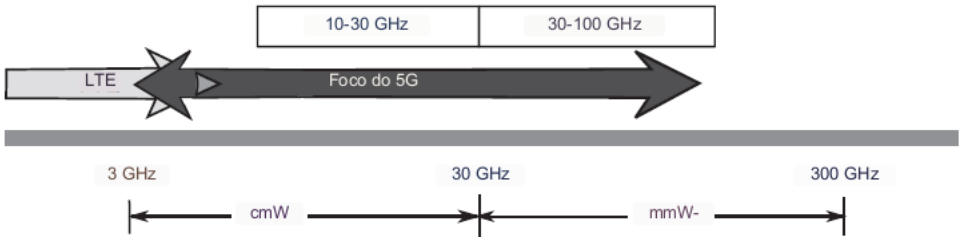

Figura 2.4: Faixas do EEM com Micro-ondas centimétricas e milimétricas usadas no Ecossistema 5G [11]

As faixas do EEM destinadas para o Ecossistema 5G Global foram definidas pela ITU-R nas **IMT–2020 e Além** e estão descritas conforme a Tabela 2.2 – Informações do Espectro Eletromagnético do Ecossistema 5G Global a seguir.

Tabela 2.2: Informações do Espectro Eletromagnético do Ecossistema 5G Global

Nomenclatura	**Frequência**	**Comprimento de onda**	**Identificação métrica**	**Denominação oficial**
Ultra Alta Frequência (UHF)	300 MHz – 3 GHz	1 m – 10 cm	Decimétricas	Micro-ondas
Super Alta Frequência (SHF)	3 – 30 GHz	10 cm – 1 cm	Centimétricas	Micro-ondas
Extremamente Alta Frequência (EHF)	30 – 300 GHz	1 cm – 1 mm	Milimétricas	Micro-ondas

Fonte: [90]

No ano de 2018, o Projeto de Parceria de Terceira Geração (3GPP) (*3rd Generation Partnership Project*) 3GPPP 5G (5GS) publicou o "**Guia Rota para 5G: Introdução e Migração**"(*ROAD TO 5G: INTRODUCTION AND MIGRATION*) [81], no qual definiu as faixas de frequências do EEM para uso dos 3 (três) serviços no 5G, cada um com suas características de capacidade, cobertura e emprego: (i) **infra** 1 GHz; (ii) **inter** 1 GHz – 6 GHz; e (i) **supra** 6 GHz. A Figura 2.5 – Capacidade, cobertura e local de emprego do 5GS demonstra os 3 usos previstos pelo 5GS a seguir.

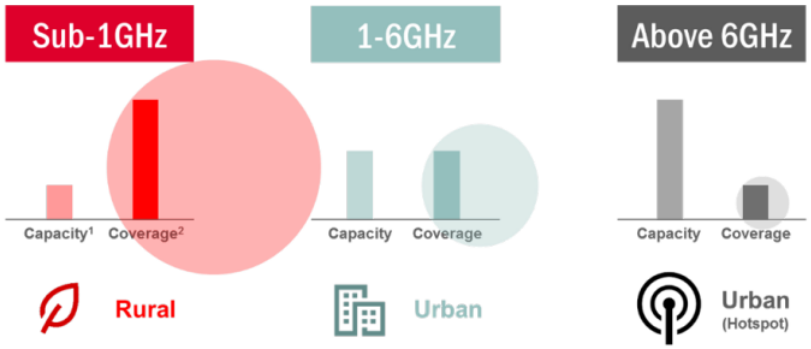

Figura 2.5: Capacidade, cobertura e local de emprego do 5G 3GPP [81].

Das assertivas acima e da análise da Figura 2.5, pode-se observar que as frequências das ondas mili-

métricas usadas terão o efeito esperado para cada caso de uso planejado:

(i) sub 6 GHz [81]: as faixas de frequências abaixo de 1 GHz (e.g. 600 – 800 MHz) propiciam pequenas capacidades de utilização de equipamentos usuários simultâneos, mas grandes áreas de coberturas quando comparadas às outras duas bandas de frequências, sendo ideal para emprego rural e semi-urbano, como na eMBB;

(ii) intra 6 GHz [81]: as faixas de frequências médias entre 1 – 6 GHz (e.g. 2.300 – 2.399 MHz e 3.400 – 3.800 MHz) propiciam médias capacidades de utilização de equipamentos usuários simultâneos e médias áreas de coberturas, sendo ideal para emprego urbano em áreas abertas, como na mMTC (*outdoors*); e

(iii) supra 6 GHz [81]: as faixas de frequências acima de 6 GHz (e.g. 24 – 28 GHz e 50 – 87 GHz) propiciam grandes capacidades de utilização de equipamentos usuários simultâneos, mas pequenas áreas de coberturas, sendo ideais para empregos urbanos em células pequenas (micro, pico e femto) em ambientes fechados (*indoor*), como na URLCC.

2.2.5 Ecossistema 5G Global e suas tecnologias avançadas e futuras

De acordo com [22] e [13] foram estabelecidos rigorosos requisitos para a implantação do 5G global, e diversas tecnologias candidatas foram amplamente discutidas. Em [13] o desenvolvimento das tecnologias do Ecossistema 5G Global ocorre tanto no Rádio de Acesso à Rede (RAN) e na própria Rede Principal 5G (5G Core Network), quanto no sistema fim–a–fim (*end-to-end*), conforme demonstra a Tabela 2.3 – Principais requerimentos e tecnologias candidatas ao 5G a seguir.

Tabela 2.3: Principais requerimentos e tecnologias candidatas ao 5G

Requerimentos do 5G	**Tecnologias candidatas ao 5G**
Alta taxa de dados	Ondas milimétricas, MIMO Massivo, Pequenas células
Latência Ultrabaixa	Borda Móvel/Computação em Nuvem, D2D
Conectividade Massiva Maciça	MIMO, D2D, M2M, Pequenas Células
Confiabilidade e Alta Disponibilidade	Cloud-RAN, SDN, NFV, MANO, Computação em Nuvem
Flexibilidade e Programabilidade	*Cloud-RAN*, SDN, NFV, Fatiamento de Rede (SN), MANO
Eficiência Energética e de Custos	*Cloud-RAN*, SDN, NFV, Fatiamento de Rede (SN), MANO
Eficiência de Espectro	MIMO Massivo, Pequenas células, D2D
Segurança e Privacidade	Centralizar os elementos de controle, Controlar o SDN e *Switchs*, Controlar as Interfaces Aéreas Abertas, Controlar os Canais, Controlar os Canais Encriptados, Localização de Assinante, Identificação de Assinante

Fonte: Adaptado do livro [13]

Segundo [91] no Ecossistema 5G foi possível melhorar a eficiência do EEM já usado no 4G Core do *Evolved Packet Core* (EPC) por meio do Compartilhamento Dinâmico do Espectro (*Dinamic Spectrum*

Sharing (DSS)) no 5GC (5G *Core*). Dessa forma o *5G New Radio* (5G NR) reaproveita as bandas de frequências de 410 MHz até 7,125 GHz já utilizadas no 4G LTE *(Long Term Evolution)* para estabelecer novas conexões de usuários móveis nas Redes Heterogêneas disponíveis no 5GC [81].

Isso gera uma economia de custos financeiros e de processamento de dados nas ERB com o reaproveitamento de frequências importantes com *Backhaul*, pois antes do DSS no 4G LTE eram removidas algumas bandas de frequências selecionadas para que o Rádio 5G NR pudesse ser instalado na mesma torre ou no mesmo sítio de antenas do 4G LTE [91].

2.2.6 Ecossistema 5G Global e seu emprego na Pandemia da COVID-19

Conforme publicado na Pesquisa de Trabalhos Futuros 2020 (*Future Jobs Survey 2020*) o ano de 2020 ficou marcado pela intensa crise de saúde mundial causada pela pandemia da doença infecto-contagiosa do sistema respiratório denominada COVID-19 [92].

O vírus SARS-CoV-2, causador da doença COVID-19, ficou mais conhecido como Coronavírus [92]. Ele surgiu na China durante as atividades dos VII Jogos Mundiais Militares, em 2019, na cidade de Wuhan, capital da província de Hubei, megalópole com mais de 11 milhões habitantes, considerada uma importante base industrial, científica, educacional e tecnológica da China [93].

Suspeita-se que esse Coronavírus pode ter sido conduzido para todos os 5 continentes após a realização dos VII Jogos Mundiais Militares, celebrados em prol da Paz mundial, ocorridos entre os dias 18 e 27 de outubro de 2019, onde participaram cerca de 10 mil atletas militares que retornaram aos mais de cem países de origem [94].

Participaram cerca de 10 mil atletas de mais de cem países, que partiram para os seus países de origem através das 63 rotas aéreas internacionais e domésticas, pois era a única cidade na China central a ter voos diretos para os 5 continentes (Americano, Africano, Asiático, Europeu e Oceania) e dispunha de extensa rede de transporte urbano com 334 Km de linhas de metrô e 225 estações em operação [93].

A China somente notificou a Organização Mundial de Saúde (OMS) sobre o novo Coronavírus, surgido em Wuhan, somente em dezembro de 2019. E a OMS decretou a doença COVID-19 como Emergência de Saúde Pública de Interesse Internacional (*Public Health Emergency of International Concern – PHEIC)* em 31 de janeiro de 2020 [92].

O Coronavírus se espalhou rapidamente por todos os 5 continentes e contaminou milhões de pessoas, muitas destas acabaram levadas para hospitais e realizaram tratamentos em Unidades de Terapia Intensivas (UTI) e muitas outras acabaram falecidas com a COVID-19. Assim, diversos Governos tomaram medidas drásticas para a conter a doença em seus territórios fecharam suas fronteiras e passaram a controlar as viagens externas e internas [95].

As pessoas foram obrigadas a permanecerem em suas casas, cumprindo rigoroso isolamento social sem entender realmente o que ocorreria com os doentes infectados e com suas economias financeiras. As autoridades sanitárias orientaram as pessoas para: (i) aumentarem a higiene pessoal em lavar as mãos regularmente; (ii) usar lenços de papel ao tossir/espirrar e descartar o lenço diretamente em uma lixeira; (iii) usar proteção pessoal tipo máscara cirúrgica e visor em público; (iv) manter distância social de no mínimo

2 m e evitar o contato humano; (v) realizar auto-isolamento doméstico de uma pessoa suspeita/infectada pelo COVID-19; e (vi) procurar tratamento médico quando apresentar sintomas da COVID-19 [92].

Exemplos de locais e atividades suspensas durante a pandemia de COVID-19: (i) fronteiras; (ii) comércios; (iii) universidades, faculdades e escolas; (iv) locais de entretenimento (*shows*, teatros, cinemas, restaurantes, lanchonetes, *lanhouses*); (v) locais de lazer (clubes, parques, praias e reservas ambientais); entre outros locais. Essa crise da pandemia de COVID-19 exacerbou ainda mais as diferenças sócio-econômicas entre as pessoas e também entre os países, que tiveram que superar a crise mais rapidamente com a produção de vacinas sem muitos testes e realizando uma imunização em massa da população [84].

No entanto, a pandemia de COVID-19 conduziu as pessoas, as empresas e os Governos a adotarem o uso da Internet como meio de comunicação primário. Realmente o acesso à Internet via redes móveis de comunicação celular permitiu a continuidade dos trabalhos e dos estudos remotamente durante os períodos de distanciamento social, quarentena e confinamento obrigatórios, veiculados como soluções eficazes pela Organização Mundial de Saúde (OMS) [84].

Demais Governos, inclusive o governo brasileiro, a fim de diminuir o contágio da doença e também para diminuir as chances de internações graves em Unidades de Terapia Intensiva (UTI) e as chances de mortes, apesar de 80% dos casos terem sintomas são leves como um resfriado ou gripe mais leve, porém alguns casos evoluíram para outras formas mais graves da doença com complicações cardíacas onde 16,7% desenvolveram arritmia e 7,2% apresentaram lesão cardíaca aguda em estudos na Itália [96].

Hoje, verifica-se que o distanciamento social, o confinamento e a quarentena impostos pelos governantes mundiais, foram ineficazes contra a disseminação e o contágio dessa doença mundial. Foram infectadas 765,2 milhões de pessoas com COVID-19 até o dia 5 de março de 2023 e registradas quase 7 milhões de óbitos no mundo. Ainda de acordo com a OMS cerca de 13,3 bilhões de doses de vacinas foram administradas em todo o mundo contra o Coronavírus [97].

De acordo com [95] no artigo publicado *"The role of 5G for digital healthcare against COVID-19 pandemic: Opportunities and challenges"* o Ecossistema 5G demonstrou boas performances nos 3 casos de uso previstos na IMT–2020 e Além (eMBB, mMTC e URLLC) no estudo de caso de um realizado em julho de 2020, Hospital situado na Coreia do Sul, pelo Instituto Coreano de Ciências da Comunicação e Informação (KICS).

Apesar dos desafios financeiros, dos cuidados de saúde para evitar a infecção do Coronavirus pelas equipes do hospital, a implantação da telesaúde com o 5G durante a pandemia de COVID-19 demonstrou bons resultados [95], desde a aquisição dos insumos (álcool em gel, luvas e máscaras cirúrgicas, medicamentos, vacinas, etc), passando pelas consultas com testes rápidos de COVID-19, pelos tratamentos mais simples e tratamentos mais complexos com UTI e/ou telecirurgia, até o monitoramento remoto dos pacientes curados em suas residências, conforme demonstra a Figura 2.6 – Uma visão geral da implantação do 5G para telessaúde em um hospital da Coreia do Sul abaixo.

Este estudo foi publicado na revista eletrônica denominada Tecnologia da Informação e Comunicações Expresso[1] com o título: **O papel do 5G para a saúde digital contra a pandemia de COVID-19: Opor-**

[1]Em [95] a *Information & Communications Technology Express*), Volume 7 de março de 2021 está disponível para leitura ou *dowload* na página eletrônica da url: <https://www.sciencedirect.com/journal/ict-express/vol/7/issue/1.>

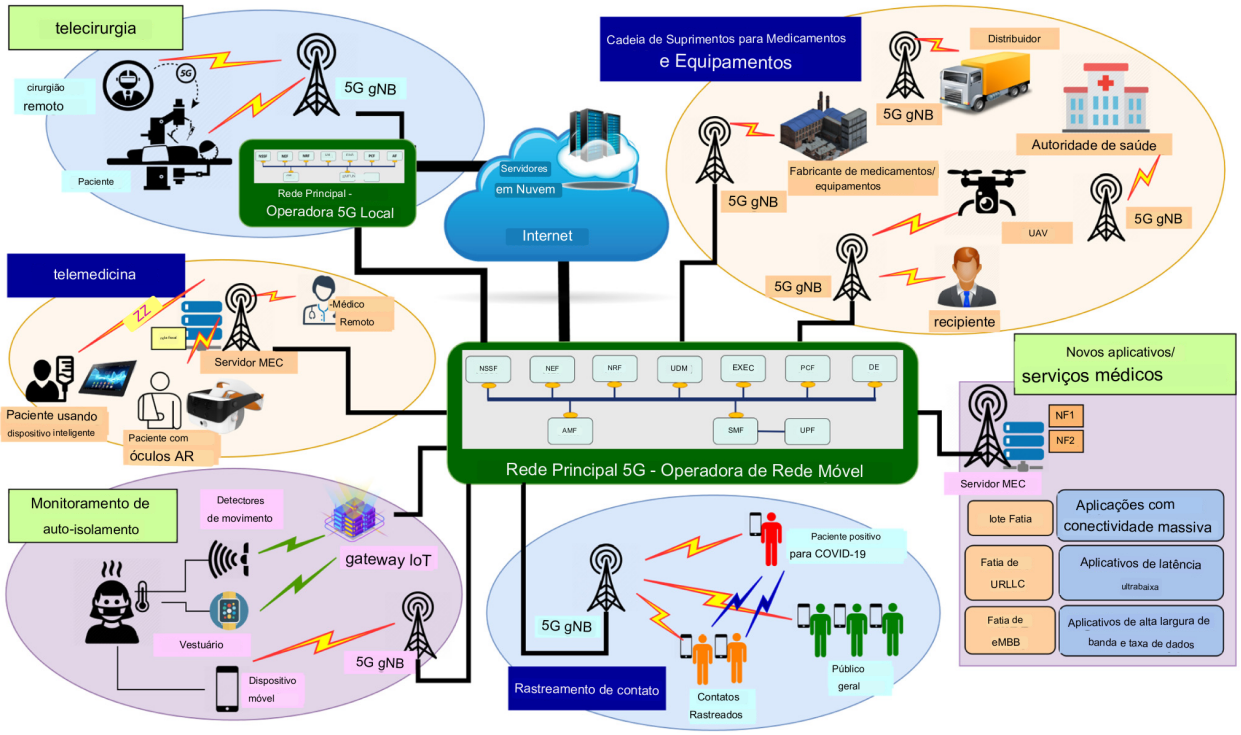

Figura 2.6: Uma visão geral da implantação do 5G para telessaúde em um hospital da Coreia do Sul [95].

tunidades e desafios (*The role of 5G for digital healthcare against COVID-19 pandemic: Opportunities and challenges*); e trouxe uma visão mais clara da aplicação das tecnologias futuras do 5G em um ambiente caótico de saúde e segurança pública durante a pandemia do Coronavírus entre 2020 e 2023.

Das assertivas acima e da Figura 2.6, infere-se que os setores de saúde dos países foram os primeiros a receber pessoas doentes afetadas pela propagação rápida da doença COVID-19, e os enfermeiros e médicos enfrentaram inúmeros desafios. Como os países asiáticos já possuem mecanismos de controle para minimizar a disseminação da COVID-19, eles estão reabrindo suas economias mais cedo para que o público possa retomar suas estilo de vida normal, já que estão controladas as pessoas infectadas.

Para prevenir qualquer ressurgimento da doença, setores de saúde de cada país estão equipados adequadamente com novas soluções para enfrentar quaisquer desafios emergentes de forma eficaz, pois refizeram seus estoques de medicamentos e insumos (esparadrapos, agulhas, luvas, máscaras, algodão, álcool em gel, medicamentos e vacinas) na forma de pedidos *On-line* via 5G. E também estão realizando o acompanhamento cerrado (*Contact Tracing*) dos pacientes doentes e após a alta hospitalar em suas residências por meio de aplicativos interligados via tecnologias e serviços do 5G.

Para isso, as tecnologias 5G são cruciais, utilizando ondas milimétricas em altas frequências do EEM, com Estações Base de células pequenas podem fornecer melhor conectividade, incluindo-as no interior de ambientes fechados (*in door*) conectadas ao aparelho celular tipo sem visada direta (NLOS). O serviço de **URLLC** entrega uma oferta eficaz de rede ultra segura com baixíssima latência para a Telecirurgia robótica e para a Telemedicina (exames e consultas) por meio de videoconferência, Realidade Aumentada (RA) e Realidade Virtual (RV) no hospital.

Enquanto que o MU-MIMO massivo combinado com a com propagação dos feixes direcionais (*Be-*

amforming) das Antenas Ortogonais Painéis Planas e multiplexação tipo Acesso Múltiplo por Divisão de Frequência Ortogonal (*Orthogonal Frequency-Division Multiple Access* (OFDMA)) atendem um grande número de dispositivos/usuários IoT via 5G com altas taxas de dados, garantidas pelo serviço de **mMTC** na Cadeia de Suprimento e no controle automatizado de pedidos/estoques, e também nas entregas realizadas por *drones* e carros autônomos (V2X) [95].

O serviço **eMBB** pode oferecer grandes coberturas em áreas abertas e também fechadas do hospital. Com ótimas taxas de dados é possível o paciente isolado ser monitorado em tempo real, é possível o paciente assistir um filme 4K em *streamming* ou *on-demand* da sua maca digital com tela *FullHD* ou passear com a sua cadeira de rodas inteligente pelo jardim ou pátio do hospital conectado ao sistema de segurança e geolocalização do hospital. Ainda os enfermeiros e médicos podem contar com o apoio presencial de robôs colaborativos atendendo às pessoas na recepção, nos corredores e no restaurante do hospital.

Assim, soluções desenvolvidas com tecnologias 5G podem atendem a vários casos de uso relacionados à saúde, como: (i) acompanhamento dos doentes no hospital e dos curados em casa; (ii) telemedicina; (iii) telecirurgia; (iv) gerenciamento da cadeia de suprimentos; (v) rastreamento de contatos e implantações rápidas de serviços de saúde.

No entanto, uma ampla gama de desafios de implementação, como privacidade e segurança dos dados sensíveis, escalabilidade, e questões sociais devem ser abordadas antes do país implantar os 3 serviços do 5G (eMBB, mMTC e URLLC) com funcionalidades completas nos hospitais e clínicas de saúde. É necessária a regulamentação legal interna do 5G no país para isso.

Segundo [98] destaca que a pandemia de COVID-19 confirmou a necessidade primordial dos serviços de telecomunicações no cotidiano dos cidadãos e empresas no mundo. Serviços financeiros, telemedicina, ensino a distância, e sessões de trabalho remoto somente se tornaram possíveis e se massificaram com o uso da tecnologia da Internet, tanto utilizada via cabeada, quanto utilizada via redes móveis celulares.

De acordo com a [97] em 05/05/2023 a OMS declarou o fim da pandemia de COVID-19 com 765,2 milhões de casos de COVID-19 confirmados no mundo até o momento, e aproximadamente 7 milhões de mortes registradas pela doença no mundo.

No Brasil ocorreram 37.449.418 casos de infectados acumulados (17,82% considerando a população de 210.147.125 habitantes), foram 701.494 casos de óbitos acumulados (0,33% considerando a população de 210.147.125 habitantes) e a taxa de mortalidade de 3,33% (333,8 para 100 mil habitantes) até 26/04/2023 [99].

Ainda de acordo com a OMS, cerca de 13,3 bilhões de doses de vacinas contra a doença foram administradas em todo o mundo [97]. E segundo [84], [100] as tecnologias derivadas do 5G ajudaram o Brasil e o mundo a superarem as dificuldades de comunicações durante a pandemia de COVID-19 vivenciada entre os anos de 2020 a 2023.

Finalmente [97] informou o fim da pandemia global de Coronavívus em 5 de março de 2023. O Relatório Global de Conectividade de 2022, elaborado pela ITU-D, informa que a pandemia global de COVID-19 causou uma enorme crise econômica mundial e crise social com milhões de mortes como fatores negativos, porém como fator positivo causou uma resiliência para futuras crises com a aceleração

da implantação do Ecossistema 5G Global, onde 437 operadores adotaram o 5G em 137 países durante o período da pandemia (2020-2022) [83].

2.2.7 Ecossistema 5G Global e suas evoluções previstas

A ITU-R emitiu a ***Recommendation ITU-T Y.3001*** no ano 2017 [16], a qual descreveu que as próximas gerações de redes móveis denominadas **Redes Futuras** (*Future Nets* (FN)) do 5G estão baseadas em 4 Objetivos de Conscientização, os quais deveriam ter sido implantados até 2020 junto do Ecossistema 5G Global: (i) Conscientização de dados (*Data awareness*); (ii) Conscientização social e econômica (*Social and economic awareness*); (iii) Conscientização ambiental (*Enviromental awareness*); e (iv) Conscientização do serviço (*Service awareness*).

De acordo com [13] a Rec ITU-R M.2083-0 (**IMT–2020 e Além**) definiu alguns parâmetros do Ecossistema 5G Global, tais como: (i) estrutura e os objetivos gerais; (ii) descrição dos principais cenários de uso; (iii) principais recursos; (iv) tendências tecnológicas; (v) implicações do espectro; e (vi) os cronogramas para o desenvolvimento das IMT–2020 e Além.

Tão logo o avanço tecnológico permita a utilização de algumas faixas de frequências momentaneamente inutilizadas no EEM licenciado e não licenciado, ou aproveitar os Espaços Brancos (*White Spaces*) das faixas do 5G. Talvez seja possível realizar a expansão nas bandas das faixas das Ondas milimétricas acima de 6 GHz não licenciadas pela ITU. As agências reguladoras ao redor do mundo poderão subdividir e licenciar o uso dessas novas bandas liberadas pela ITU. As operadoras do mundo todo investem grandes volumes financeiros pelo privilégio de explorar essas estreitas faixas do EEM licenciado em seus serviços de comunicação móvel celular [4].

O relatório *The Mobile Economy 2022* publicado em [78], em tradução livre "A Economia Móvel 2022", estima que o 5G habilitará uma nova geração de aplicações e aportará USD$ 960 bilhões à economia global em 2030, agregando valor em diversos setores, tais como: (i) 42% Serviços; (ii) 38% Manufatura; (iii) 8% TICs; 8% Utilitários, construção, gás & petróleo, agro; 3% comércio; e 2% Outros".

Segundo [22] a evolução sociotécnica nas últimas décadas tem sido significativamente impulsionada pela evolução das comunicações móveis e tem contribuído para o desenvolvimento econômico e social de países desenvolvidos e também em desenvolvimento. Já o Fórum Econômico Mundial (*World Economic Forum*) prevê incremento de US$ 12,3 trilhões na produção econômica envolvendo o 5G até 2035, contribuindo para o PIB global [88].

Já [12] e [22] estimam que os usuários móveis devem poder acessar os serviços do 5G em qualquer hora e de qualquer lugar. Assim, é fundamental a interconexão e o funcionamento entre diversas e diferentes tecnologias de acesso à rede 5G. As Redes Heterogêneas (*Het Nets*) podem combinar diferentes tecnologias de redes: (i) via satélite; (ii) fixas cabeadas (fibra óptica, cabo coaxial, e cabo UTP); e (iii) móveis celulares.

De acordo com [101] de 2022 até 2029 teremos a implantação mundial do *5G Advanced*, em tradução literal "5G Avançado", com os lançamentos (*releases*) 18 a 22 definidos na IMT-2020 *Advanced*, como preparação para a transição das tecnologias do 5G para o 6G, conforme demonstra a Figura 2.7 – Evolução 5G-6G com previsão da Ericsson para os lançamentos futuros abaixo.

Figura 2.7: Evolução 5G-6G com previsão da Ericsson para os lançamentos futuros [85]

Da linha do tempo ilustrada na Figura 2.7 – Evolução 5G-6G com previsão da Ericsson para os lançamentos futuros, verifica-se que após a pandemia de COVID-19, mesmo com resultados socioeconômicos tão negativos com altas taxas de inflações, aumento do desemprego e aumento da pobreza geral nos países estrangeiros, tais obstáculos ainda permitiram a implantação do Ecossistema 5G Global entre os anos 2020 a 2022 no auge da pandemia de acordo com [84].

Em [85] cita que o uso da largura de banda internacional continua a crescer fortemente, pois subiu 30% de 719 Tbit/s em 2020 para 932 Tbit/s em 2021. Contudo, no mundo, ainda permanece o contraste de consumo por usuário da Internet de cerca de 150 Kbit/s entre as pessoas dos países desenvolvidos (média de 296 Kbits/s) e aquelas pessoas dos países em desenvolvimento (média de 144 Kbits/s), segundo publicado na página eletrônica da ITU na url: <https://www.itu.int/highlights-report-activities/highlights-report-activities/agenda_section/international-bandwidth-continues-to-grow-strongly/>.

A ITU-Telecomunicações (ITU-T) criou o *Focus Group NET-20230 (FG NET-2030)* em 2018, em tradução literal "Grupo Foco Rede 2030", o qual está concentrado na exploração das novas tecnologias para os sistemas 6G para além de 2030 [79].

Esse FGNET-2030 divulgou em 2019 o *White Paper* intitulado ***Network 2030*** *A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond*, em tradução livre "**Rede 2030** Um projeto de tecnologia, aplicações e factores de mercado para o ano 2030 e mais além"[86].

De acordo com [31] a Sociedade 5.0 prevê um sistema socioeconômico sustentável e inclusivo, alimentado por tecnologias digitais, tais como: (i) Sistemas de Comunicação baseados nas gerações 5G e 6G; (ii) IoT; (iii) AI; (iv) Big Data; e (v) outras tecnologias emergentes de comunicação, computação e tecnologias de detecção/atuação no setor industrial e na vida social.

Segundo [30] seu estudo realizado nos campos das Tecnologias Digitais, Indústria 4.0, Cadeias de Valor Globais e Economias Emergentes, foram avaliados 143 documentos, entre 2012 e 2021. Concluiu-se que o desenvolvimento das tecnologias da 4IR resultará no crescimento e desenvolvimento das economias emergentes, na melhoria da qualidade de vida, assim como no incremento da renda per capita dos países adotantes dessas tecnologias que serão possíveis com o Ecossistema 5G Global, por meio das Sustentabilidades (Econômica, Social e Ambiental).

O relatório ***The Impact of 5G*** publicado em janeiro de 2020 [88], estima que o Ecossistema 5G Global contribua com um total de US$ 13,2 trilhões de produção econômica até 2035, com cerca de 22,3 milhões

de empregos apenas na cadeia de valor global 5G. Por exemplo: (i) Fabricação U$ 4,7 trilhões; (ii) Informações e Comunicações U$ 1,6 trilhões; (iii) Atacado e Varejo U$ 1,2 trilhões; e (iv) Serviço público U$ 1 trilhão. A Figura 2.8 – Impacto financeiro cumulativo global do 5G previsto entre 2020 – 2035 demonstra as possibilidades que o 5G poderá causar na economia global a seguir.

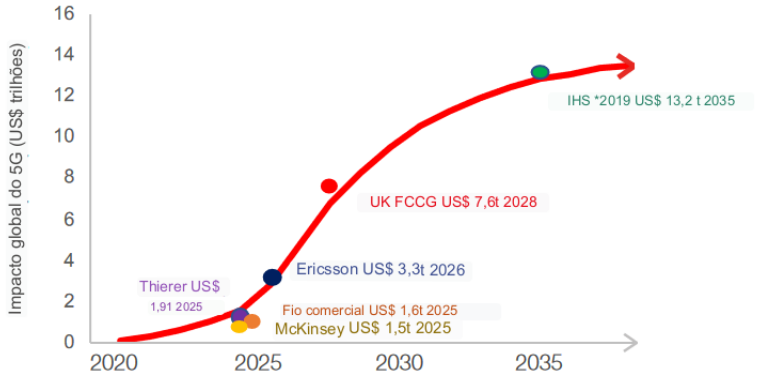

Figura 2.8: Impacto cumulativo global do 5G entre 2020 – 2035 [88]

Por todo o exposto nas assertivas acima, especula-se que talvez agora no período pós-pandemia da COVID-19 os 4 Objetivos de Conscientização das Redes Futuras do 5G sejam plenamente consolidados com o término da implementação do Ecossistema 5G Global já no final de 2023. Logo, a ITU propõe a migração para o 5G Avançado em 2025 (*5G Advanced*) e, a partir de 2028, a evolução para o 6G [102].

2.2.8 5G Brasil

Sobre o Ecossistema 5G Brasil em **A EVOLUÇÃO DAS REDES CELULARES: DO 1G AO 5G** [103] cita que é a primeira vez que pesquisadores brasileiros atuaram de forma significativa na concepção de um padrão de rede móvel celular típico, baseado nas tecnologias e serviços derivados do Ecossistema 5G Global, adaptando-o para uma arquitetura exequível para atender aos interesses do governo brasileiro.

Em [27] o Brasil se fez presente e opinou nas discussões sobre a identificação das faixas de frequências para as IMT–2020 e Além durante a WRC-19, as quais serão abordadas mais a frente na Subseção **2.2.12 Faixas do Espectro Eletromagnético (EEM) destinado para o Ecossistema 5G Brasil**.

De acordo com [104] o Brasil conseguiu uma vaga no Conselho da ITU em 3 de outubro de 2022, durante a Conferência de Plenipotenciários da ITU, ocorrida em Bucareste, na Romênia. Inclusive o especialista em regulação de telecomunicações, Sr Agostinho Linhares de Souza, servidor de carreira da Anatel, que atua no Ministério das Comunicações (MCom) foi eleito para compor a Junta de Regulação de Rádio (RRB) da ITU-R.

As pesquisas internacionais sobre o 5G priorizam melhorar a velocidade de conexão e diminuir a latência com mMTC para viabilizar a implantação da IoT em seus países. No entanto, as pesquisas brasileiras priorizam a expansão da cobertura do sinal de Internet para além dos centros urbanos, fornecendo-os as para áreas rurais e suburbanas com eMBB, apoiando as instituições responsáveis pelo Agronegócio[2], im-

[2]Em [105] 5G na Agropecuária: irá impulsionar ainda mais a produção agrícola por meio das tecnologias ligadas ao 5G: (i)

portante vetor econômico brasileiro gerador de empregos, de tecnologias e de impostos no Brasil [98].

A [106] divulgou o documento intitulado **O caminho para um Brasil digital Agenda para 2023-2026**[3], entregando-o para o governo brasileiro em setembro de 2022. Esse documento visava o panorama eleitoral presidencial de 2022 e seus reflexos para o futuro do Ecossistema 5G na época. A Agenda proposta pela GSMA encaminhou diversas recomendações específicas com os seguintes temas [78]: (i) Brasil indutor da estratégia digital; (ii) Regulação à prova de futuro; (iii) Menos impostos para a conectividade. Mais acesso; (iv) Desenvolvimento das redes; e (v) 5G: capacitação e expansão da produtividade.

Ainda o Governo federal brasileiro recebeu 14 medidas e recomendações específicas para dar continuidade à implantação do Ecossistema 5G Brasil com sucesso, já iniciado no Brasil em 2019 segundo [106]:

1. promoção de simetria regulatória para sustentabilidade dos serviços e potenciar a inovação;
2. aplicação de instrumentos de melhora regulatória como Análise de Impacto Regulatório (AIR) e Análise de Resultado Regulatório (ARR) para compreender o impacto das normas;
3. envolvimento prévio do setor na discussão de acordos do Brasil com outros países que envolvam matérias de telecomunicações;
4. redução tributária sobre acesso à conectividade para promover a inclusão digital;
5. fomentar uma reforma tributária com foco na sustentabilidade dos investimentos;
6. concessão de incentivos para o investimento na infraestrutura 5G, tais como depreciação/amortização acelerada fiscal e suspensão do PIS/COFINS para toda a cadeia;
7. harmonizar políticas públicas com a Lei Geral de Antenas (Lei 13.116/15) e assistência aos governos locais no desenvolvimento de políticas de simplificação, atualização e desburocratização para implantação de redes nos municípios;
8. planejar, aplicar e executar continuamente o uso dos recursos do Fundo de Universalização dos Serviços de Telecomunicações (FUST) em ações de redução do hiato digital;
9. estruturar política pública de segurança, em conjunto com o setor privado, para mitigar os roubos e furtos de equipamentos de telecomunicações;
10. construir um marco intersetorial de infraestrutura junto com o setor privado;

---

emprego de sensores para coleta de dados para avaliar os rendimentos das colheitas, níveis de umidade e topografia dos terrenos; (ii) Internet das Coisas (IoT) com Irrigação inteligente, dispositivos inteligentes poderão aferir a umidade do solo e a temperatura para avaliar as necessidades de rega e poderão diminuindo o consumo de água nos momentos ideais; (iii) emprego de Veículos Aéreos não Tripulados (*Unmanned Aerial Vehicles* tipo "*drones*") para identificação de necessidades de manutenção preventiva nas fazendas, relacionadas a equipamentos de elevado valor financeiro e patrimonial empregados na produção agropecuária e para monitorizar a saúde das colheitas e fotografar os campos, permitindo a redução do consumo de pesticidas e o aumento da eficiência do uso de nitrogênio diretamente na plantação; e (iv) empregar a monitorização eletrônica de rebanhos em tempo real, verificação do bem-estar e da saúde do gado/bufalino/equino/caprino, visando reduzir as perdas de animais fugitivos, incrementar a transparência e a rastreabilidade no mercado pecuário e diminuir os custos de fiscalização.

[3]Em [106] o relatório "O caminho para um Brasil digital Agenda para 2023-2026"pode ser acessado e lido na íntegra por meio da página eletrônica na url: <https://www.gsma.com/latinamerica/wp-content/uploads/2022/09/O-caminho-para-um-Brasil-digital_GSMA-2022.pdf>.

11. garantir segurança dos investimentos realizados nas radiofrequências adquiridas em leilões para expansão da conectividade;

12. acelerar e ampliar a aplicação e execução de recursos do Fundo de Universalização dos Serviços de Telecomunicações (FUST) em ações de redução do hiato digital, inclusive em projetos de educação e impulsionamento de uso de serviços móveis;

13. fomentar a digitalização dos setores produtivos, em especial da indústria, do agronegócio e do setor logístico: emprego, desenvolvimento e capacitação das habilidades digitais; e

14. aprofundar a estratégia e-Gov, estímulo à aprendizagem geral do usuário e gerar incentivos ao acesso patrocinado dos serviços.

Já o Ecossistema 5G Brasil estima os seguintes incrementos para a população brasileira [106]: (i) 6,49% na quantidade de acessos móveis de 154 milhões (2022) para 164 milhões (2026); (ii) 97,7% de dispositivos usuários de 4 milhões (2022) para 87 milhões (2026); e (iii) 27% de conexões de 1% (2022) para 28% (2026).

Por fim, destaca-se a importância para o Brasil, país com dimensões continentais e líder na América Latina, dispor de um membro no Conselho da ITU, o Sr Agostinho Linhares de Souza, para participar das discussões nas futuras WRC, as quais definirão o futuro das redes móveis celulares nos próximos anos [104].

2.2.9 Histórico e conceitos gerais do Ecossistema 5G Brasil

De acordo com a [68] o Brasil deve priorizar os investimentos em áreas que promovam o bem-estar social, bem como o desenvolvimento do País, tais como: (i) Saúde; (ii) Educação; (iii) Ciência, Tecnologia e Inovação. Estes recursos financeiros e humanos devem ser aplicados em produtos de defesa de uso dual, visando ao fortalecimento da Base Industrial de Defesa (BID) e à autonomia tecnológica no Brasil.

A **Estratégia Brasileira de Redes de Quinta Geração (5G)**, de 2019, abordou 5 (cinco) eixos de atuação para a implantação do Ecossistema 5G Brasil [26], a saber: (i) radiofrequência; (ii) outorga e licenciamento; (iii) pesquisa, desenvolvimento e inovação; (iv) aplicações; e (v) segurança no ambiente 5G.

De acordo com [107] o Edital de Licitação nº 1/2021-SOR/SPR/CD-ANATEL, em 24 de setembro de 2021, o Ecossistema 5G Brasil firmou obrigações relacionadas a oferta do serviço em todos os distritos urbanos do Brasil, assim como a cobertura de todas as rodovias federais, e infraestrutura de transporte de fibra óptica de diversas localidades, sem esquecer dos compromissos de levar a tecnologia 5G para todos os municípios brasileiros num prazo de até 20 anos.

O site do Senado Notícias [98] informou que o leilão do Ecossistema 5G Brasil pode gerar ao Tesouro Nacional algo em torno de R$ 3,06 bilhões com as vendas diretas dos lotes de frequências. Poderão surgir até R$ 49,7 bilhões das vendas dos espaços de radiofrequências do 5G, dos quais R$ 7,57 bilhões atenderão à demanda de Internet para a rede de Educação Básica e os outros R$ 39,1 bilhões de reais comporão o restante dos investimentos obrigatórios constantes do edital da Anatel de 2021, incluindo uma rede ex-

clusiva de comunicações para a área governamental da Administração Pública Federal (APF), situada em Brasília/DF, capital oficial do Brasil e importante centro decisório dos Três Poderes: (i) Executivo; (ii) Legislativo; e (iii) Judiciário.

O Projeto 5G Brasil batizou o 5G 3GPP de **Ecossistema 5G Brasil** no ano de 2021 [26]. Esse Projeto 5G Brasil busca desde o ano de 2017, de forma voluntária, divulgar o Ecossistema 5G Brasil para a sociedade brasileira e, principalmente, para o governo brasileiro, assim como a GSMA divulga o Ecossistema 5G Global por meio dos seus escritórios espalhados pelo mundo, conferências e *workshops* com eventos presenciais e remotos (*on-line*) [25].

De acordo com [27] o Ecossistema 5G usará a infraestrutura das fibras ópticas já instaladas nos municípios para realizar o reuso de frequências nas ERBs do 5G, o termo técnico correto para isso é *Backhaul*. Assim sendo, as redes 5G podem utilizar ondas milimétricas (GHz) com o objetivo de prover altas taxas de transmissão na interface aérea, que somada às outras tecnologias do 5G como o MU-MIMO e células pequenas (*small cells*) aumentará a eficiência espectral dos sistemas instalados nas localidades brasileiras pela **densificação de rede**. A arquitetura terrestre do 5G contém as fibras ópticas, enquanto que as interfaces aéreas contém as macrocélulas com o *5G Core* e as demais pequenas células (micro, pico e femto), que poderão ser conectadas ao 5G Core com essas fibras ópticas ou com enlaces de micro-ondas ou satelitais.

De acordo com o Grupo de Trabalho 5G, instituído na Câmara dos Deputados [108], a Anatel previu no Edital de Licitação nº 1/2021-SOR/SPR/CD-ANATEL, em 24 de setembro de 2021, que as empresas vencedoras dos lotes do 5G Nacional e 5G Regional terão compromissos nacionais e regionais de investimentos na ampliação da cobertura 5G e no *Backhaul*, obrigando-as a atenderem áreas pouco ou não servidas com sinal de Internet, por exemplo as localidades e estradas serão atendidas com a tecnologia 4G-LTE, enquanto que os municípios com mais de 30 mil habitantes serão atendidos com o 5G [107], [27].

Abaixo a Tabela 2.4 – Precificação das radiofrequências do 5G brasileiro estimada pela Anatel, descreve os valores estimados em R$ bilhões que poderão ser arrecadados com os leilões dos Lotes Nacionais e Regionais do 5G Brasil a partir de 2021.

Tabela 2.4: Precificação das radiofrequências do 5G brasileiro estimada pela Anatel

Faixa de frequência	**Valor Presente Líquido**	**Valor dos compromissos**	**Preço mínimo de todos os lotes**
700 MHz	R$ 2,2 bilhões	R$ 2 bilhões	R$ 150 milhões
2,3 GHz (50MHz)	R$ 4,8 bilhões	R$ 4,3 bilhões	R$ 445 milhões
2,3 GHz (40MHz)	R$ 3,85 bilhões	R$ 3,5 bilhões	R$ 356 milhões
3,5 GHz (Nacional)	R$ 22,8 bilhões	R$ 21,4 bilhões	R$ 1,35 bilhões
3,5 GHz (Regional)	R$ 5,7 bilhões	R$ 5,7 bilhões	R$ 41,8 milhões
26 GHz [1]	R$ 6,3 bilhões	-	R$ 6,3 bilhões
Total	R$ 45,6 bilhões	R$ 37,1 bilhões	R$ 8,68 bilhões

Fonte: Adaptado de [108]

Das informações da Tabela 2.4 da Anatel acima, o Tribunal de Contas da União (TCU) ratificou que

os recursos financeiros na ordem de R$ 6,3 bilhões advindos das vendas dos 5 Lotes Nacionais e 21 Lotes Regionais das bandas supra 6 GHz (24,5 GHz – 26 GHz) [108], os quais ficarão destinados para atender à implantação da Internet Banda Larga nas Escolas Públicas, por meio do Programa de Inovação Educação Conectada[4] de 2019, que foi duramente prejudicado pela pandemia de COVID-19 entre os anos de 2020-2023, não cumprindo o seu papel de realizar a inclusão digital escolar previsto inicialmente.

Em 2017, o Banco Nacional de Desenvolvimento Social (BNDES) estimou um impacto de até US$ 21,1 bilhões [26] advindo do uso de IoT no Agronegócio brasileiro até 2025, com a implantação das denominadas Fazendas Inteligentes (*Smart Farms*) .

No Brasil a Lei nº 8.248, de 23 de outubro de 1991, mais conhecida como Lei da Informática, concede incentivos fiscais na forma de redução do Imposto sobre Produtos Industrializados (IPI) para empresas que invistam em PD&I no setor de TICs retendo no mínimo 5% do faturamento bruto anual (Art. 4º desta Lei) [26]. Essa lei garante os investimentos financeiros para o desenvolvimento dados programas do governo federal na ampliação das redes de banda larga cabeadas nas escolas públicas.

A Anatel regula os termos dos contratos entre os órgãos governamentais (MCom, MCTI, e MEC) e as empresas parceiras (Oi, Telefônica, Sercomtel e Algar Telecom) no Serviço de Comunicação Multimídia (SCM) prestado em regime privado. Além disso, o edital do leilão do 5G também contempla o Programa Amazônia Integrada e Sustentável (PAIS[5]) e a construção da Rede Privativa de Comunicação da Administração Pública Federal (RPCAPF), segundo o Decreto nº 9.612, de 17 de dezembro de 2018. Esses compromissos foram definidos na Portaria nº 1.924/SEIMCOM, de 29 de janeiro de 2021, do MCom [27].

O projeto **Conectividade** coordenado pelo o Centro de Gestão e Estudos Estratégicos (CGEE) do MCTIC é o responsável pela formulação de política pública orientadora da atuação do Estado no desenvolvimento das telecomunicações brasileiras [27].

A Rede Nacional de Ensino e Pesquisa (RNP) também faz parte do Projeto Conectividade e também será beneficiada com o Ecossistema 5G Brasil, pois está presente em todas as unidades da federação com 27 Pontos de Presença, que formam a espinha dorsal (*Backbone*) da rede acadêmica nacional, a conhecida Rede Ipê (www.rnp.br), que participa de outras redes de pesquisa e universidades pelo mundo. O Programa Interministerial da RNP (PI-RNP) é formado pelos ministérios: (i) MCTIC; (ii) Educação (MEC); (iii) Saúde (MS); (iv) Defesa (MD); e a Secretaria Especial da Cultura. A RNP mantém acordos com empresas estaduais de tecnologia da informação, operadoras de telecomunicações privadas e ainda com a Telebrás, com a qual compartilha a infraestrutura da rede no âmbito do Programa Nacional de Banda Larga (PNBL) [27].

[4]Em [27] o Programa de Inovação Educação Conectada é originalmente o Plano de Banda Larga nas Escolas (PBLE), previsto para ser executado na década de 2014 até 2024.

[5]Em [98] o Programa Amazônia Integrada e Sustentável (PAIS) é um projeto estratégico brasileiro que está implementando redes de transporte em fibra óptica na Região Norte, por meio de 6 Infovias, ligando os municípios de: (i) Tefé/AM a Tabatinga/AM; (ii) Macapá/AP a Belém/PA; (iii) Novo Airão/AM a Boa Vista/RR; (iv) Itacoatiara/AM a Porto Velho/RO; (v) Manacapuru/AM a Rio Branco/AC; e (vi) Tabatinga/AM a Cruzeiro/AM.

2.2.10 Os três casos de uso previstos definidos para o Ecossistema 5G Brasil

De acordo com [23] as novas tecnologias do Ecossistema 5G Global [22] dispõe de 3 (três) modos de uso, os quais serão adaptados para as necessidades e realidades brasileiras, conforme demonstra a Figura 2.9 – Os 3 modos de uso do 5G brasileiro abaixo:

1. **Internet das Coisas massiva** (*mMTC - massive Machine Type Communication*) é dedicada em atender grande quantidade de dispositivos de Internet das Coisas (IoT) na comunicação máquina para máquina (M2M), com ampla cobertura e baixo consumo de bateria, levando a IoT a um novo patamar de atendimento ao público brasileiro;

2. **Controle de Missão Crítica** (*URLLC - Ultra-Reliable Low Latency Communication*) é dedicada em prover requisitos rigorosos de conexão com baixíssima latência e altíssima confiabilidade, voltada para aplicações sensíveis a atrasos e a erros, possibilitando o uso de veículos autônomos, cirurgias remotas, controle remoto de maquinário industrial e a nova Internet tátil contendo as Realidades Virtual (RV) e Aumentada (RA); e

3. **Banda Larga Móvel avançada** (*eMBB - Enhanced Mobile Broadband*) é dedicada em fornecer altas taxas de dados para descarregamento/carregamento (*download/upload*), ampla área de cobertura para as novas necessidades do usuário humano e onipresença de pontos de acessos comuns nas macros e micros células das diversas redes.

Figura 2.9: Os três modos de uso do 5G brasileiro [23]

2.2.11 Os requisitos técnicos definidos para o Ecossistema 5G Brasil

Segundo [98] foram realizados diversos estudos e pesquisas para a definição dos principais requisitos das redes móveis 5G brasileiras, tais como:

(i) aumento da velocidade de transmissão para até 100 *Gigabits* por segundo (Gbps);

(ii) cerca de cem vezes mais rápida do que a geração anterior (4G LTE);

(iii) redução da latência (atraso) das transmissões para menos de 1 milissegundo (ms);

(iv) aproximadamente cem vezes menor que nas redes 4G;

(v) a capacidade de conectar até 1 milhão de dispositivos por quilômetro quadrado, também ampliando em cem vezes a capacidade atual;

(vi) maior eficiência no uso das faixas de radiofrequência associadas, representando maior quantidade de dados transmitidos no espectro eletromagnético; e

(vii) maior eficiência energética de seus equipamentos, gerando economia de eletricidade e garantindo a sustentabilidade em relação às tecnologias anteriores já instaladas (3G/4G).

De acordo com [12] os 3 serviços do 5G possibilitam uma gama de melhorias no cotidiano da sociedade atual, conforme descritos na Tabela 2.5 – Exemplos dos três serviços (eMBB, mMTC, e URLLC) oferecidos pelo 5G NR abaixo.

Tabela 2.5: Exemplos dos três serviços (eMBB, mMTC, e URLLC) oferecidos pelo 5G NR

eMBB - aprimorada Banda Larga Móvel	**mMTC - Comunicação maciça Tipo Máquina**	**URLLC - Comunicações Ultra-confiáveis de Baixa Latência**
Altas taxas de dados	e-Saúde	IoT Industrial
Experiência do usuário aprimorada	Redes Capilares	Cirurgia Remota
Cobertura imensa	Cidades Inteligentes	Entrega por *Drone*
Conectividade aprimorada	Rede de Energia Inteligente	Grade de Automação Inteligente
Realidade Virtual	Medição Inteligente	Manufatura e Treinamento remotos
Realidade Aumentada	Varejo inteligente	Veículo de Comunicação de Tudo
Realidade Estendida	Logística e Gestão de Frotas	Veículos Autônomos (terrestres, aéreos e marítimos)
Maior mobilidade do usuário	IoT de baixo custo	Internet Tátil
A taxa de dados de pico de 20 Gb/s para *download* (DL) e 10 Gb/s para *upload* (UL)		
Capacidade de tráfego de área de 10 Mbits/s/m2	Alta densidade de conexão de 1 milhão (M) dispositivos/Km2	Latência do plano do usuário de até 1 ms para uRLLC
Aumentar a eficiência energética em 100 vezes em relação ao 4G		Confiabilidade de 99,999% de probabilidade de sucesso
Fornecer eficiência espectral de pico de cerca de 30 b/s/Hz para DL e de 15b/s/Hz para UL	Maior cobertura de comunicação de borda	Latência do plano de controle de até 10 – 20ms
O usuário experimentará uma taxa de dados de 100 Mb/s para DL e 50 Mb/s para UL	Alta Mobilidade de 10 Km/h para *indoor*, 30 Km/h para urbano denso e 500 Km/h para rural	Tempo de interrupção da mobilidade inferior a 1 ms
Suporta alta mobilidade de cerca de 500 Km/h até 1.000 Km/h		
Menos de 1 ms de tempo de interrupção móvel		

Fonte: Adaptado do livro [12]

2.2.12 Faixas do espectro eletromagnético destinado para o Ecossistema 5G Brasil

A Anatel teve participação ativa e destacada nesse grupo, pois desenvolveu um software de simulação de compatibilidade e compartilhamento de sistemas **IMT–2020 e Além** com outros sistemas de radiocomunicação denominado *SHARC – SHARing and Compatibility studies between radiocommunication systems*[109]. Esse software SHARC foi uma iniciativa brasileira de Doutores em Comunicações da Anatel e da Universidade de Brasília (UnB) para apoiar futuras posições técnicas da administração brasileira junto ao Ecossistema 5G Brasil no emprego do Serviço de Satélites Fixos e nos sistemas de comunicações 5G propostos na [29] .

Na WRC-19 realizada em Sharm El-Sheikh, no Egito, de 28 de outubro a 22 de novembro de 2019,

a ITU-R identificou as faixas de radiofrequências de 24,25 GHz – 27,5 GHz; 37 GHz – 43,5 GHz; 45,5 GHz – 47 GHz; 47,2 GHz – 48,2 GHz; e 66 GHz – 71 GHz como livres para uso no 5G. Trata-se de um acréscimo de 17,25 GHz do espectro eletromagnético para uso no 5G Global, com 14,75 GHz de espectro já harmonizado mundialmente, alcançando 85% da harmonização global [110], na qual poderá beneficiar o Ecossistema 5G Brasil.

A Anatel publicou o Edital de Licitação nº 1/2021-SOR/SPR/CD-ANATEL, em 24 de setembro de 2021 e expediu a outorga necessária para liberar o uso comercial das radiofrequências nas faixas: (i) **infra 6 GHz** com a banda de **700 MHz**; (ii) **intra 6 GHz** com as bandas de **2,3 GHz e 3,5 GHz**; e (iii) **supra 6 G Hz** com a banda de **26 GHz**; e (iv) a implementação dessas bandas (infra, intra e supra 6 GHz) terão o prazo total de 20 (vinte) anos para exploração pelas operadoras de telefonia móveis vencedoras do leilão, e poderá ser prorrogável por mais 10 (dez) anos de exploração, conforme detalha a Figura 2.10 – Quadro Resumo do Edital de Licitação nº 1/2021, do 5G, elaborado pela Anatel abaixo [107].

A Estratégia Brasileira de Redes de Quinta Geração (5G) [26], de 2019, estabeleceu que o 5G 3GPP no Brasil deverá atender a múltiplos requisitos, focando nas qualidades das faixas para cada aplicação nos 3 usos: urbano, semi-urbano e rural.

As faixas de frequências mais baixas podem oferecer possibilidade de ampla cobertura em relação ao padrão atual 4G (LTE), mas com baixa disponibilidade de largura de banda:

- **700 MHz**: radiofrequências em caráter primário de bloco de 10 + 10 MHz ou blocos de 5 + 5 MHz, na Subfaixa de radiofrequências de 708 MHz a 718 MHz e de 763 MHz a 773 MHz, para cidades de até 100 mil habitantes.
- **2,3 GHz**: radiofrequências em caráter primário de blocos de 50 MHz, na Subfaixa de radiofrequências de 2.300 MHz a 2.350 MHz, e de blocos de 40 MHz, na Subfaixa de radiofrequências de 2.350 MHz a 2.390 MHz e
- **3,5 GHz**: radiofrequências em caráter primário de blocos de 80 MHz ou de 20 MHz na Subfaixa de radiofrequências de 3.300 MHz a 3.700 MHz.
- As faixas de frequências mais altas podem permitir grandes taxas de transmissão, mas com menor área de cobertura em relação ao padrão atual 4G (LTE), como em **26 GHz**: radiofrequências em caráter primário com blocos de 400 MHz ou 200 MHz, na Subfaixa de Radiofrequências de **24,3 GHz a 27,5 GHz**.

Das informações da Figura 2.10 acima, estima-se que o Ecossistema 5G Brasil [26], [27], [108]: (i) licitará 3.710 MHz do espectro eletromagnético licitado pela Anatel; (ii) poderá gerar desenvolvimento socio-econômico por meio de empregos diretos e indiretos nas comunidades que estão implantando o 5G; (iii) poderá ser o principal meio da população obter comunicações, informação e lazer; (iv) poderá realizar a inclusão digital na Educação Básica; (v) poderá atender áreas remotas da Amazônia e áreas das cidades fronteiriças do Brasil; e (iv) poderá ampliar significativamente a cobertura atual do 4G LTE nos municípios com até 200 mil habitantes e nas rodovias federais, como cláusula obrigatória para as Operadoras de telefonia móveis concorrentes dos pregões da Anatel.

Faixa	Banda	Bloco	Oferta de bloco na 1ª rodada	Resultado esperado	Oferta de bloco na 2ª rodada	Spectrum Cap	Compromisso	Observação
700 MHz	708 - 718 MHz 763 - 773 MHz	Nacional	10 + 10 MHz	Sobras de 10 + 10 MHz para nova operadora atacadista	5 + 5 MHz	Art. 1º, Inciso I, da Resolução nº 703/2018	ERB 4G ou superior em localidades e trechos de estradas	Não é admitida a participação no Leilão daquelas operadoras que já dispõe de autorização na Faixa 700 MHz ou esteja em processo de transferência de controle societário
2,3 GHz	2.300 - 2.390 MHz	Regional	90 MHz	8 operadoras com 40 MHz e 8 operadoras com 50 MHz	Não há	50 MHz	95% de cobertura de municípios sem 4G + Ativar 4G em localidades	Não há
3,5 GHz	3.300 - 3.700 MHz	Nacional e Regional	400 MHz	80 MHz por operadora	20 MHz	100 MHz	ERBs 5G + Limpeza da Banda C + Programa Amazônia Integrada e Sustentável (PAIS) + Rede Privativa de Comunicação da Administração Pública Federal (RAAPF)	1ª rodada com único bloco de 10 + 10 MHz: - 4 nacionais de 80 MHz. - 8 regionais de 80 MHz, sendo possível arrematar no máximo dois blocos regionais 2ª rodada com 2 blocos de 5 + 5 MHz: - Blocos de 20 MHz, caso não haja vencedor para algum dos lotes nacionais ou ao menos um lote regional
26 GHz	24,3 - 27,5 GHz	Nacional e Regional	3.200 MHz	400 MHz por operadora	200 MHz	1 GHz	Não há	5 blocos nacionais com 400 MHz e 21 blocos regionais com 400 MHz

Figura 2.10: Quadro Resumo do Edital de Licitação nº 1/2021, do 5G, elaborado pela Anatel [107]

Das assertivas acima, conclui-se que o Governo Federal brasileiro conquistou importantes marcas na trajetória tecnológica das telecomunicações mundiais, pois implementou o Ecossistema 5G Brasil em todas as suas 27 Capitais Estaduais já em meados de 2022, equiparando-se aos outros países estrangeiros detentores do 5G 3GPP instalados em suas capitais. Por exemplo: Alemanha, China, Coreia do Sul, EUA, Espanha, França, Israel, Índia, Inglaterra, Portugal, entre outros países europeus que ainda estão na mesma fase de implementação do 5G no Brasil.

Em fevereiro de 2021, a Anatel aprovou o edital do leilão das faixas de radiofrequência para a prestação de serviços de telecomunicações 5G no Brasil. Assim previu os compromissos para as operadoras de telefonia celular comprarem a outorga de uso por 20 (vinte) anos, podendo ser prorrogável por mais 10 (dez) anos, mediante pagamento de acordo com o estabelecido na lei vigente, conforme descreve a Tabela 2.6 – Compromissos de atendimento da Anatel com as Faixas do Ecossistema 5G Brasil abaixo.

Conforme divulgado por [111] o sinal do 5G Autônomo (5G SA) já está em operação desde o dia 06/10/2022 em todas as 27 capitais brasileiras, a saber: (i) Brasília/DF; (ii) São Paulo/SP; (iii) Rio de Janeiro/RJ; (iv) Vitória/ES; (v) Goiânia/GO; (vi) Palmas/TO; (vii) Florianópolis/SC; (viii) Porto Alegre/RS; (ix) Curitiba/PR; (x) Belo Horizonte/MG; (xi) Salvador/BA; (xii) João Pessoa/PB; (xiii) Fortaleza/CE; (xiv) Natal/RN; (xv) Recife/PE; (xvi) Aracaju (SE); (xvii) Boa Vista (RR); (xviii) Campo Grande (MS); (xix) Cuiabá (MT); (xx) Maceió (AL); (xxi) São Luís (MA); (xxii) Teresina (PI); (xxiii) Belém (PA); (xxiv) Macapá (AP); (xxv) Manaus (AM); (xxvi) Porto Velho (RO); e (xxvii) Rio Branco (AC).

Tabela 2.6: Compromissos de atendimento da Anatel com as Faixas do Ecossistema 5G Brasil

Compromissos assumidos da Anatel	**Faixas**
Oferecer o SMP nas rodovias federais e nas localidades sem 4G indicadas no edital	700 MHz
Oferecer o SMP em 95% da área urbana dos municípios sem 4G	2,3 GHz
Instalar estações rádio base com tecnologia 5G Autônomo (*Standalone* (SA)), na proporção mínima de 1 ERB para cada 10 mil habitantes Ressarcir, à população afetada, as soluções para mitigar a interferência prejudicial na recepção do sinal de TVRO – Portaria MCTIC nº 418, de 2020 Implantar o Programa Amazônia Integrada e Sustentável (PAIS) – Decreto nº 10.800, de 2021 Implantar a Rede Privativa de Comunicação da Administração Pública Federal – Decreto nº 10.799, de 2021	3,5 GHz (abrangência nacional)
Instalar rede de transporte de fibra ótica nos municípios indicados no edital	3,5 GHz (abrangência regional)
Investir em projetos de conectividade de escolas públicas de Educação Básica (Creches, Ensinos Fundamental e Médio), com a qualidade e a velocidade necessárias para o uso pedagógico das TICs nas atividades educacionais regulamentadas pela Política de Inovação Educação Conectada	26 GHz

Fonte: Adaptado de [107], [98]

O estudo sobre o Ecossistema de Soluções Digitais e Aplicações do 5G no Brasil [112] realizado pela Secretaria Especial de Produtividade e Competitividade (SEPEC), do Ministério da Economia, em parceria com o Programa das Nações Unidas para o Desenvolvimento (PNUD) e parceira com a empresa Deloitte, concluiu que o uso de soluções 5G pode representar um benefício de R$ 590 bilhões por ano para a economia brasileira, considerando-se somente a demanda potencial de software e a expectativa de valor total de R$ 101 bilhões até 2031. A nova geração de internet móvel pode gerar até R$ 22,8 milhões de empregos no mundo até o ano de 2035.

A página eletrônica Direito da Comunicação informou que o Departamento de Defesa (DoD) dos Estados Unidos da América (EUA), mais conhecido como Pentágono, está empregando o uso dual – civil e militar – do 5G do EEM norte-americano nas faixas de 3.100–3.450 MHz e 3.450–3.980 MHz, nos programas de modernização da defesa norte-americana e considera isso essencial para a segurança econômica e segurança nacional dos EUA.

O Pentágono está desenvolvendo tecnologias e serviços derivados do Ecossistema 5G Global para as Forças Armadas dos EUA: Marinha (*Navy*), Exército (*Army*) e Força Aérea (*USAF*), por meio de parcerias comerciais com diversas empresas de alta tecnologia, tais como: (i) Ericsson; (ii) AT&T; (iii) Vectrus; (iv) GE Research; (v) General Dynamics Mission Systems; (vi) Nokia; entre outras dezenas não citadas aqui.

Das assertivas acima e das abordagens realizadas nas subseções anteriores, conclui-se que o MD (Brasil) poderia seguir o exemplo do Pentágono (EUA) e institucionalizar desde já o emprego dual – civil e militar – do Ecossistema 5G Brasil na defesa e segurança nacional, incorporando as tecnologias aos programas e projetos estratégicos das FA já em desenvolvimento: (i) MB (Programa do Submarino Nuclear); (ii) EB (Programa Proteger); e (iii) FAB (Programa de Satélites de Baixa Altura).

2.3 AMEAÇAS CIBERNÉTICAS EM UM TÍPICO ECOSSISTEMA 5G E SUAS IMPLICAÇÕES PARA A DEFESA BRASILEIRA

2.3.1 Contextualização

As tecnologias do 5G foram eleitas como a nova geração de redes móveis para acesso a dados entre 2020 – 2030 [12], [22], mas podem se tornarem plataformas de difusão de ameaças à Segurança Cibernética mundial [13].

De acordo com [13], [22], [113], foram estabelecidos rigorosos requisitos de segurança no 5G, porém como todo sistema de comunicações móveis ainda existem algumas vulnerabilidades herdadas das tecnologias anteriores 4G e 3G, e a cada dia surgem novas ameaças.

De acordo com [114] as Ameaças Persistentes Avançadas (*Advance Persistent Threats* (APTs)) são ataques realizados com as características acima; são difíceis de mitigar e proteger e, eventualmente, tornam-se ameaças sérias, causando grande dano aos sistemas de comunicações e de informações. As APTs geralmente visam instalações de IC, grandes provedores de serviços e bancos de dados, os quais atendem às massas e causam grande perturbação e impacto multidimensional, e também demonstradas na Figura 2.11 – Cenário de APTs presentes no Ecossistema 5G a seguir.

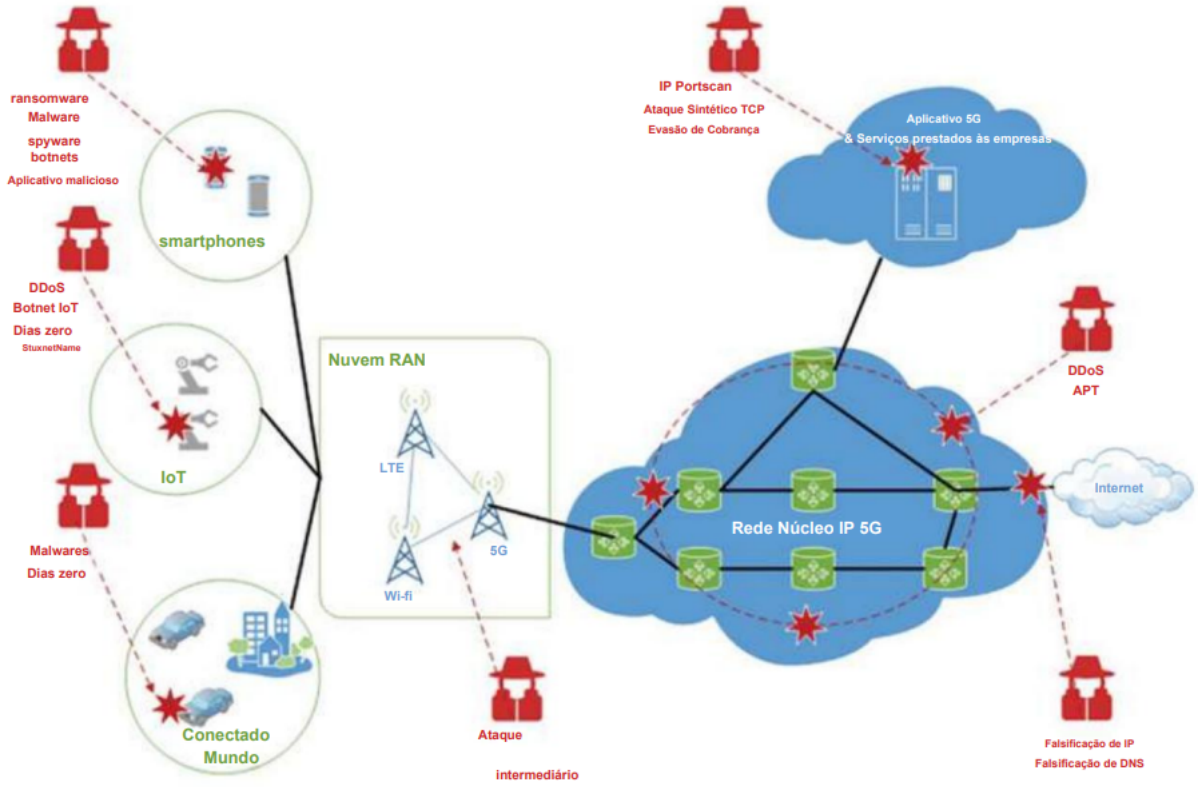

Figura 2.11: Cenário de APTs presentes no Ecossistema 5G [13]

Prevê-se que as ameaças de segurança da próxima geração tenham as seguintes características [13]: (i) **sofisticada**: porque pode usar uma mistura de vários estágios e de vários vetores de ataque e de ferramentas de intrusão, tornando-se complexas para a detecção (e.g. Kit de exploração *Angler* que é empacotado para explorar um múltiplo fornecedor em um único ataque); (ii) **ofuscatória**: porque os ataques devem ser mascarados por múltiplas camadas, tornando-se muito difíceis de serem detectados; (iii) **evasiva**: porque tem capacidade de se esconder no sistema (e.g. ataque de criptografia tipo *ransomware*) e ser detectado; e (iv) **persistente**: porque os ataques devem ser consistentes e evoluírem após cada tentativa falhada de intrusão no sistema invadido.

2.3.2 Ecossistema 5G e os tipos de Ameaças Cibernéticas

De acordo com [114] uma Ameaça Persistente Avançada (*Advanced Persistent Threat* (APT)) é usada para obter informações ou causar danos nos seus alvos, empregando técnicas de invasões sofisticadas, furtivas e contínuas. Há diversos tipos de APTs e são elaboradas para obterem acesso a um sistema, permanecerem nele por um período prolongado de tempo sem serem descobertas, e visam ações destrutivas em potencial.

Geralmente são 5 estágios de uma APT [114]: (i) primeiro estágio: obter acesso; (ii) segundo estágio: estabelecer um Ponto de Apoio; (iii) terceiro estágio: aprofundar o Acesso; (iv) quarto estágio: mover-se lateralmente, ou seja, mover-se como administrador do sistema, pois sem ser detectado pelo sistema invadido obterá mais acesso e informações; e (v) quinto estágio: observar, aprender e se esconder. Como

exemplos alguns tipos de APT estão descritos na Tabela 2.7 – Principais APT no Ecossistema 5G abaixo.

Segundo [114] o maior problema é que as APTs deixam brechas abertas pelos invasores (*hackers/crackers*) permitindo o retorno deles para espionagem eletrônica com coleta de dados e novos ataques. Ainda, muitas defesas cibernéticas tradicionais, tipo antivírus e *firewalls* nem sempre conseguem proteger os sistemas contra esses tipos de ataques persistentes. As soluções encontradas para evitar APTs são medidas de segurança e contramedidas APTs [116], tais como:

1. **Implementar Autenticação Multifator (AMF)**: é uma das formas de segurança cibernética mais eficazes para evitar/dificultar o acesso não autorizado de invasores em um sistema informático. Pois a AMF exige que os usuários forneçam mais de uma forma de autenticação para acessar um sistema ou rede, tornando mais difícil para os atacantes obterem acesso na invasão desse sistema;

2. **Implementar *Firewalls* de Próxima Geração**: são computadores especialmente projetados para proteger o tráfego na rede em tempo real e bloquear tentativas de acesso não autorizado (atividades suspeitas ou maliciosas) contra ataques de rede avançados tipo APTs;

3. **Adotar Criptografia de dados**: a criptografia é uma técnica de segurança que permite a cifragem/-Decifragem dos dados transmitidos em uma mensagem, juntamente de seus anexos, e dos dados armazenados em um sistema ou banco de dados, por meio de códigos algoritmos que tornam os dados inacessíveis/ilegíveis para outros sistemas que não disponham das Chaves (Simples ou Dupla) para Cifragem/Decifragem dos dados seguros. Essa medida garante a Proteção da Informação ou dos dados confidenciais de uma organização contra acesso não autorizado;

4. **Detectar Anomalias**: é o monitoramento constante do tráfego da rede em busca de atividades incomuns ou suspeitas (e.g. altas taxas de tráfegos de dados fora do expediente comum de uma instituição). A detecção de anomalias pode ajudar a identificar atividades maliciosas que podem ser causadas por APTs instalados na rede ou em uma máquina hospedeira;

5. **Implementar soluções de gerenciamento de vulnerabilidades**: é interessante a equipe de segurança cibernética da organização aliar-se às demais equipes de segurança patrimonial e de segurança do trabalho para executar ações visando soluções combinadas com diversas técnicas de segurança (e.g. usar AMF, Criptografia, Verificação da Rede em tempo real, alarmes e câmeras de vigilância em áreas importantes, usar cartões especiais de acesso restrito, uso de biometria, restrição de acesso à Informação por compartimentação de setores e níveis de acesso), pois ajudam a identificar e corrigir as vulnerabilidades da segurança física e lógica da rede, do ambiente de trabalho, de acesso às áreas proibidas, das pessoas responsáveis pelos sistemas (Administradores), as quais podem ser exploradas pelos atacantes externos e também internos. A implementação dessas soluções podem ajudar a minimizar as chances de um ataque bem-sucedido;

6. **Realizar Testes de Penetração de Rede (PENTEST)**: para identificar vulnerabilidades de segurança em um sistema ou rede. A regularidade desses testes de penetração pode ajudar a identificar e corrigir vulnerabilidades antes dos atacantes as explorarem; e

7. **Treinar, regular, e conscientizar o conceito de Segurança dentro da organizações**: um ambiente seguro é aquele já identificado e escalonado em níveis de segurança, definindo tarefas e modos de

Tabela 2.7: Principais Ameaças Persistentes Avançadas (APT) no Ecossistema 5G

Ameaça	**Descrição da ameaça**	**Gravidade do impacto (Menor, Moderado, Severo, Extremo)**	**Ocorrência de Ameaça Probabilidade (1 – 5, Baixo – Alto)**
Ransomware	São *Malwares* especializados que usam exploração, criptografia e o bloqueio no acesso aos dados das informações críticas capturadas. A devolução do acesso das informações sequestradas é liberado mediante pagamento (geralmente em dinheiro e/ou *Bitcoins*) exigido no resgate	Severo	3
Advance Malware	São *Malwares* avançados que realizam ataques em bilhões de dispositivos móveis e de IoT com capacidade de explorar as vulnerabilidades de rede e o sistema operacional (SO)	Extremo	3
IoT Botnets	São Redes de Robôs formadas por dispositivos móveis e de IoT, as quais hospedam um robô/agente mestre que exerce o C² sobre os demais equipamentos hospedeiros (*hosts*) da rede. Os Robôs mestres emitem comandos de telemetria remotos e os hospedeiros provém o vazamento das informações continuamente. Esse tipo de ameaça é usado para ambos ataques: Passivos e Ativos	Severo	2
Critical Infrastructure Threats	São ameaças prejudiciais direcionadas aos serviços das Infraestruturas Críticas (IC) para causar danos ou destruição da infraestrutura, como o SCADA[6], i.e. ataques tipo *Stuxnet/Shamoon*	Extremo	3
Zero-day Attacks	É um ataque avançado denominado "Dia Zero Ataque", o qual explora as vulnerabilidades ainda não descobertas de sistemas. Pode ser uma combinação de diversos ataques ou um pacote de vários tipos de ataques simultâneos, e.g. *malware, rootkits e botnets*	Extremo	1

Fonte: Adaptado do Livro [13]

operação prévios para combater os diversos tipos de ameaças, com palestras de conscientização e capacitação de de todo com as melhores práticas de segurança. O treinamento regular pode ajudar a garantir que todos estejam alertas dos riscos e saibam como neutralizá-los e/ou minimizá-los.

Em resumo, as APTs representam uma ameaça significativa para as organizações em todo o mundo. Em contrapartida disso, o NIST [55], a *National Security Agency* (NSA), a *The Cybersecurity and Infrastructure Security* Agency (CISA) [117], e as Normas ABNT da família 27.000 definem regras claras de estruturas (*frameworks*) e também emitem alertas sobre a importância da **Segurança da Informação**, dispõe de questionários de identificação e avaliação dos níveis dos riscos cibernéticos, propõe medidas de proteção e de combate contra muitos ataques, inclusive tipo APT.

Segundo [114] o Fator Humano é decisivo para o sucesso na ação de uma APT, pois através de um agente interno da organização ações de Engenharia Social obtém-se senhas e outros códigos de acessos para locais não autorizados a quaisquer pessoas (e.g. impressões digitais, escaneamento facial, cartões de acesso, etc).

Enfim, no Ecossistema 5G existem as APTs e as organizações no mundo devem: (i) prevenir; (ii) combater; e (iii) neutralizar, essas ameaças avançadas. Para essas ações é necessário implantar estruturas internas e externas de Segurança Cibernética [116], as quais devem incluir: (i) tecnologias avançadas de segurança; (ii) gerenciamento das vulnerabilidades e dos riscos de cada uma; (iii) treinamento e testes regulares dos Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs); e (iv) palestras, filmes e panfletos com conscientização e boas práticas de Seg Info.

2.3.3 Consequências das ameaças cibernéticas do 5 G para a Segurança Cibernética brasileira

A Presidência da República (PR) visando estabelecer critérios e padronizar ações para os diversos órgãos do Governo brasileiro, buscando manter e aprimorar a Seg Info oficial, a qual engloba a Seg Com e a Seg Ciber, contra possíveis ameaças[7] cibernéticos publicou os seguintes documentos como marcos legais, que devem ser cumpridos sob penas dos órgãos competentes: (i) Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) em 2018 [57]; (ii) Política Nacional de Segurança da Informação (PNSI) em 2018 [58]; e (iii) Estratégia Nacional de Segurança Cibernética (E-Ciber) em 2020 [59].

A Anatel seguindo o exemplo do GSI/PR e também da Comissão Federal de Comunicações (*Federal Communications Commission* (FCC)) órgão regulador das áreas de telecomunicações e radiodifusão nos Estados Unidos desde 1934, a qual vem combatendo as ameaças estrangeiras dentro do Ecossistema 5G nos EUA, emitiu a Resolução nº 740, de 21 de dezembro de 2020 [122], que se tornou mais conhecida como **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações**.

Esse regulamento estabeleceu os critérios padronizados para que as Operadoras de Telefonia Móvel brasileiras busquem implementar equipamentos e produtos de telecomunicações provenientes de fornece-

[7] Em [118], [119], [120], [121] descrevem alguns tipos de Ameaças Cibernéticas: atualmente muitas ações cibernéticas podem ser executadas contra equipamentos de TIC em rede, isolados por meio de inserções de páginas *Web*, arquivos e/ou códigos maliciosos, tais como: (i) Vírus; (ii) *Malwares*; (iii) *Ransomwares*; (iv) *Cryptojackings*; (v) *Zero-day exploits*; (vi) *Rootkits*; (vii) *Trojans*; (viii) *Spywares*; (ix) *Phishings*; (x) *Spearphishings*; (xi) *Distributed Denial of Service (DDOS)*; (xii) *Man-in-the-Middle (MitM)*; (xiii) *Cross-site Scripting (XSS)*; e (xiv) *Advanced Persistente Threat (APT)*.

dores que possuam política de segurança cibernética compatíveis com os princípios e diretrizes dispostos naquele Regulamento; e empresas que realizem processos de auditorias periódicos independentes, no âmbito das redes e serviços de telecomunicações; e a mitigação de riscos em Infraestruturas Críticas, também denominadas Infraestruturas Estratégicas [50].

Segundo [123], no estudo realizado pelo Banco Interamericano de Desenvolvimento (BID) em parceria com a Universidade Oxford, no ano de 2020, na América Latina e Caribe somente 7 de 32 países analisados dispõe de plantas de contenção na IC contra ataques cibernéticos. Esses ataques cibernéticos podem causar danos econômicos na ordem de 1% do PIB de alguns países e, até 6% do PIB, se submetidos diretamente às IC dos países, agravando-se ainda mais os danos econômicos, sociais e políticos nesses países.

Nesse estudo o Brasil foi analisado na sua capacidade de Seg Ciber comparativa nos anos 2016 e 2020. Os resultados apresentaram melhoras significativas nas cinco dimensões avaliadas: D1 – Política e Estratégia de Segurança Cibernética; D2 – Cibercultura e Sociedade; D3 – Educação, treinamento e habilidades em segurança cibernética; D4 – Estruturas Legais e Regulatórias; e D5 – Padrões, Organizações e Tecnologias. Ainda sobre o Brasil, concluiu-se que tanto o Marco Civil da Internet (Lei n° 12.965/2014) como a E-Ciber (Decreto nº 10.222/2020) são marcos importantes para a Seg Ciber brasileira [123] pois instituíram ações e responsabilidades aos atores governamentais brasileiros.

Já o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional e de último recurso [118]. É mantido pelo Núcleo de Informação e Coordenação Brasil (NIC.br), orienta as medidas de proteção e atualizações de segurança da Internet no Brasil, realizando a divulgação de ações em Boletins Especiais para a Administração Pública Federal (APF) e para as empresas de TIC, visando aumentar a resiliência e a proteção cibernéticas brasileiras. Segundo [64] já foram comprovados atos de espionagem eletrônica dos EUA contra o Brasil em 2013, durante o governo da ex-Presidente da República Dilma Roussef.

O **Plano Estratégico do Exército 2020-2023** indica os investimentos da Força Terrestre para o quadriênio 2020-2023, visando o processo de transformação do Exército rumo à Era do Conhecimento [72].

O Objetivo Estratégico do Exército nº 4 descreve as ações para o Exército atuar no Espaço Cibernético com liberdade de ação, conforme **OEE 4 – ATUAR NO ESPAÇO CIBERNÉTICO COM LIBERDADE DE AÇÃO**, o qual descreve 2 Estratégias (4.1 Implantação do Setor Cibernético na Defesa; e 4.2 Implantação do Setor Cibernético no Exército), além de 2 Ações Estratégicas (4.1.1 Implantar o Sistema Militar de Defesa Cibernética (SMDC); e 4.2.1 Implantar a estrutura de defesa e guerra cibernética), bem como as demais atividades e os responsáveis por cada uma delas.

Nesse PEEx constam que as atividades já iniciadas em 2020, tendo como alvo o ano de 2023 para a implantação total do **Sistema Militar de Defesa Cibernética (SMDC)**, por meio do Comando de Defesa Cibernética (Com D Ciber) e da Escola Nacional de Defesa Cibernética (ENaDCiber) [72]. Dessa forma, aumentar-se-ão as capacidades dos militares e também dos agentes civis da APF responsáveis pela resiliência e segurança cibernéticas nacionais, de interesse para a Defesa (MD). Tanto o Com D Ciber, como a ENaDCiber estão vinculadas diretamente ao MD.

A implantação do Setor Cibernético no Exército, missão determinada ao EB na [51] está ocorrendo

paulatinamente com investimentos nos componentes operacionais e táticos nos níveis da Defesa Cibernética (MD) e da Guerra Cibernética (EB). Nesse sentido de convergência de esforços o EB criou o 9º Batalhão de Comunicações (9º B Com GE) em 2010 e o 1º B Com GE em Manuas/AM em 2013, ambos com capacidades operacionais de realizarem ações de Guerra Cibernética (ataque, defesa e exploração cibernéticos).

Por fim, para complementar as ações de preparação do Brasil contra os atores e os Poderes Cibernéticos (P Ciber) das demais nações estrangeiras, ocorre a capacitação de pessoal das 3 FA (MB, EB, e FAB) e de agentes do GSI/PR (Abin e outros setores do Governo federal) na ENaDCiber, lotada no Forte Rondon, e localizada em Sobradinho/DF.

Anualmente, o Centro de Instrução de Guerra Eletrônica (CIGE), localizado em Sobradinho/DF, promove as especializações dos militares do EB, MB e FAB nos cursos para oficiais (Majores, Capitães e Tenentes) e praças (Subtenentes e Sargentos) de carreira com mais de 10 anos (vínculo na Força Armada) por meio do Curso de Planejamento de Guerra Eletrônica e Cibernética em Apoio às Operações.

2.4 TRABALHOS CORRELATOS NO EMPREGO MILITAR DO 5G

Estudos recentes já publicados no meio acadêmico global apontam algumas possibilidades e limitações do emprego dual das tecnologias derivadas do 5G na esfera militar, conforme descrito na Tabela 2.8 – Estudos publicados sobre emprego militar do 5G na Defesa e Segurança nacional abaixo.

Nos estudos de [124] a abordagem foca no emprego das ondas milimétricas do 5G nas comunicações militares do EEM supra 6 GHz (27 GHz, 39 GHz, 41 GHz, 72 GHz e 141 GHz) com arranjos de antenas painéis em simulações realizadas no MATLAB. Foram analisadas as alterações das comunicações dentre diversas antenas e frequências (área de cobertura, radiância, direcionalidade do lóbulo principal e atenuação do sinal em dBi) sob parâmetros de condições ambientais críticos como chuva e outras atenuações de absorção atmosférica. Constatou-se que tais fatores críticos influenciam diretamente nas áreas de cobertura e nas taxas de dados trafegados (transmitidos e recebidos) entre os rádios 5G NG usados na área do Posto de Comando da Brigada (Bda) do Exército dos EUA.

Nesse estudo de [124] são destacadas as exigências de comunicações especiais em Redes de Área Locais (LAN) militares para uma Grande Unidade (Brigada (Bda) dos EUA composta por 3.000 até 11.000 militares, tipo modular, comandada por 1 (um) Coronel do Exército dos EUA. Essa Bda é dotada de diversos sistemas: (i) inteligência; (ii) comunicações, (iii) armas; (iv) logística; (v) redes WiFi especiais contra sortidas de enxames de *drones* equipados com munições letais ou não letais, capacidades de guerra eletrônica em interferência (*anti-jamming*) e cibernética em aquisição/interceptação (*anti-hacking*); (vi) tecnologia de engodo; (vii) sistemas de navegação falsa; e (viii) sensores avançados para Inteligência, Vigilância e Reconhecimento. A Figura 2.12 ilustra o Posto de Comando de uma Brigada do Exército dos EUA no terreno abaixo.

Tabela 2.8: Estudos publicados sobre emprego dual do 5G na defesa e segurança nacional

Estudos publicados	**Citações de até 3 aplicações militares do 5G**
Em [124]	Sugere Redes Rádio Locais especiais de baixíssima área de cobertura que aumentam o sigilo; arranjos de antenas com Feixes Direcionais de alto ganho e alta eficiência energética; emprego de enxames de *drones* robôs autônomos ou semi-autônomos para ações de espionagem, vigilância, e ataques com fogos cinéticos (mísseis e bombas) e ataques eletrônicos não-cinéticos (com ondas eletromagnéticas)
Em [125]	Demonstram desde as plataformas de comunicações aéreas para as interligações dos diversos níveis de Comando e seus Comandantes (Brigada, Batalhão, Pelotão e Grupo de Combate) diferentes entre si com outros grupos de combate, aumentando-se a Consciência Situacional no Centro de Comando e melhorando o processo de Tomada de Decisões sob estresse no Campo de Batalha; propõe uso de exoesqueleto que reduz a fadiga do combatente em marchas em combate e atividades logísticas (carregamento/descarregamento) de suprimentos; e sugere a computação confiável para o C² com usos da *Blockchain*, Redes Definidas por Software (SDN) e Aprendizado Distribuído
Em [126]	Sugere a Gestão Automatizada em Bases Inteligentes para controle de estoque, separação automatizada de suprimentos, remessa automatizada dos suprimentos com *drones* com mMTC; uso da Telemedicina com URLLC; e propõe a segurança das instalações de bases com câmeras IP dotadas com Inteligência Artificial (IA) no reconhecimento automatizado de Agentes Perturbadores da Ordem Pública
Em [127]	Propõe Bases Militares Inteligentes com logística autônoma executada por robôs, veículos autônomos (terrestres, aéreos e embarcações) no ressuprimento automático no Campo de Batalha (água, sangue, ração, remédio, combustível, munição, armamentos, etc); emprego de relógios inteligentes com sensores diversos para facilitar a rotina do militar em combate (altímetro, barômetro, bússola, pedômetro, batimentos cardíacos, pressão sanguínea, GPS e ligações rádio); e sugere Redes Móveis Definidas por Software com anti-bloqueio (*anti-jamming*) e anti-aquisição (*anti-hacking*) contra enxames de *drones* dos inimigos
Em [128]	Sugere empregar as Ondas milimétricas das Faixas de Frequência (FR) 1 (410 MHz – 7.125 MHz) e (FR) 2 (24,25 GHz – 52,60 GHz) da IMT–2020 e Além para estabelecer Grandes Sedes Operacionais Destacáveis (DHQs) e Pequenas Sedes Operacionais Destacáveis, fornecendo conectividade sem fio dentro dessas áreas. Também sugere empregar Redes Não Terrestres *Non Terrestrial Networks* (NTN) permitem criar redes de comunicação universais via satélites de órbitas de Baixa Altura (*Low Earth Orbit* LEO: 1.000 km), Média Altura (*Medium Earth Orbit* MEO: 10.000 Km) e Geossíncrono (*Geosynchronous Earth Orbit* GEO: 35.838 Km) [129]
Em [130]	Colabora com a personalização para as Comunicações Críticas, voltadas para atividades de Segurança Pública e de contenção de calamidades públicas usando o Sistema IP Multimídia (IMS) com a função de Aperte-para-Falar *Push-to-Talk* (PTT) nos aparelhos móveis celulares; propõe uso de robôs controlados remotamente para atividades de risco de morte como a desativação de explosivos e de materiais cancerígenos radioativos suspeitos deixados em áreas públicas ou privadas; e sugere a integração das imagens geradas em câmeras fixadas nos uniformes dos agentes de segurança denominadas de Câmeras Corporais (*Bodycam*)

Figura 2.12: Posto de Comando de uma Brigada do Exército dos EUA no terreno [124]

Os estudos discutidos e testes do MATLAB das ondas milimétricas do EEM não licenciado abordado 50 GHz e 70 GHz, concluiu que as frequências de onda mm mais altas fornecem condições de perda de caminho significativamente melhores para enlaces de rede em Posto de Comando ou Enxame de *drone* robótico, com antenas de aberturas do sinal limitadas por uma área fixa, proporcionando o uso das antenas principais. As altas frequências das Ondas milimétricas podem oferecer oportunidades adaptativas à ocultação e vulnerabilidade (ou potencial para interferir nas proximidades redes) da rede, pois seriam úteis para outras aplicações militares de comunicações sem fio [124].

Segundo [125] os editores apresentaram conceitos inovadores do 5G, baseados em equipamentos e serviços da Internet das Coisas do Campo de Batalha (IoBT), os quais possibilitam plena realização do sensoriamento, de comunicações e de computação onipresentes, entre humanos e máquinas no campo de batalha.

Propõe uma Taxionomia de Computação Vestível dentro de 5 (cinco) campos: (i) Forças: Marinha, Exército e Força Aérea; (ii) Bem-estar: relógio inteligente, rastreador de atividades físicas e metabólicas, sensores médicos, roupas inteligentes, exoesqueleto; (iii) Computação confiável: Aprendizagem Distribuída, Aprendizagem Federada, Rede Definida por Software, Cadeia de Blocos; (iv) Consciência Situacional: Realidade Aumentada, Óculos de Visão Noturna, e Câmera Termográfica; (v) Visão e vigilância: capacete inteligente, óculos inteligente, e câmera vestível. A Figura 2.13 – A Taxonomia ilustra a Computação Vestível na Automação do Sistema de Defesa abaixo.

Ainda [125] discute como as soluções baseadas em computação vestíveis desempenham um papel importante na automação da Defesa. A automação na defesa proporciona maior agilidade no Ciclo de Tomada de Decisão dos Comandantes aliados e inimigos, influenciando diretamente nas ações futuras das tropas, porque permite que as agências de inteligência militares tomem decisões com base nas análises em tempo real, geradas pela integração de informações (voz, dados e imagens) de uma ampla gama de dispositivos vestíveis (IoBT) no Campo de Batalha.

Enfim, [125] concluiu no seu estudo sobre os desafios futuros no desenvolvimento de tecnologias vestíveis e propõe um protótipo de relógio inteligente (*Smartwatch*) com tecnologia de criptografia simétrica denominada PUF ID.

De acordo com [126] é apresentada uma visão geral das diversas tecnologias 5G e também são identificados os impactos das redes 5G nas Forças Armadas Portuguesas, baseadas nas orientações da União

Figura 2.13: Taxonomia ilustrada da computação vestível IoTB na automação de Defesa [125]

Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN), especificamente sobre os cenários desenvolvidos pelo Grupo de Cooperação Segurança das Redes e da Informação (GCSRI) e pela *NATO Communications and Information Agency* (NCIA).

Foram levantados diversos Fatores Críticos de Sucesso e Fatores Críticos de Insucesso, a fim de realizar uma Análise SWOT das informações coletadas nas entrevistas junto de autoridades militares portuguesas da Marinha, do Exército e da Aeronáutica. Nessas entrevistas eram preenchidos questionários através da plataforma *Microsoft Teams* de janeiro até fevereiro de 2020. Inicialmente estavam previstas 13 entrevistas relativas às QD, mas uma pesquisa foi anulada pois o entrevistado julgou-se incapaz. Então foram validadas 12 entrevistas no total, sendo 8 de oficiais das FA com elevadas responsabilidades no assunto (66,7%) e mais 4 de altos civis responsáveis por áreas técnica e científica (33,3%) das FA portuguesas.

Em [126] foram apresentados os resultados de sua pesquisa por meio da **Análise SWOT**[8]. Não é conhecida a origem formal da análise SWOT e alguns acreditam que esse processo de análise foi desenvolvido na década de 1960, por professores da Universidade *Stanford*, nos EUA, a partir da análise das 500 maiores empresas dos EUA, aplicado o processo de análise nas respostas obtidas de 4 Questões Principais, conforme demonstra a Figura 2.14 – Análise SWOT aplicado ao estudo de [126] abaixo:

- QD1 – Quais são as oportunidades para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?
- QD2 – Quais são as ameaças para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?
- QD3 – Quais são os pontos fortes das FFAA portuguesas para a implantação das redes?
- QD4 – Quais são pontos fracos das FFAA portuguesas para a implantação das redes 5G

Enfim, o estudo de [126] conclui sobre as Linhas de Ação a serem adotadas pelas autoridades militares e civis portuguesas para a implantação do 5G nas FFAA, pois acredita que as redes 5G irá proporcionar benefícios transversais, tanto em tempo de paz, como em missões executadas em campanha, tais como: (i) segurança física das instalações; (ii) formação e treino; (iii) manutenção de equipamentos; (iv) telemedicina; (v) operação de veículos não tripulados; (vi) comando e controlo das missões; dentre outras.

Em [127] são abordados aspectos teóricos das tecnologias 5G para uso militar global e também realiza uma comparação de velocidade de transmissão de pacotes de dados de um arquivo em uma rede móvel entre dois protocolos distintos: (i) *Low Latency Communication Ultra-Reliable (LLCUR)*; e (ii) *Data Named Design (DND)*.

O *Ebook* de [127] discorre sobre muitas tecnologias já abordadas em outros artigos científicos relativos aos 3 (três) serviços do 5G (eMBB, mMTC, e URLLC), assim como as inovações tecnológicas derivadas do 5G podem ser muito úteis no emprego dual em indústrias e cidades inteligentes, assim como nos sistemas militares no campo de batalha: (i) C^2; (ii) comunicações com ondas milimétricas e antenas inteligentes com MU-MIMO; (iii) radares de vigilância aérea, terrestre e marítima; (iv) armas coletivas e individuais

[8]Em [131] descreve que **SWOT** é uma sigla em inglês dos termos: *Strengths* (Pontos Fortes), *Weaknesses* (Pontos Fracos), *Opportunities* (Oportunidades) para o seu negócio e *Threats* (Ameaças) para o seu negócio.

Quadro 2 – Análise SWOT

O / S / W / T	Ambiente Interno	
Ambiente Externo	**PONTOS FORTES (S)** S1 - Competências e conhecimentos existentes S2 - Resiliência organizacional S3 - Cultura orientada para cumprimento da missão S4 - Existência de uma cultura de segurança	**PONTOS FRACOS (W)** W1 - Falta de recursos humanos especializados/qualificados W2 - Insuficiência de recursos financeiros W3 - Falta de consciencialização das chefias W4 - Inexistência de normas técnicas/doutrina
OPORTUNIDADES (O) O1 - Desenvolvimento de aplicações 5G específicas para as FFAA O2 - Edificação de redes 5G privadas O3 - Operação remota de veículos e equipamentos O4 - Caraterísticas da tecnologia 5G	**CRESCIMENTO** SO1 - **CRIAR** cenários de emprego operacional do 5G nas FFAA (S1, S2, S3) x (O1, O2, O3) SO2 - **CONSOLIDAR** a interoperabilidade 5G nas FFAA e com os países aliados (S1, S2, S4) x (O1, O2, O3, O4)	**OTIMIZAÇÃO** WO1 - **CONSTITUIR** grupos de acompanhamento especializados em 5G (W1, W3, W4) x (O1, O4) WO2 - **ADEQUAR** os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações (W1, W2) x (O2, O4)
AMEAÇAS (T) T1 - Interferência de Estados Terceiros T2 - Tecnologia disruptiva/ imaturidade da tecnologia T3 - Ciberataques e cibercriminalidade T4 - Fraca qualidade dos produtos	**DINAMIZAÇÃO** ST1 - **ENVOLVER** as chefias no processo de implantação do 5G nas FFAA (S2, S3, S4) x (T2) ST2 - **EXPLORAR** a utilização segura de redes 5G próprias (S1, S2, S4) x (T1, T3, T4)	**PROTEÇÃO** WT1 - **POTENCIAR** a formação em cibersegurança/ciberdefesa e a especialização em 5G (W1, W2, W3, W4) x (T1, T3, T4) WT2 - **PROMOVER** a evolução sustentada das soluções tecnológicas 5G (W2) x (T3, T4)

Figura 2.14: Análise SWOT aplicado ao estudo de [126]

inteligentes; (v) controle logístico e ressuprimento automatizados; (vii) saúde e resgate autônomo; (viii) equipamentos vestíveis; (ix) munições leves e pesadas inteligentes; (x) exo-esqueleto; (xi) simuladores com Realidade Aumentada e Realidade Virtual para simulação e para treinamento; (xii) enxames de *drones* para: vigilância, ataque eletrônico/ataque cibernético, ataque cinético, reconhecimento, busca e salvamento.

O estudo de [127] concluiu demonstrando um incremento de 23,8% de velocidade na transmissão de pacotes TCP e UDP usando o algoritmo de Comunicação Ultra Confiável de Baixa Latência (*Low-Latency Communication Ultra-Reliable* (LLCUR)) com taxa de 95% de velocidade de rede, 90% de eficiência na transferência em 32 milisegundos para transmissão de pacotes de arquivos na ordem de 40 Gbits, sobre o protocolo Projeto de Dados Nomeado (*Data Named Desig* (DND)) com taxa de 76,19% de velocidade de rede em 42 milisegundos para transmissão de pacotes de arquivos na ordem de 40 Gbits. Ou seja, esse ganho significativo nas redes militares de C², poderia reduzir o número de mortes no Teatro de Operações devido ao incremento da velocidade no tráfego de mensagens por meio do algoritmo da LLCUR em substituição a outros algoritmos de comunicação como o DND. A Figura ilustra o resultado do teste comparativo entre os algoritmos DND x LLCUR em uma rede militar na transferência de 40 Gbits de dados 2.15 abaixo.

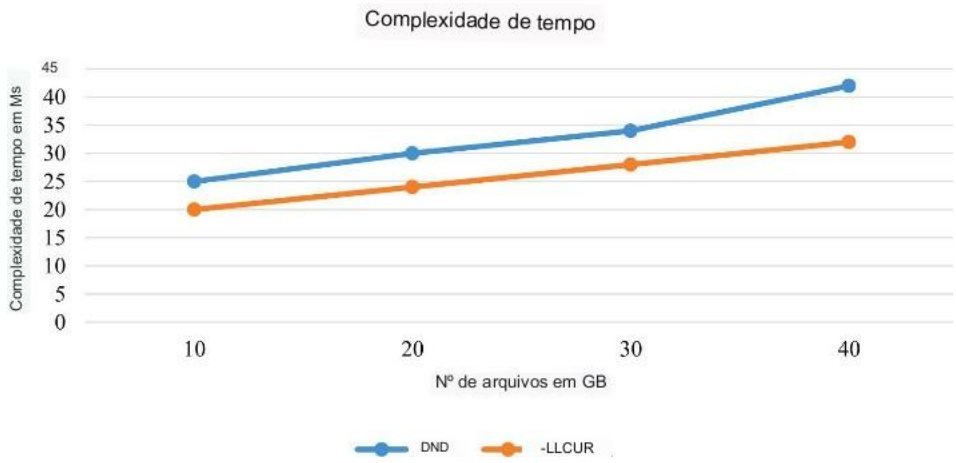

Figura 2.15: Resultado do teste comparativo entre os algoritmos DND x LLCUR em uma rede militar na transferência de 40 Gbits de dados [127]

De acordo com [128], sugere-se empregar as Ondas Milimétricas (*mmWaves*) das Faixas de Frequência (FR) 1 (410 MHz – 7.125 MHz) e (FR) 2 (24,25 GHz – 52,60 GHz) informadas nos lançamentos R-15 e R-16 da **IMT–2020 e Além**, a fim de aumentar a Seg Com nos cenários propostos:

(i) estabelecer Centros de Integração de Sistemas (CIS) em Grandes Sedes Operacionais Destacáveis (*Large Operational Deployable Headquarters* (DHQs)) com uma célula 5G privada tipo WMAN de alta capacidade operando em frequências de 26 GHz (uma banda de frequência harmonizada da OTAN) implantada como um sistema Ponto a Multiponto (PTMP) de Acesso sem Fio Fixo (FWA) e também em Pequenos DHQs Operacionais com um sistema 5G privado de alta capacidade e camada única fornecendo conectividade WMAN e Rede Local sem Fio (WLAN) combinada na banda de frequência 5G Sub-6 GHz (média), idealmente em a banda de 4,4 — 5,0 GHz muitas vezes referida como Banda IV da OTAN, fornecendo capacidade e flexibilidade. A conectividade sem fio dentro dessas áreas emprega conjuntos de antenas MIMO massivo muito grandes combinadas com tecnologias de formação de Feixes Direcionais (*Beamforming*), as quais aumentam significativamente o desempenho do 5G NR com altas taxas de descarregamento (*download* DL) e carregamento (*upload* UL) em relação aos sistemas tradicionais, conforme demonstra a Figura 2.16 – Grande Sede Operacional Destacável (DHQ) abaixo;

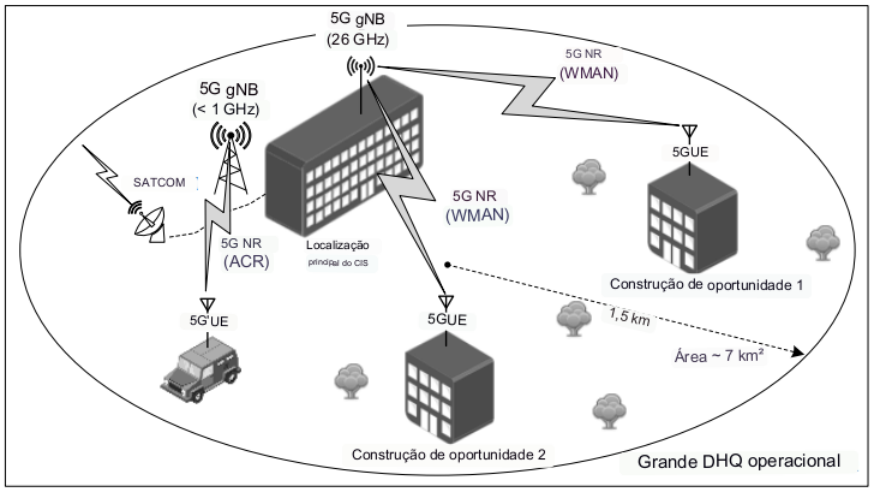

Figura 2.16: Grande Sede Operacional Destacável (DHQ) [128]

(ii) Operações Marítimas exigem comunicações navais de proximidade em condição de Linha de Visão de Rádio (LOS) e consideram o uso de sistemas 5G de alto desempenho para aprimorar a conectividade Navio – Navio, Navio – Anfíbio e Navio – Costa, com sistemas de comunicações de baixa latência e alta capacidade para Satélite Tático Nominal (TACSAT), comunicações marítimas nominais de retransmissão de sub-rede e Redes Rádio de Combate (CNR). Para o cenário da Força Tarefa Naval um sistema 5G é proposto para fornecer comunicações Navio – Navio com frequências Sub-6-GHz (média e baixa, por exemplo 2,3 GHz e 3,6 GHz) baseado na tecnologia 5G IAB NR, conforme demonstra a Figura 2.17 – Cenário 5G da Força Tarefa Naval a seguir.

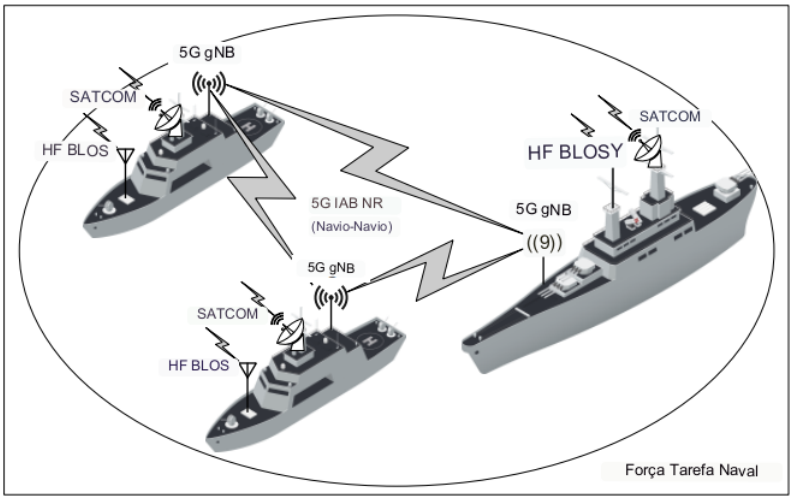

Figura 2.17: Cenário 5G da Força Tarefa Naval [128]

(iii) Operações Táticas Terrestres Multinacionais ocorrem quando as Brigadas (Bda) abordam o uso de sistemas 5G para fornecerem conectividade sem fio aumentada em níveis táticos para os seus escalões abaixo (Batalhão e Companhia), como uma solução prática para comunicações táticas de banda larga interoperáveis em situações benignas no uso de Rede Não Terrestre via comunicação satelital de baixa altura (LEO), conforme demonstra a Figura 2.18 – Cenário de Operações Táticas Terrestres

com Rede Não Terrestre a seguir.

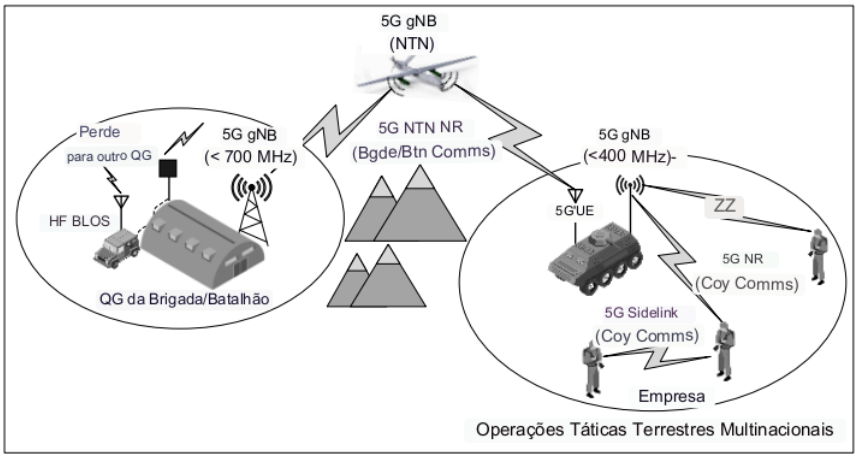

Figura 2.18: Cenário de Operações Táticas Terrestres com Rede Não Terrestre [128]

Da Fig 2.18 observa-se que a Viatura Blindada de Transporte de Pessoal (VBTP) é um Posto de Comando Tático Móvel, e realiza a extensão da cobertura da célula da Brigada/Batalhão no terreno mais à frente, no segundo nível com uma célula 5G tática na banda Sub-1 GHz na extremidade superior da banda UHF da OTAN de 400 MHz, fornecendo comunicações e outros serviços para tropas móveis equipadas com terminais móveis táticos 5G do tipo 5G *Sidelink*. Assim esses serviços de aumento da célula de banda larga de comunicações móveis complementam as CNR em condições de Guerra Eletrônica (EW) amigas, aprimorando-se a consciência situacional e os serviços funcionais até o soldado desembarcado mais distante da VBTP.

(iv) Comunicações Estáticas são delimitadas em 2 cenários usando o 5G com Infraestrutura interna de TI e Conectividade WAN de retrocesso/reuso. No primeiro caso usando a Infraestrutura interna privada do 5G é proposta para fornecer distribuição de WLAN em locais militares estáticos. Logo, um sistema WLAN baseado em 5G de alta capacidade nas bandas de frequência não licenciadas nas subfaixas não licenciadas de 5,0 GHz (com regulação diferente em cada país da OTAN) criam redes corporativas para os dispositivos da WLAN em um QG estático da OTAN. No segundo caso do cenário de WAN com conectividade por retrocesso/reuso a infraestrutura 5G pública é proposta para fornecer conectividade de rede de longa distância (WAN) com reuso para a sede estática da OTAN, se houver falha na conexão nominal momentaneamente indisponível. Logo uma fatia da rede de um 5G MNO é usada para fornecer conectividade WAN de retorno à Internet quando a conectividade WAN nominal não estiver disponível e para manter o tráfego de alta prioridade durante esses períodos, conforme demonstra a Figura 2.19 – Conectividade com 5G WAN Alternativa abaixo.

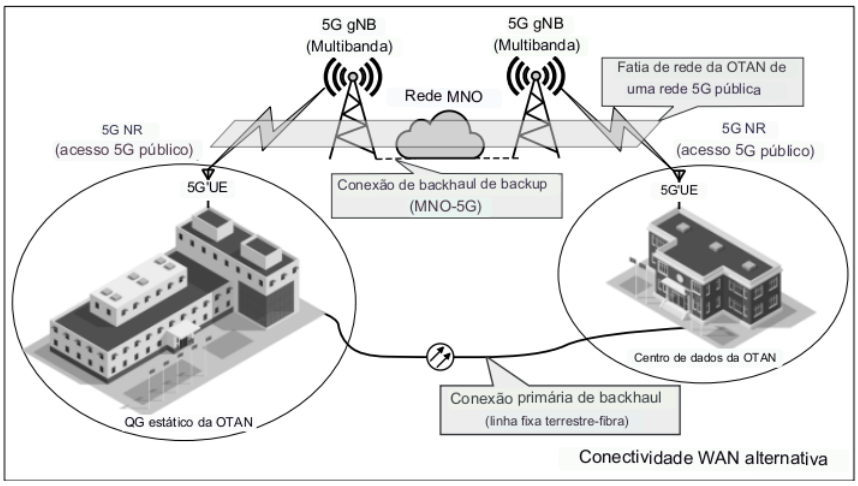

Figura 2.19: Conectividade com 5G WAN Alternativa [128]

Por todo o exposto, deduz-se que as tecnologias desenvolvidas para o 5G podem estimular ainda mais seu emprego na esfera militar nos próximos anos. Em que pese a necessidade de estudos mais detalhados por causa dos desafios técnicos intrínsecos na pesquisa, no desenvolvimento, na produção industrial, na adoção pelas FA e na implantação de novos produtos e serviços derivados do 5G para sistemas de defesa de cada país adotante.

O estudo de [130] aborda uma arquitetura 5G Rádio de Acesso à Rede (5G *(Radio Access Network* (5G RAN)) por meio das Redes Definidas por Software (SDN) em multicamadas de Virtualização das Funções de Rede (NFV), sendo que cada camada independente tem potência de transmissão e área de cobertura diferente das demais outras camadas nas Redes Heterogêneas *HetNets*).

O uso do EEM do 5G brasileiro (Bandas: 700 MHz; 2,3 GHz; 3,5 GHz; e 26 GHz) possibilitarão diversas funcionalidades nos 3 serviços (eMBB, mMTC e URLLC) típicos no emprego tático do 5G para as Comunicações Críticas. Por meio da cobertura 5G em uma determinada região que necessite de Comunicação Crítica, para obter alta taxas de dados, como emprego de equipamentos de segurança, de busca e de salvamento, conforme citado por [130]. Por exemplo: (i) *drones*; (ii) captação de vídeos analíticos ao vivo com câmeras IP e *drones*; (iii) viaturas de resgate autônomas; (iv) automação de dispositivos policiais; (v) robôs conectados com o Centro de C² para executar remotamente atividades de risco de morte humana para a desativação de explosivos ou coleta de artefatos químicos, biológicos e nucleares; (vi) realizar a Inteligência de Imagens; (vii) realizar aplicações de Inteligência Artificial; e (viii) realizar a integração de imagens geradas por câmeras fixadas nas vias públicas e também por câmeras instaladas nos uniformes dos agentes de segurança pública em câmeras corporais (*Bodycams*).

O estudo de [130] destaca e conclui que o 5G proporcionará maior interoperabilidade, confiabilidade, segurança e disponibilidade de comunicações efetivas, para o Sistema Nacional de Comunicações Críticas (SISNACC) do Brasil, o qual envolve o emprego das Forças Armadas (MB, EB e FAB), dos Órgãos de Segurança Pública (PM, BM, PF, PRF, Pol Civ, Guarda Nacional, etc), dos Órgãos de Fiscalização (IBAMA, Receita Federal do Brasil, etc) e da Defesa Civil para situações críticas em desastres naturais.

Por todo o exposto acima, conclui-se que o emprego militar do 5G é possível de ser realizado em diversos cenários voltados para ações de Defesa nacional e também de Segurança pública.

3 PROPOSTA CONCEITUAL DE ARQUITETURA DE 5G TÁTICO PARA O EXÉRCITO BRASILEIRO EMPREGAR NA DEFESA E SEGURANÇA NACIONAL

3.1 CONTEXTUALIZAÇÃO

3.1.1 Situação Geral

O Sistema de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA) prevê a confecção e a guarda segura de todos os Planos de Emprego Conjunto das Forças Armadas (PCEFA) e dos Planos Operacionais elaborados pelas FA (MB, EB e FAB). Todos esses planos regulam os empregos das OM e das frações das tropas no território brasileiro e, excepcionalmente, em territórios estrangeiros, para o resgate de cidadãos brasileiros em situação vulnerável ou risco de morte, no caso o país migrado entrar nas situações de Confronto Armado ou de Guerra segundo [39].

Na realidade brasileira atual, as FA (MB, EB, e FAB) podem ser empregadas na defesa externa e na segurança interna, atuando contra forças militares externas presentes nas Faixas de Fronteiras Terrestre e Marítima, e contra forças paramilitares internas, que podem tentar desestabilizar o Governo Federal, e contra Organizações Criminosas (OrCrim) que podem determinar atos terroristas contra instituições do Estado Brasileiro. Desde que emitidos decretos pelo Presidente da República com o apoio do Congresso Nacional para:

(i) **Estado de Defesa** – Art 136 da [61], cujo prazo pode ser de até 30 dias, sendo prorrogado única vez por igual período de 30 dias, caso persistam as razões que justificam a decretação, limitado aos locais restritos e determinados definidos no decreto presidencial;

(ii) **Estado de Sítio** – Art 137 [61] cujo prazo pode ser de 30 dias, sendo prorrogado por diversas vezes por igual período de 30 dias, caso persistam as razões que justificam a decretação, limitado a todo o território brasileiro; e

(iii) **Operações de GLO** – Lei Complementar (LC) nº 97, de 9 de junho de 1999 [69], alterada pela LC nº 117, de 2 de setembro de 2004 [132], e pela LC nº 136, de 25 de agosto de 2010 [133].

Das assertivas acima e da Figura 3.1 acima, deduz-se que as políticas externa e de defesa devem ser conjuntas e complementares, se possível indissociáveis [51]. Considerando-se ações simultâneas do Ministério das Relações Exteriores (MRE) e do Ministério da Defesa (MD) por meio da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo [134], busca-se a manutenção da estabilidade nacional, da estabilidade regional e a construção de um ambiente internacional mais cooperativo é de grande interesse para o Brasil [67].

Outra forma de emprego das FA brasileiras foi para realizar a defesa e a segurança nacionais nos **Grandes Eventos** [135]. O EB foi empregado ativamente na segurança das capitais brasileiras nos Grandes

Eventos, com emprego maciço de tropas na segurança pública das vias de acesso e nas cidades sedes dos jogos e competições desportivas, tais como: (i) Jogos Pan-Americanos de 12 a 29 de julho de 2007; (ii) Jogos Mundiais Militares de 16 a 24 de julho de 2011; (iii) Conferência Rio +20 de 13 a 22 de junho de 2012; (iv) Copa das Confederações de 15 a 30 de junho de 2013; (v) Jornada Mundial da Juventude de 23 a 28 de julho de 2013; (vi) Copa do Mundo de 12 de junho a 13 de julho de 2014; Jogos Olímpicos de 3 a 21 de agosto de 2016; e Jogos Paralímpicos de 7 a 18 de setembro de 2016.

Houve um retorno muito positivo para as FA na participação dos Grandes Eventos no Brasil, devido aos investimentos financeiros vultuosos do Governo Federal, na ordem de bilhões de reais diretos para a modernização dos Meios de Emprego Militar (MEM), no desenvolvimento da Indústria Nacional de Defesa (IND) e também na atualização da Doutrina Militar de Op GLO.

Na época dos Grandes Eventos, ocorridos entre julho de 2007 e setembro de 2016, o governo brasileiro e as diversas operadoras de telefonia móvel privadas realizaram investimentos financeiros no modo de parcerias público-privadas, que culminaram com as implantações de diversas infraestruturas de telecomunicações móveis civis dos sistemas 4G-LTE e 4.5G*LTE-Advanced*.

O EB também implantou alguns sistemas de comunicações militares para atender aos Grandes Eventos, por meio do Comando de Comunicações e Guerra Eletrônica do Exército (C Com GE Ex) [135], foram mobiliados nas capitais dos Grandes Eventos: (i) Sistema Rádio Digital Troncalizado (SRDT) APCO25 da empresa norte-americana Motorola; e (ii) Sistema Estratégico de Comunicações (SEC) da empresa norte-americana Harris.

Ambos sistemas de Com possibilitaram melhorias no Comando e Controle (C^2), na Consciência Situacional (CS) e nas Comunicações (Com) das tropas empregadas nas missões de defesa e segurança públicas dos Grandes Eventos.

Realmente os sistemas de Com tipo SRDT (Motorola) e SEC (Harris) foram empregados de forma dual – civil e militar – pois conseguiram realizar perfeitamente a integração das diversas agências governamentais (Defesa civil, Receita Federal Brasileira, IBAMA, entre outras), das forças policiais do Ministério da Justiça (MJ) (Polícia Federal (PF), Polícia Rodoviária Federal (PRF) e Força Nacional (FN)) junto das Forças Singulares MB, EB e FAB, por meio dos Centros de Gerenciamento de Crises estabelecidos nas cidades-sedes dos Grandes Eventos [135].

O Estado-Maior Conjunto das Forças Armadas (EMCFA), do Ministério da Defesa (MD) coordenou todas as ações em prol da segurança pública e da defesa durante as atividades dos Grandes Eventos, conforme descrito em [135]. É por meio dessas ações estratégicas e operacionais que o MD promove o desencadeamento das operações militares táticas no Brasil e, raramente, no Mundo, por meio de: (i) Diretrizes Ministeriais; (ii) Diretrizes do Estado-Maior Conjunto das Forças Armadas (EMCFA); e (iii) Planos Estratégicos Conjuntos das Forças Armadas (PECFA), conforme exemplifica a Figura 3.1 – Níveis de Segurança e Instrumentos Estatais de Defesa abaixo.

<table>
<tr><th rowspan="2">ÂMBITO</th><th colspan="3">SEGURANÇA</th><th colspan="3">INSTRUMENTOS ESTATAIS DE DEFESA</th></tr>
<tr><th>NÍVEL</th><th>DIMENSÃO</th><th>INTERESSES</th><th>COERCITIVOS</th><th colspan="2">NÃO COERCITIVOS</th></tr>
<tr><td rowspan="3">Interno</td><td>Individual</td><td rowspan="2">Pública</td><td>Direitos e Garantias Individuais</td><td rowspan="2">Órgãos de Segurança Pública (Poder de Polícia) e
FA (casos previstos em lei)</td><td rowspan="2">FA (atribuições subsidiárias)</td><td rowspan="3">Outros organismos e instituições do Estado</td></tr>
<tr><td>Comunitário</td><td>Grupais setoriais</td></tr>
<tr><td>Nacional</td><td>Nacional</td><td>Objetivos Nacionais</td><td>FA</td></tr>
<tr><td>Externo</td><td>Coletivo</td><td>Internacional</td><td>Objetivos vitais do conjunto de nações (coincidentes com o interesse nacional)</td><td>FA coligadas sob a égide de um Órgão de Segurança Coletiva</td><td>FA (ajuda humanitária)</td></tr>
</table>

Figura 3.1: Níveis de Segurança e Instrumentos Estatais de Defesa [70]

O MD quando determina o emprego do Exército Brasileiro (EB), é o Órgão de Direção Operacional (ODOp) denominado Comando de Operações Terrestres (COTER), o responsável direto por planejar, coordenar e executar o Preparo e o Emprego das diversas tropas operacionais da Força Terrestre (F Ter) [136], seja no emprego no território brasileiro, seja quando necessário para a proteção e/ou resgate de brasileiros emigrantes nos territórios estrangeiros.

O Comandante do COTER participa da Reunião do Alto Comando do Exército (RACE), sendo responsável pela gestão dos recursos públicos federais destinados para o **Preparo** e **Emprego da F Ter**. O Comandante do COTER também assessora o Comandante do Exército nas situações de anormalidades político-militares. Ambos órgãos ODOp e Gab Cmt Ex estão lotados no Forte Caxias Quartel General do Exército (QGEx), situado no SMU, no DF [136].

De acordo com [67] descreve a função primordial do EB:

> **Cabe ao Exército o preparo da Força Terrestre** para cumprir sua missão constitucional da defesa da Pátria e da garantia dos poderes constitucionais, da lei e da ordem. Além disso, como atribuição subsidiária geral, deve cooperar com o desenvolvimento nacional e com a Defesa Civil. Deve, ainda, apoiar a política externa do País e participar de operações internacionais. (Grifo nosso)

A **Força Terrestre (F Ter)** é o instrumento de ação do EB mais conhecido como **Braço Forte**, necessário para cumprir as missões e tarefas de defesa da Pátria, manutenção dos poderes constitucionais e garantia da lei e da ordem, conforme demonstra a Figura 3.2 – Componentes do Poder Terrestre brasileiro abaixo.

No emprego da F Ter poderão ser mobiliados até 8 Centros de Coordenação de Operações (C C Op) e, caso necessário também até 8 Centros de Coordenação de Operações Móvel (C C Op Mv).

A fim de atender às atividades e às ações do C4ISTAR (Comando e Controle, Comunicações, Inteligência, Computador, Vigilância, Aquisição de Alvos e Reconhecimento) durante o transcurso das operações terrestres, facilitando o Processo de Tomada de Decisão do Comandante Militar de Área (Cmt Mil A) empregado na operação.

Ambos C C Op e C C Op Mv são dotados de diversos meios de TIC e contam com equipes de militares especializados e organizados em células de Estados-Maiores (EM) ou células de Comandos Conjuntos (C

Figura 3.2: Componentes do Poder Terrestre brasileiro denominado Braço Forte [136]

Cj), estas últimas quando participam militares das outras Forças Singulares da MB e/ou FAB juntamente do EB nos C C Op ou C C Op Mv.

No caso específico do CMP, é o único C Mil A comandando por um General de Divisão e não por um General de Exército. O C Op realiza a mesma função do C C Op, enquanto que o C Op Mv realiza a função do C C Op Mv. As imagens dos C Op e do C Op Mv do CMP estão na Figura 3.3 – C Op/CMP e na Figura 3.4 – C Op Mv da 6ª Cia Com a seguir.

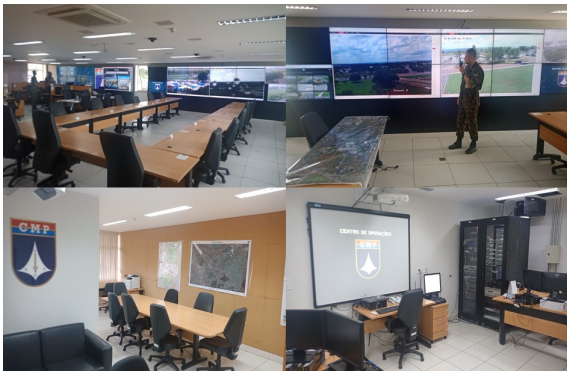

Figura 3.3: Centro de Operações (C Op) do CMP [74]

Figura 3.4: Centro de Operações Móvel (C Op Mv) do C Op Esp [137]

Todos estes Centros Operacionais podem ser apoiados diretamente pelo MD, com quaisquer outros meios do SisMC² formado pelos seus subsistemas orgânicos de C² instalados no MD e nos Grandes Comandos das FA (MB, EB e FAB) [70]: (i) Rede Operacional de Defesa (ROD); (ii) Sistema de Planejamento de Operações Militares (SIPLOM); (iii) Sistema Tático de Enlace de Dados (SISTED); (iv) Sistema de Comunicações Militares por Satélite (SISCOMIS); e (v) Satélite Geoestacionário de Defesa e Comunicações Estratégicas 1 (SGDC-1).

3.1.2 Situação Particular

Inicialmente essa pesquisa científica realizaria uma proposta de arquitetura com 3 (três) sistemas eletrônicos baseados na tecnologia dual – civil e militar – do 5G para emprego na defesa e segurança nacional, sob domínio do EB, na área central de Brasília/DF, considerada área estratégica pelo GSI/PR, a saber: (i) Esplanada dos Ministérios; (ii) Palácio do Planalto; (iii) Congresso Nacional; (iv) Palácio da Justiça; (v) Palácio da Alvorada; (vi) Palácio do Jaburu; (vii) Granja do Torto; e (viii) outras áreas específicas do Entorno do DF, as quais detém as vias de acesso rodoviárias para entrada/saída do Plano Piloto de Brasília/DF.

No entanto, após o período eleitoral presidencial ocorrido nos mês de outubro de 2022, diversos grupos de pessoas se aglomeraram, estacionaram e acamparam defronte aos diversos C Mil A do EB, nas diversas capitais brasileiras para manifestarem contra o resultado da eleição presidencial de 2022.

Muitas dessas pessoas permaneceram no último bimestre de 2022 clamando por uma possível Intervenção Militar, a qual não ocorreu devido ao fiel cumprimento do ordenamento jurídico previsto na CRFB/88 [61] pelo ex-Presidente da República, garantindo a passagem sem óbices do cargo e os comandos do Governo Federal e das Forças Armadas para o atual Presidente da República.

Especificamente, no DF, cerca de 5 mil pessoas manifestantes se aglomeraram na Praça Cívica, local mais conhecido como Praça dos Cristais, situado defronte ao Forte Caxias Quartel General do Exército (QGEx) no SMU, no DF.

Ressalta-se que foi permitida a permanência pacífica dos manifestantes na Praça Cívica no período desde 31/10/2022 até 08/01/2023, fundamentada no Art. 5 da CRFB/88, amparado pelo inciso XVI citado a seguir [61]:

> XVI – todos podem reunir-se pacificamente, sem armas, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso à autoridade competente.

Diariamente o Batalhão de Polícia do Exército de Brasília (BPEB) realiza patrulhamentos motorizado e à pe nas vias de acesso aos aquartelamentos e vias de acesso das Vilas Militares lotados no SMU. Além disso, o BPEB também controla o trânsito das principais vias de acesso ao SMU com suas frações escaladas de serviço diário: (i) Av. do Exército; (ii) Av. Duque de Caxias; e (iii) Av. Guararapes. Conforme exemplifica a Figura 3.5 -– Áreas estratégicas do SMU abaixo.

Figura 3.5: Áreas estratégicas do SMU [74]

Da análise das informações da Figura 3.5, pode-se identificar os Objetivos para defender, proteger e vigiar presentes nas áreas estratégicas do SMU, descritas a seguir:

1. Objetivo I – Área do estacionamento de veículos pequenos ao S do QGEx, identificada pela área (I) de cor azul (O1);
2. Objetivo II – Praça Cívica, identificada pela área (II) de cor vermelha (O2);
3. Objetivo III – Área de Acampamento adjacente à VMG, identificada pela área (III) de cor bege (O3);
4. Objetivo IV – Área de estacionamento de veículos grandes ao N do QGEx, identificada pela área IV de cor verde escura (O4);
5. Objetivo Forte Caxias Quartel-General do Exército – identificado pela inscrição QGEx de cor vermelha (O5);
6. Objetivo Quartel-General do Comando Militar do Planalto/Quartel-General do Comando da 11ª Região Militar – identificado pela inscrição QG Cmdo CMP/11ª RM na cor azul marinho (O6);
7. Objetivo Vila Militar dos Oficiais-Generais – identificada pela inscrição VMG na cor verde (O7); e
8. Objetivo das Vias de Acesso ao SMU – identificado pelas setas azuis com bordas vermelhas com as inscrições Av. do Exército, Av. Duque de Caxias e Av. Guararapes (O8).

3.2 PROPOSTA DE UMA ARQUITETURA CONCEITUAL 5G PARA EMPREGO MILITAR

De acordo com [65] as **Informações** são os insumos fundamentais para o **Processo de Tomada de Decisão do Comandante**, no qual se baseia na velocidade do Ciclo de C² definido pelas ações de "**Observar, Orientar, Decidir e Atuar**" (OODA) (Grifo nosso), conforme demonstra a Figura 3.6 – Ciclo de Inteligência Militar (Ciclo OODA) a seguir.

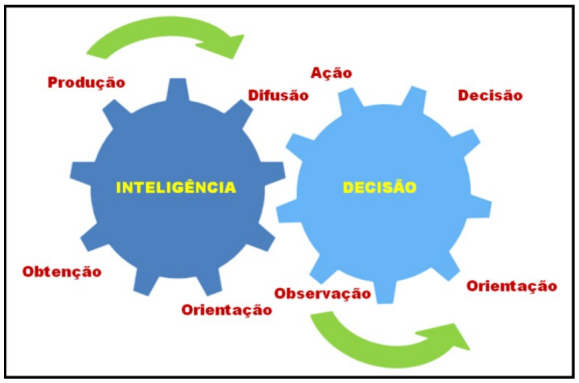

Figura 3.6: Ciclo de Inteligência Militar – Ciclo OODA [65]

Em primeiro plano, ressalta-se que não importa qual tecnologia é usada para trafegar as Informações, pois o mais importante é a informação entrar/sair na área de operações e chegar/partir do decisor com oportunidade [39]. O canal de comunicação diversas vezes pode empregar meios de Com menos seguros, porém mais rápidos a fim de tornar o Ciclo OODA amigo mais rápido possível e superior ao Ciclo OODA inimigo [43].

A finalidade principal do Sistema de Vigilância Eletrônica com câmeras IP do C Op/CMP e do Sistema de Monitoramento Eletrônico aéreo e automatizado com *drone* é proporcionar o acompanhamento das ações dos militares durante os serviços diuturnos de escala das OM do CMP realizados no SMU para salvaguardar a área sob jurisdição militar[1].

Em segundo plano, ambos sistemas eletrônicos de Vigilância e de Monitoramento também serviram para observar as atividades realizadas pelos manifestantes, vendedores ambulantes e transeuntes que surgiram na Praça Cívica (Cristais), na Av. do Exército, acampamentos e estacionamentos, durante as aglomerações de pessoas e veículos usados nas manifestações populares ocorridas no último bimestre de 2022.

Ressalta-se que o principal item da Arquitetura Conceitual de emprego militar do 5G neste trabalho é o Sistema de Comunicações 5G embarcado em uma viatura civil tipo Mercedes Benz Sprinter 413, pintada na cor branca, descaracterizada como Material de Emprego Militar, que normalmente é pintado na cor verde-oliva ou com cores do camuflado do EB.

Esse Sistema de Comunicações 5G Móvel Tim foi denominado como **Sistema 5G Tático EB** pode ser empregado tanto em operações reais na Faixa de Fronteira (e.g. Op Ágata e Op Verde Brasil) amparada

[1]De acordo com o PARECER nº 00484/2019/CONJUR-MD/CGU/AGU, de 5 de julho de 2019 [138], baseado no Decreto-lei nº 3.437, de 17 de julho de 1941 [139], ambos documentos traçam os limites da ingerência do poder militar em regiões contíguas às fortificações militares num raio máximo de 1.320 m do imóvel militar.

pelo Art. 20 da [61], quanto em operações reais em ambiente urbano e semi-urbano tipo Intervenção Federal amparada pelo Art. 34 da CRFB/88 [61], bem como em operações tipo GLO, amparada pela lei Complementar nº 97/1999 [69].

Caso o C Op/CMP resolvesse implementar os 3 sistemas eletrônicos no SMU permanentemente, há uma série de legislações, projetos técnicos para adequação e a solicitação das necessidades de recursos financeiros por meio do Escritório de Projetos (EPEx), do EME, e da Agência de Gestão e Inovação Tecnológica (AGITEC) do Departamento de Ciência e Tecnologia (DCT) do Exército.

As necessidades das FA devem seguir para o MD, que poderá solicitar os recursos financeiros via portaria interministerial ou via emenda parlamentar. Ambas seriam incluídas na Lei Orçamentária Anual (LOA), a qual é votada no Congresso Nacional brasileiro (CN). Somente assim o MD poderia repassar os recursos financeiros para as FA usarem em suas pesquisas científicas, nas atividades do Preparo e, principalmente, nas atividades do Emprego, realizando operações militares das FA (MB, EB, e FAB) no Brasil.

A seguir serão descritos os 3 sistemas eletrônicos de comunicações com detalhes, sem maiores aprofundamentos técnicos de implantação, **visto que a proposta do emprego militar do 5G neste trabalho é puramente conceitual**. Mas todos os 3 sistemas eletrônicos funcionaram com eficiência, eficácia, e efetividade[2] nas áreas estratégicas do SMU, sob supervisão do C Op/CMP.

3.2.1 Sistema de Vigilância Eletrônica com câmeras IP

O Sistema de Vigilância Eletrônica do C Op/CMP é formado por:

- 1 (um) Servidor com *software* de gerenciamento de imagens digitais tipo *Videowall* e mais 24 (telas) telas de 60 polegadas no interior do Salão do C Op/CMP;
- 2 (duas) câmeras Hikivision Full HD IP com controle remoto, para permanecerem fixas: (i) na torre metálica no telhado N do Cmdo CMP; e (ii) em cima da caixa d'água do Batalhão da Guarda Presidencial (BGP);
- 2 (duas) câmeras Hikivision Full HD IP com controle remoto, instaladas nos mastros pneumáticos dos 2 (dois) Módulos de Telemática Operacional (MTO) da 6ª Cia Com, a fim de flexibilizar o emprego imediato em torno das áreas estratégicas do SMU que não dispunham da cobertura visual proporcionada pelas 2 (duas) câmeras fixas (CMP e BGP); e
- 2 (duas) viaturas MTO Marruá, as quais podiam ser deslocadas para quaisquer áreas de interesse do SMU.

Observe o Croqui do Sistema de Vigilância Eletrônica do C Op/CMP segundo ilustrado na Figura 3.7 abaixo.

[2]Em [140] explica esses 3 conceitos: (i) **eficiência** é a qualidade de um sistema conseguir executar as tarefas considerando-se seus custos e recursos humanos disponíveis, cuja palavra chave é "Recursos"; (ii) **eficácia** é a qualidade de um sistema realizar completamente todas as etapas planejadas de um processo, cuja palavra chave é "Resultado"; e (iii) **efetividade** é a qualidade resultante da eficiência e eficácia de um sistema que garante o serviço, produto ou cargo, cuja palavra chave é "Impacto".

Figura 3.7: Croqui do Sistema de Vigilância Eletrônica do C Op/CMP no SMU [74]

Para implementar o Sistema de Vigilância Eletrônica no SMU, o C Op/CMP estabeleceu uma rede rádio digital exclusiva com acesso à EBNet, onde todos os enlaces de comunicações para interligação do Servidor do *Videowall* e suas 24 (vinte e quatro) telas de 60' com as 4 (quatro) câmeras *Hikivision Full HD IP* dispostas no terreno do SMU, foi realizada por meio de 4 (quatro) Rádios Definidos por Software (RDS) da empresa Motorola, modelo PTP 450 (Per to Per), na modalidade de conexão ponto a ponto (P2P) com tráfego limitado a 50 Mbps, comunicação *fullduplex*, na banda de frequências de 3.500 MHz a 3.750 MHz, com canais configurados com espaçamentos de 10 MHz, tais como:

- Câmera 1 fixa nos canais 3.550 Mhz (principal) e 3.560 MHz (reserva);
- Câmera 2 fixa nos canais 3.570 Mz (principal) e 3.580 Mhz (reserva); e
- Câmera móvel 1 nos canais 3.590 Mz (principal) e 3.600 Mhz (reserva); e
- Câmera móvel 2 nos canais 3.610 Mz (principal) e 3.620 Mhz (reserva).

Os componentes internos compostos pelo Servidor e telas do *Videowall* do Sistema de Vigilância Eletrônica do C Op/CMP podem ser visualizados na Figura 3.3 – C Op/CMP presente acima na **3.1 CONTEXTUALIZAÇÃO**.

Enquanto que os componentes externos compostos pelas Viaturas Módulo de Telemática Operacional (MTO) (com mastros pneumáticos e geradores internos) e as câmeras IP podem ser visualizados na Figura 3.8 – Sistema de Vigilância Eletrônica com 2 (duas) câmeras fixas (CMP e BGP) e 2 (duas) câmeras móveis (MTO da 6ª Cia Com) no SMU abaixo.

Figura 3.8: Sistema de Vigilância Eletrônica com 2 (duas) câmeras fixas (CMP e BGP) e 2 (duas) câmeras móveis (MTO 6ª Cia Com) no SMU [74]

A EBNet é a rede de comunicação corporativa desenvolvida e operada exclusivamente pelo EB. É utilizada para realizar o tráfego de dados, voz sobre IP (*VoIP*) e imagens, por meio da interconexão com o Sistema Nacional de Telefonia (SNT), com a Rede Integrada de Telefonia do Exército (RITEx) com protocolos de segurança próprios [141] e também com o Sistema Militar de Comando e Controle (SisMC²).

Esse Sistema de Vigilância Eletrônica operava na Rede de Acesso Local (LAN) **10.133.136.0/28**, tipo Classe A, em modo exclusivo na **EBNet**, conforme demonstra a Tabela 3.1 – Parâmetros da Rede, dos Equipamentos e os IP utilizados no Sistema de Vigilância Eletrônica do C Op/CMP abaixo.

Tabela 3.1: Parâmetros da Rede, dos Equipamentos e os IP utilizados no Sistema de Vigilância Eletrônica do C Op/CMP

Parâmetros/Equipamentos	**Endereços IP**
Máscara da Rede	255.255.255.240 ou /28
Quantidade de Subredes/Clientes	16/16
Endereço da Rede (*Gateway*)	10.133.136.0/28
Endereço de Difusão (*Broadcast*)	10.133.136.15/28
1ª Faixa de IP disponíveis para Clientes na 1ª Subrede das 16 disponíveis	10.133.136.1 a 10.133.136.14
Servidor *Videowall* no C Op/CMP	10.133.136.10/28
Câmera Fixa 1 (CMP)	10.133.136.1/28
Câmera Fixa 2 (BGP)	10.133.136.2/28
Câmera Móvel 1 (Entrada/saída N do QGEx)	10.133.136.3/28
Câmera Móvel 2 (Entrada/saída S do QGEx)	10.133.136.4/28

Fonte: [74]

O SisMC² é formado pelos seus subsistemas orgânicos de C² instalados no MD e nos Grandes Comandos das FA (MB, EB e FAB): (i) Rede Operacional de Defesa (ROD); (ii) Sistema de Planejamento

de Operações Militares (SIPLOM); (iii) Sistema Tático de Enlace de Dados (SISTED); (iv) Sistema de Comunicações Militares por Satélite (SISCOMIS); e (v) Satélite Geoestacionário de Defesa e Comunicações Estratégicas 1 (SGDC-1), conforme demonstra a Figura 3.9 – Sistema Militar de Comando e Controle (SisMC²) na Estrutura Militar de Defesa (EttaMiD) a seguir.

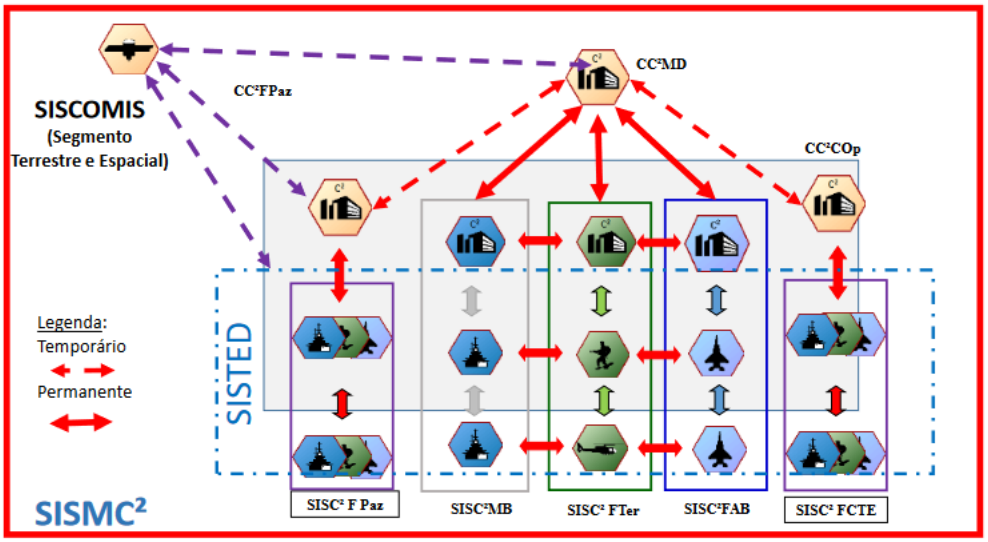

Figura 3.9: Sistema Militar de Comando e Controle (SisMC²) na Estrutura Militar de Defesa (EttaMiD) [142]

A EBNet é um sistema complexo formado por Redes Heterogêneas, que envolvem redes de enlaces de dados com fibras ópticas, cabos UTP, e rádios de enlaces de microondas, além de roteadores, *switchs*, servidores vinculados aos *Datacenters* presentes no Centro Integrado de Telemática do Exército (CITEx), situado em Brasília/DF, e *Datacenters* situados nos demais Centros de Telemática de Área (CTA) lotados em cada C Mil A, e nos demais Centros de Telemática (CT) lotados em cada C Mil A. A EBNet compreende ainda redes de enlaces de radiofrequências em HF vinculadas à Rede Rádio Fixa do Sistema Estratégico de Comunicações [143].

A EBNet também dispõe de *Datacenters* instalados no 7º Centro de Telemática de Área (7º CTA), em Brasília/DF (posição central da rede e com maiores recursos tecnológicos) e nos *Datacenters* regionais situados nos outros Centros de Telemática de Área (CTA) e nos Centros de Telemática (CT) dos outros 7 C Mil A no Brasil (CMA, CMN, CMNE, CMO, CML, CMSE e CMS), conforme demonstra a Figura **??** acima.

O CITEx, CTA e CT disponibilizam os serviços dos Sistemas Corporativos do EB (pagamento, controle de pessoal, controle de material, etc) diariamente para as atividades do cotidiano [144]. No total são 75 sistemas informáticos diversos produzidos no Centro de Desenvolvimento de Sistemas (CDS) do Exército [145], desde páginas eletrônicas do EB para acessos restritos dos militares do EB, bem como páginas da Internet para acesso livre da nação brasileira, e também Bancos de Dados dos militares da ativa e da reserva, bem como os seus pensionistas e familiares.

A EBNet ainda fornece contas de correio eletrônico denominado *EBMail*, contas da rede social por meio do aplicativo denominado *EBChat*, e também contas pessoais de armazenamento na Nuvem denominada *EBCloud*, a fim de atender aos trabalhos diários dos militares do EB no Brasil e no exterior.

Em resumo, a EBNet interliga todas as 662 Organizações Militares (OM) do Exército por meio de diversas WAN, MAN e LAN compostas por fibras ópticas proprietárias do EB e também por fibras ópticas contratadas da Embratel [141], cujo valor anual está em torno de R$ 27 milhões [144], além de empregar enlaces micro-ondas entre transceptores terrestres e também enlaces satelitais, principalmente nas OM lotadas na Amazônia Legal.[3]

O Programa Estratégico Gestão de Tecnologia da Informação e Comunicações (Prg EE G TIC) é um conjunto de projetos que visa dar ao EB o suporte de TIC necessário para o cumprimento de sua missão. Por intermédio desse Programa é possível oferecer informações corretas e oportunas por meios eficazes de C², de modo a garantir "Liberdade de Ação"no Espaço Cibernético e no espaço geoestratégico de interesse da Nação brasileira, segundo regula o Escritório de Projetos do Exército (EPEx) [72].

O Sistema de Vigilância Eletrônico com câmeras IP poderia ter sido avançado, caso tivesse sido usada Inteligência Artificial (IA) no Servidor (*Videowall*) das 4 câmeras IP Hikivision do C Op/CMP por meio do *software* **YOLOv5**, pois a placa de vídeo dedicada do servidor auxiliaria no processamento das imagens captadas pelas 4 câmeras via rede privada na EBNet.

Atualmente a IA é usada em sistemas de vigilância eletrônica para realizar o reconhecimento facial automatizado, o reconhecimento de placas de veículos e o reconhecimento de objetos (suspeitos ou comuns), bastando treinar o servidor/computador/notebook para os alvos desejados. Inclusive a China empregou IA em suas câmeras públicas para controlar a população durante o isolamento social na pandemia de COVID-19.

3.2.2 Sistema de Monitoramento Eletrônico com *Drone* Autônomo do C OP/CMP

O Sistema de Monitoramento Eletrônico com *drone* automatizado é formado por:

- 1 (um) Servidor com *software* de gerenciamento de imagens digitais tipo *Videowall* e mais 24 (telas) telas de 60 polegadas e um sistema de som com alto-falantes fixos no teto do Salão do C Op/CMP; e
- 1 (um) Kit *drone* da 7ª Cia Intlg dispõe dos componentes táticos a seguir:

  (i) *Drone Mavic 2 Enterprise*;

  (ii) controle remoto com visor LCD;

  (iii) Kit de alimentação elétrica com 1 (uma) fonte de alimentação bivolt (110V – 220V) e 3 (três) baterias de Lítio;

  (iv) cabo de transmissão de dados (fotos/filmagens) HDMI; e

  (v) bolsa de couro com alça de transporte.

A composição do Sistema *Videowall* está apresentado na Figura 3.10 – Componentes do *Wideowall* do C Op/CMP abaixo.

[3]Em [146] **Amazônia Legal** é definida como a região Norte do Brasil formada por: 52 municípios de Rondônia/RO, 22 municípios do Acre/AC, 62 municípios do Amazonas, 15 municípios de Roraima/RR, 144 municípios do Pará/PA, 16 municípios do Amapá/AP, 139 municípios do Tocantins/TO, 181 municípios do Maranhão/MA, e 141 municípios do Mato Grosso/MT.

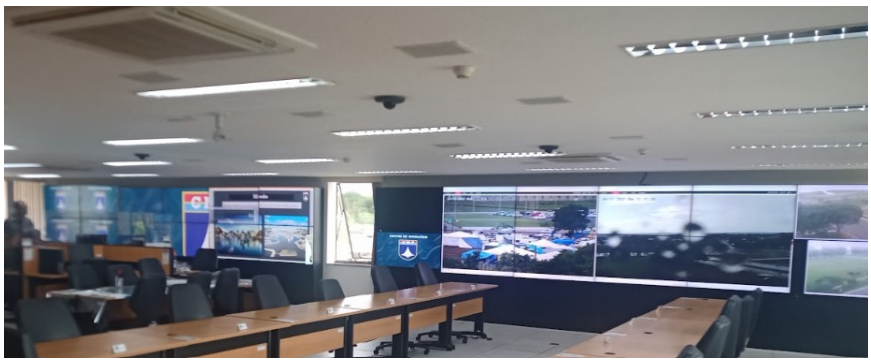

Figura 3.10: Componentes do *Wideowall* do C Op/CMP [74]

A composição do Kit *drone* está apresentada na Figura 3.11 – Componentes Táticos do *drone Mavic 2 Enterprise* a seguir.

Figura 3.11: Componentes Táticos do *drone Mavic 2 Enterprise* [74]

O Sistema de Monitoramento eletrônico com *drone Mavic 2 Enterprise* operava na LAN tipo Classe A **10.133.136.0/28** do C Op/CMP, sob uso exclusivo na EBNet, conforme demonstra a Tabela 3.2 – Parâmetros da Rede, equipamentos e endereços IP utilizados no Sistema de Monitoramento Eletrônico do C Op/CMP a seguir.

Tabela 3.2: Parâmetros da Rede, equipamentos e endereços IP utilizados no Sistema de Monitoramento eletrônico do C Op/CMP

Parâmetros/Equipamentos	**Endereços IP**
Máscara da Rede	255.255.255.240 ou /28
Quantidade de Subredes/Clientes	16/16
Endereço da Rede (*Gateway*)	10.133.136.0/28
Endereço de Difusão (*Broadcast*)	10.133.136.15/28
1ª Faixa de IP disponíveis para Clientes (*Hosts*)	10.133.136.1 a 10.133.136.14
Servidor *Videowall* no C Op/CMP	10.133.136.10/28
Drone Mavic 2 Enterprise	10.133.136.5/28

Fonte [74]

O *drone Mavic 2 Enterprise* foi fabricado pela empresa chinesa DJI, com sede em Shenzhen, no sudeste da China, cunhada como o "Vale do Silício"chinês é a principal expoente da chamada *Greater Bay Area* região formada por nove cidades chinesas (Shenzhen, Guangzhou, Zhuhai, Foshan, Dongguan, Zhongshan, Jiangmen, Huizhou, Zhaoqing) e duas regiões administrativas especiais Hong Kong e Macau [147].

O *drone Mavic 2 Enterprise* é um equipamento intermediário e no mercado atual custa aproximadamente R$ 65 mil. É considerado um equipamento robusto, de fácil manobrabilidade e muito operacional, suportando pequenos choques mecânicos contra anteparos verticais/horizontais, é à prova d'água, dispõe de uma autonomia de voo de até 1 (uma) hora, e pode ser equipado com câmera infravermelha (item opcional) habilitando operar em condições severas de falta de iluminação natural, como no interior de grutas, nevoeiros, e à noite [148].

Esse equipamento *drone* foi desenvolvido para cumprir um leque de missões voltadas para a segurança pública e privada, mas pode ser usado também para atividades profissionais diversas e lazer [148], tais como:

(i) resgate (geolocalização) com luz LED e microfone/alto-falante embutidos;

(ii) busca e salvamento em áreas de risco de morte (incendiadas, desmoronadas, inundadas, envenenadas, etc);

(iii) inspeções em locais de difícil acesso ou que exija maior atenção (represas, rios, lagos, pontes, galerias de mineração, linhas de alta tensão, reservatórios de líquidos inflamáveis e depósitos de resíduos tóxicos/radioativos);

(iv) vistoria de locais com grandes dimensões para percurso humano a pé (plantações, estacionamentos de shoppings centers, estradas, etc);

(v) capta/grava/transmite imagens cinematográficas para fins comerciais ou privados (festas de casamentos, aniversários, passeios, animais, pessoas, veículos, natureza, etc).

Os sobrevoos das áreas estratégicas no SMU para observação e coleta de dados de Intlg (fotos/filmetes/transmissões ao vivo pela plataforma YouTube) direcionados para o Sistema *Videowall* do C Op/CMP foram realizadas em horários diversos nos dias com melhores condições meteorológicas (sem precipitações e ventos fortes), conforme ilustrado na Figura 3.12 – Tela do sobrevoo do *Drone Mavic 2 Enterprise* nas áreas estratégicas do SMU a seguir.

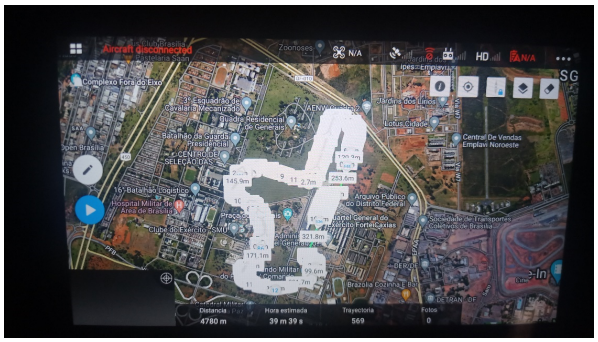

Figura 3.12: Tela do sobrevoo do *drone Mavic 2 Enterprise* nas áreas estratégicas do SMU [74]

3.2.3 Sistema 5G Tático EB

A arquitetura de Sistemas de Comunicações baseados em tecnologias dos 3 serviços do 5G embarcados já é uma realidade no emprego civil em áreas sem cobertura do sinal 5G SA (Autônomo, do inglês *Standalone*) no Brasil e em muitos países no exterior, por exemplo: (i) China; (ii) Coreia do Sul; e (iii) EUA.

Neste trabalho, uma proposta de arquitetura conceitual de Sistema de Comunicação 5G foi denominada simplesmente como "**Sistema 5G Tático EB**".

Esse modelo de Sistema 5G Tático EB pode ser considerado como uma tecnologia dual – civil e militar – pois pode ser empregado tanto nas comunicações civis em uma localidade sem ERB, bem como nas comunicações militares durante as Operações do EB nas regiões urbanas (e.g. Operações tipo GLO) e nas regiões fronteiriças (e.g. Operações tipo Ágata) [39]. Contudo, nenhum tipo de Sistema de Comunicação 5G foi sugerido para ser empregado em operações militares no Brasil antes desse trabalho.

Durante as pesquisas bibliográficas neste trabalho foram lidos muitos artigos científicos, porém poucos fizeram relacionamento do emprego típico militar das tecnologias derivadas dos 3 serviços do 5G (eMBB, mMTC e URLLC) em operações nas FA estrangeiras, conforme verificado anteriormente na Seção **2.4 TRABALHOS CORRELATOS NA PREVISÃO DO EMPREGO MILITAR DAS TECNOLOGIAS E SERVIÇOS DO 5G**, presentes na Seção **2 REFERENCIAL TEÓRICO**.

Ele contém os mesmos equipamentos de uma ERB fixa instalada em um telhado/parede de um prédio, porém estão embarcados em uma viatura Furgão Mercedes Benz Sprinter 413, sendo apoiados por 1 (um) mastro pneumático e 1 (um) gerador interno de energia elétrica para alimentar o banco de baterias e todos os demais equipamentos 5G NR, roteadores, e antenas ortogonais painéis com MU-MIMO, conforme demonstram a Figura 3.13 – Sistema 5G Tático EB – Visão lateral a seguir, Figura 3.14 Sistema 5G Tático EB – Visão frontal abaixo, e Figura 3.16 – Visão interior dos equipamentos embarcados no Sistema 5G Tático EB [74] abaixo.

Figura 3.13: Sistema 5G Tático EB – Visão lateral [74]

Figura 3.14: Sistema 5G Tático EB – Visão frontal [74]

Ele foi produzido no Brasil, especificamente na cidade de São José dos Campos/SP. A maior parte dos equipamentos desse *Site* móvel 5G foi importado da Ericsson dos EUA, mas a viatura Furgão Mercedes Benz Sprinter 413 e a integração dos diversos sistemas de Com, Energia (gerador e banco de baterias), mastro pneumático e ar condicionado foi realizada pela empresa RFCom Sistemas Ltda, de São José dos Campos/SP, conforme descritos na Tabela 3.3 – Equipamentos integrados no Sistema 5G Móvel da Tim a seguir, e demonstrado na Figura 3.15 – Esquema de Ligações Internas dos Equipamentos da Ericsson no *Site* Móvel Tim DF abaixo; e 3.16 – Visão interior dos equipamentos embarcados no Sistema 5G Móvel Tim DF [74] abaixo.

Tabela 3.3: Equipamentos integrados no Sistema 5G Móvel da Tim

Equipamentos integrados na RF Com	**Qnt**	**Und R$**	**Total R$**
Mercedes Benz Sprinter 413 Furgão Longo T. Alto Diesel	1	120.000,00	120.000,00
Kit Integração Unidade Móvel	1	75.731,00	75.731,00
Sistema de Nivelamento Automático Pneumático	1	17.359,00	17.359,00
Sistema de Mastro Telescópico de 12 m	1	76.225,00	76.225,00
Grupo Moto Gerador *Cummins* 12 KVA	1	22.511,00	22.511,00
Conjunto Rádio 5G Ericsson com Antenas Ortogonais Painel Plano 3,5 GHz de 25 dB ganho	3	100.000,00	300.000,00
Conjunto Baterias de Lítio Solar de 2.4 kWh, 48 V e 50 Ah	3	7.000,00	21.000,00
Licença de utilização do *software* de gerenciamento e manutenção do 5G NR Ericsson	1	100.000,00	100.000,00
Total investido no Sistema 5G Móvel Tim R$ 732.826,00 em 2012			

Fonte: [74]

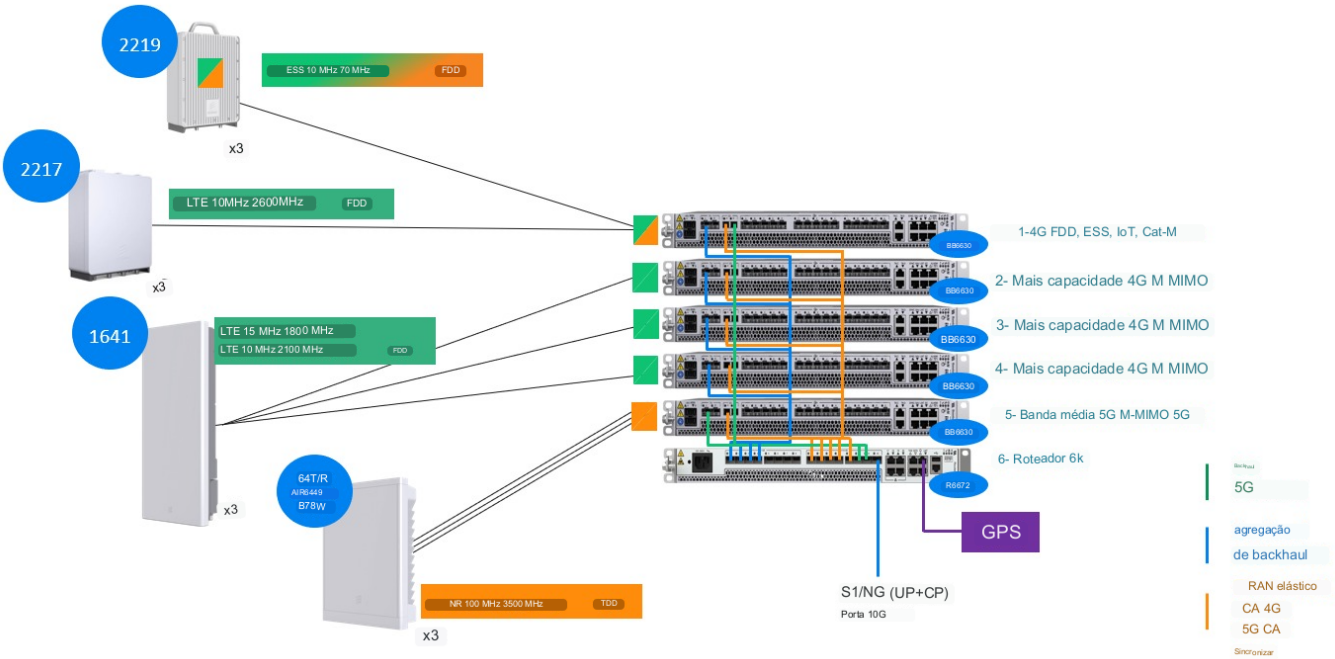

Figura 3.15: Esquema de Ligações Internas dos Equipamentos da Ericsson no Site Móvel Tim DF [149]

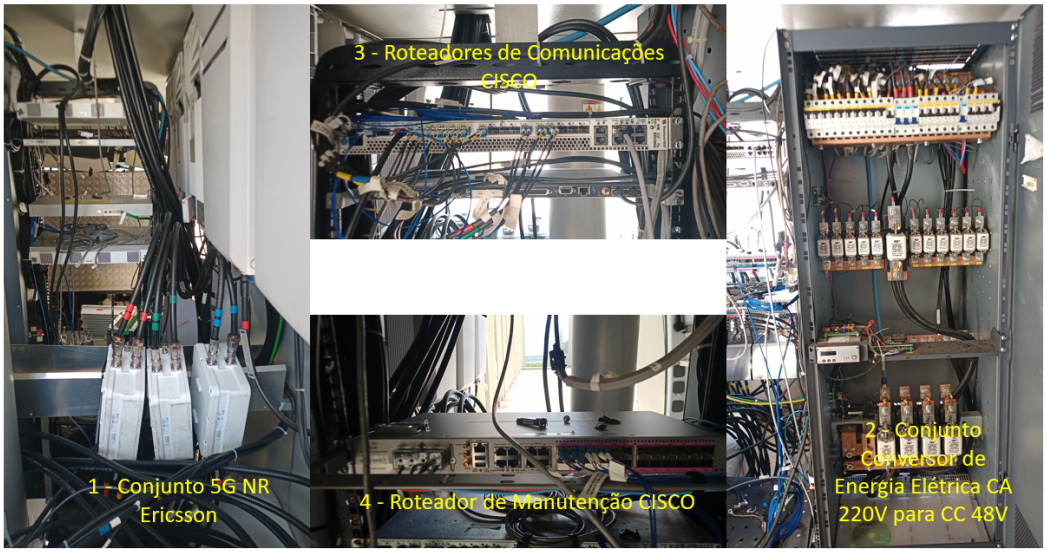

Figura 3.16: Visão interior dos equipamentos embarcados no Sistema 5G Móvel Tim DF [74]

Das assertivas acima e das análises das informações da Tabela 3.3 – Equipamentos integrados no Sistema 5G Móvel da Tim, da Figura 3.15 e da Figura 3.16, observa-se que há uma ligação física com cabo coaxial (denominada *Fronthaul*) entre cada 5G NR (3.500 Mhz) para sua específica Antena Ortogonal Painel Plana MU-MIMO 5G e também há uma ligação física do 5G NR com cabo UTP Cat 7 para seu específico Roteador BB6630 responsável em estabelecer e operar a Rede Móvel Principal (*Mobile Core Network*) [150] do Sistema 5G Tático EB, conforme demonstra a Figura 3.17 – Esquema de *Fronthaul*,*Backhaul* e Rede Móvel Principal (*Mobile Core Network*) no interior dos equipamentos embarcados no Sistema 5G Móvel Tim DF abaixo.

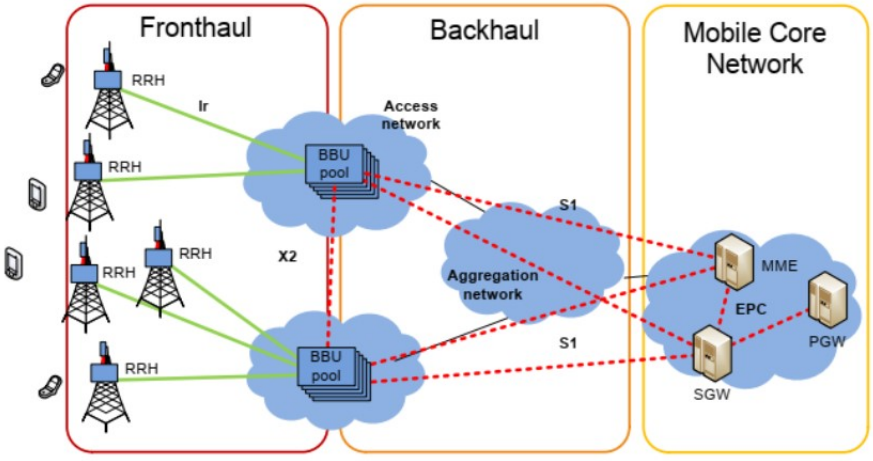

Figura 3.17: Esquema de *Fronthaul*,*Backhaul* e Rede Móvel Principal (*Mobile Core Network*) no interior dos equipamentos embarcados no Sistema 5G Móvel Tim DF [150]

Enfim, a empresa Tim DF disponibilizou esse *Site* 5G Móvel para seus clientes lotados no Forte Caxias QGEx enquanto aguarda a homologação da Anatel para concluir a instalação das 3 ERBs com seus Sítios de Antenas do 5G SA fixo sobre os telhados dos Blocos I e J do QGEx, segundo informações de [149].

4 RESULTADOS E DISCUSSÕES

4.1 QUESTIONÁRIO ONLINE SOBRE O EMPREGO DUAL CIVIL E MILITAR DO ECOSSISTEMA 5G BRASIL NA DEFESA BRASILEIRA

4.1.1 INTRODUÇÃO

O Formulário do Questionário *On-line* denominado **O emprego dual – civil e militar – do Ecossistema 5G Brasil na Defesa brasileira** consta de 37 páginas, foi elaborado na plataforma digital da Google Formulários, remetido para 67 (vinte) OM do EB, e permaneceu disponível para preenchimento entre os dias 09/11/22 a 05/12/22.

A página eletrônica [151] **<http://forms.gle/yWvSQMbYkbZ38Aat9>**, contém todos os preâmbulos das questões, os quais explicam sobre os serviços, tecnologias, possibilidades e limitações dos Ecossistemas 5G Global e 5G Brasil nesse Questionário *On-line*.

Esse Questionário On-line é composto por 4 (quatro) seções distintas:

- **Seção 1 de 4**: composta pela apresentação do autor, os Objetivos geral e específicos da pesquisa e a apresentação do questionário sobre o entendimento geral do emprego dual – civil e militar – do Ecossistema 5G Brasil na Defesa brasileira;
- **Seção 2 de 4**: composta pelos conceitos sintéticos sobre o Brasil, a Faixa de Fronteira, a Defesa, o Exército, as Seguranças: da Informação, das Comunicações e Cibernética, o Poder Cibernético, a Guerra Cibernética, o Ataque/Incidente Cibernético, e o Ecossistema 5G Brasil;
- **Seção 3 de 4**: composta por 13 perguntas com respostas diretas tipo múltipla escolha, que poderão sofrer modificações pelos participantes durante o preenchimento até 25 NOV 22 (sexta-feira). Após essa data foi finalizado o questionário e realizadas as estatísticas necessárias da Seção 4 Discussões dos resultados da dissertação; e
- **Seção 4 de 4**: composta pelas Referências Bibliográficas.

Participaram voluntariamente 117 militares do EB, os quais responderam às 13 questões contextualizadas com informações técnicas coletadas e figuras nas diversas fontes bibliográficas dessa monografia.

Ressalta-se que a ideia original desse questionário foi coletar as opiniões dos militares que trabalham com TIC nos Grandes Comandos Militares de Área (C Mil A), nas Escolas de Formação do Exército ((ECEME, ESAO, AMAN, IME, ESA, e EsLog), nos Departamentos do Alto Comando do Exército (Gab Cmt Ex, EME, DEC, DCT, DECEx, etc), nos Centros de Telemática do Exército (CITEx, CTA, e CT), Grandes Unidades (Brigada), Centro de Inteligência do Exército (CIE), Comando de Defesa Cibernética (Com D Ciber) e Gabinete de Segurança Institucional (GSI), sobre a visão futura dos possíveis impactos do Ecossistema 5G Brasil para a Defesa brasileira. Além de fornecer aos participantes do EB os con-

ceitos relacionados ao emprego dual do Ecossistema 5G, suas possibilidades e suas limitações na Defesa brasileira.

Primeiramente, a importância principal desse Questionário *On-Line* sobre o emprego tático do 5G para o Exército foi despertar alguns atores do Alto Comando do Exército, especificamente autoridades do Gabinete do Comandante do Exército (Gab Cmt Ex) e do Estado-Maior do Exército (EME) para a importância estratégica do 5G para a Estrutura Militar de Defesa (Etta M D) nos próximos 20 anos, período de transformação do Exército, conforme publicado no documento intitulado "Manual de Fundamentos CONCEITO OPERACIONAL DO EXÉRCITO BRASILEIRO OPERAÇÕES DE CONVERGÊNCIA 2040 (EB20-MF-07.101)", recém publicado por meio da PORTARIA - EME/C EX Nº 971, DE 10 DE FEVEREIRO DE 2023 [65].

Finalmente, a importância principal desse Questionário *On-Line* sobre o emprego tático do 5G para o Exército neste trabalho foi para dar subsídios para a confecção dessa dissertação e de um relatório independente baseado em artigos científicos e na legislação brasileira vigente sobre o 5G, sobre Segurança Cibernética do 5G, e sobre a doutrina militar de emprego das FA, o qual será encaminhado para o Escritório de Projetos do Estado-Maior do Exército (EPEx), situado no Bloco H do QGEx, via canal de comando pelo Departamento de Ciência e Tecnologia (DCT).

4.1.2 APRESENTAÇÃO DOS RESULTADOS DO QUESTIONÁRIO

No total 117 (cento e dezessete) militares do EB preencheram o Formulário *on-line* da *Google* contendo as 13 (treze) questões descritas a seguir:

1. O(a) senhor(a) está servindo em qual local hoje?

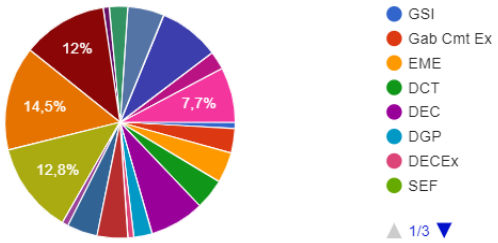

Figura 4.1: Organizações Militares dos participantes do questionário [74].

Tabela 4.1: Organizações Militares dos participantes do questionário

Quais são as Organizações Militares dos participantes do questionário?	**Quantidade**	**Porcentagem**
C Mil A (CMA, CMN, CMNE, CMSE, CMS, CML, CMO, CMP)	17	14,5%
RM (1ª RM, 2ª RM, 3ª RM, 4ª RM, 5ª RM, 6ª RM, 7ª RM, 8ª RM, 9ª RM, 10ª RM, 11ª RM, 12ª RM)	15	12,8%
Escolas de Formação (ECEME, ESAO, AMAN, IME, ESA, EsLog)	10	8,5%
DEC	09	7,7%
OMDS/CMP (1º RCG, 2º B Fv, 7ª Cia Intlg, BGP, BPEB, B Adm Ap/CMP)	09	7,7%
CT (11º CT, 21º CT, 41º CT, 51º CT, 52º CT)	06	5,1
EME	05	4,3%
DCT	05	4,3%
COTER	05	4,3%
COLOG	05	4,3%
Gab Cmt Ex	04	3,4%
DGP	03	2,6%
CTA (1º CTA, 2º CTA, 3º CTA, 4º CTA, 5º CTA, 6º CTA, 7º CTA)	03	2,6%
3ª Bda Inf Mtz	03	2,6%
GSI	01	0,9%
DECEx	01	0,9%
Com D Ciber	01	0,9%
CITEx	01	0,9%
Total de participantes	117	100%

2. O(a) senhor(a) atua diretamente com Tecnologia da Informação e Comunicação (TIC) ou gestão da Segurança da Informação no seu local de trabalho?

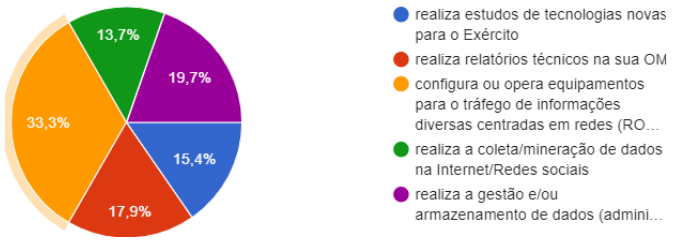

Figura 4.2: Funções dos participantes no seu local de trabalho [74].

Tabela 4.2: Funções dos participantes no seu local de trabalho

Quais as funções dos participantes no seu local de trabalho?	**Quantidade**	**Porcentagem**
Configura ou opera equipamentos para o tráfego de informações diversas centradas em redes (ROD, SISCOMIS, EBNet, Intranet, Internet, VoIP, Servidores, Roteadores, Fibras Ópticas, etc)	39	33,3%
Realiza a gestão e/ou armazenamento de dados (administra Banco de Dados)	23	19,7%
Realiza relatórios técnicos na sua OM	21	17,9%
Realiza estudos de tecnologias novas para o Exército	18	15,4%
Realiza a coleta/mineração de dados na Internet/Redes sociais	16	13,7%
Total de participantes	117	100%

3. O(a) senhor(a) acredita em qual prazo o emprego dual – civil e militar – do Ecossistema 5G Brasil possibilitará vantagens estratégicas na Defesa brasileira com relação aos 10 (dez) países vizinhos na América do Sul: Argentina, Bolívia, Colômbia, Guiana, Guiana Francesa (Departamento Ultramarino da França), Paraguai, Peru, Suriname, Uruguai, e Venezuela, os quais ainda não dispõe das tecnologias e serviços do 5G 3GPP totalmente operantes em seus territórios?

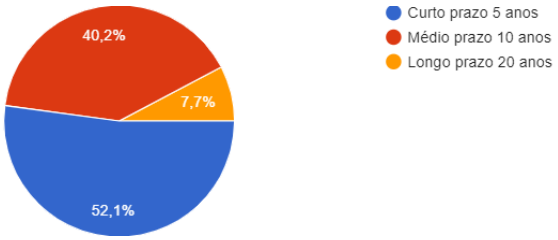

Figura 4.3: Prazos para vantagens estratégicas na Defesa brasileira com o Ecossistema 5G Brasil sobre a América do Sul [74].

Tabela 4.3: Prazos para vantagens estratégicas na Defesa brasileira com o Ecossistema 5G Brasil sobre a América do Sul

O Brasil obterá vantagens estratégicas com o 5G em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	61	52,1%
Médio prazo 10 anos	47	40,2%
Longo prazo 20 anos	09	7,7%
Total de participantes	117	100%

4. O(a) senhor(a) acredita em qual prazo que o emprego dual – civil e militar – do Ecossistema 5G Brasil possibilitará os desenvolvimentos nacionais tecnológico, social e econômico estimados pela Anatel, MCTIC, SEPEC e PNUD?

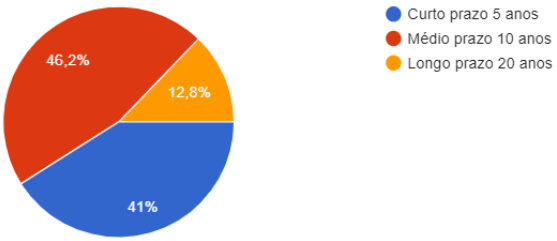

Figura 4.4: Prazos para os desenvolvimentos nacionais tecnológico, social e econômico com o Ecossistema 5G brasileiro [74].

Tabela 4.4: Prazos para os desenvolvimentos nacionais tecnológico, social e econômico com o Ecossistema 5G brasileiro

o Ecossistema 5G Brasil possibilitará os desenvolvimentos nacionais tecnológico, social e econômico em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	48	41%
Médio prazo 10 anos	54	46,2%
Longo prazo 20 anos	15	12,8%
Total de participantes	117	100%

5. O(a) senhor(a) acredita em qual prazo o emprego dual – civil e militar - do Ecossistema 5G Brasil possibilitará melhorias nos Projetos Estratégicos das Forças Armadas (Nuclear, Cibernético e Espacial) na Defesa brasileira?

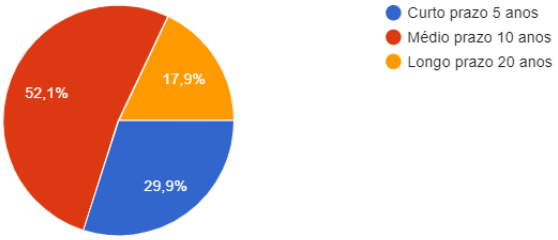

Figura 4.5: Prazos para melhorias do 5G brasileiro nos Projetos Estratégicos das FA (Nuclear, Cibernético e Espacial) [74].

Tabela 4.5: Prazos para melhorias do 5G brasileiro nos Projetos Estratégicos das FA (Nuclear, Cibernético e Espacial)

As melhorias do 5G brasileiro nos Projetos Estratégicos das FA poderá ocorrer em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	35	29,9%
Médio prazo 10 anos	61	52,1%
Longo prazo 20 anos	21	17,9%
Total de participantes	117	100%

6. O(a) senhor(a) acredita em qual prazo o emprego dual - civil e militar - do Ecossistema 5G Brasil possibilitará benefícios para as Forças Armadas brasileiras nesses campos: comunicações, comando e controle, consciência situacional, controle de veículos autônomos, defesa antiaérea, armamentos inteligentes,

munições inteligentes, bases logísticas inteligentes, equipamentos vestíveis, simulações nos treinamentos, melhorias em instalações do Serviço de Saúde?

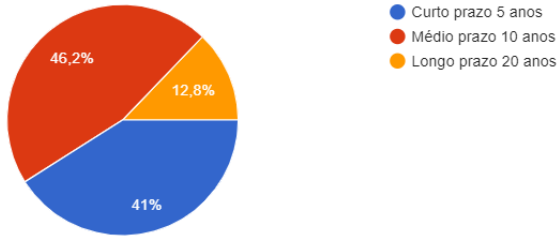

Figura 4.6: Prazos de possíveis benefícios do 5G nos sistemas de Defesa das FA brasileiras [74].

Tabela 4.6: Prazos de possíveis benefícios do 5G nos sistemas de Defesa das FA brasileiras

Prazos para o 5G brasileiro possibilitar benefícios aos sistemas de Defesa (Com, C², CS, Armto, Log, etc) das FA	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	54	46,2%
Médio prazo 10 anos	41	35%
Longo prazo 20 anos	22	18,8%
Total de participantes	117	100%

7. O(a) senhor(a) acredita que o Ecossistema 5G Brasil poderá sofrer ataques eletrônicos ou ataques cibernéticos, colocando em risco a Segurança Cibernética brasileira no curto prazo de 5 anos?

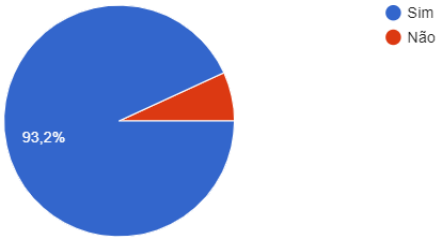

Figura 4.7: Possibilidade de ataques cibernéticos nas redes 5G brasileiras no curto prazo de 5 anos [74].

Tabela 4.7: Possibilidade de ataques cibernéticos nas redes 5G brasileiras no curto prazo de 5 anos

Há possibilidade de ataques cibernéticos nas redes 5G brasileiras no curto prazo de 5 anos?	**Quantidade**	**Porcentagem**
Sim	109	93,2%
Não	8	6,8%
Total de participantes	117	100%

8. O(a) senhor(a) acredita que o Comando de Defesa Cibernética (Com D Ciber) e a Escola Nacional de Defesa Cibernética (ENaDCiber) conseguirão desenvolver as capacidades cibernéticas necessárias para os integrantes das Forças Armadas (MB, EB e FAB) responsáveis pela Defesa Cibernética (Def Ciber) e Guerra Cibernética (G Ciber) brasileiras, considerando-se o aumento da quantidade de dispositivos eletrônicos interconectados e o aumento das ameaças cibernéticas com a implementação do Ecossistema 5G

Brasil?

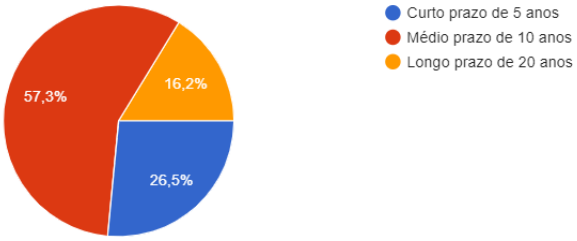

Figura 4.8: Prazos para desenvolver as capacidades cibernéticas necessárias para os integrantes das FA [74].

Tabela 4.8: Prazos para desenvolver as capacidades cibernéticas necessárias para os integrantes das FA

Com D Ciber e ENaDCiber conseguem capacitar militares das FA contra ameaças do 5G em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	31	26,5%
Médio prazo 10 anos	67	57,3%
Longo prazo 20 anos	19	16,2%
Total de participantes	117	100%

9. O(a) senhor(a) acredita que o fomento à pesquisa científica no Exército junto aos Estabelecimentos de Ensinos Superiores, Militares e Civis, Nacionais e Internacionais, apoiados pelo EME, DCT, DEC, COTER, DGP, DECEx, SEF, COLOG, C Mil A e CIE poderá ampliar a capacidade da Segurança Cibernética brasileira em qual prazo?

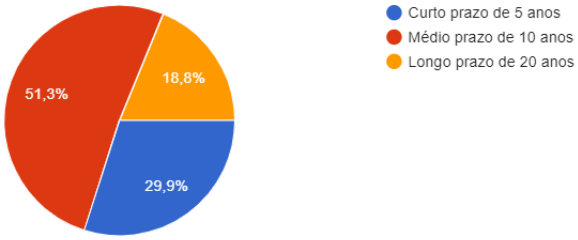

Figura 4.9: Prazos para fomentar a pesquisa 5G no EB e aumentar sua capacidade de Segurança Cibernética [74].

Tabela 4.9: Prazos para fomentar a pesquisa 5G no EB e aumentar sua capacidade de Segurança Cibernética

O incentivo à pesquisa científica do 5G poderá ampliar a capacidade da Segurança Cibernética brasileira em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	35	29,9%
Médio prazo 10 anos	60	51,3%
Longo prazo 20 anos	22	18,8%
Total de participantes	117	100%

10. O(a) senhor(a) acredita que devido à expansão dos usuários de equipamentos diversos (*laptops, desktops, tablets, smartphones, phones bluetooth e videogames*) junto dos equipamentos de Internet das Coisas (IoT) no Brasil, além das vulnerabilidades intrínsecas das redes móveis 5G, o Brasil conseguirá manter a atual resiliência na Segurança Cibernética até qual prazo?

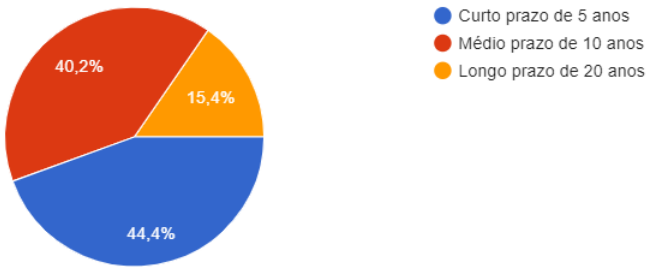

Figura 4.10: Prazos para manutenção da Resiliência Cibernética nas redes 5G brasileiras [74].

Tabela 4.10: Prazos para manutenção da Resiliência Cibernética nas redes 5G brasileiras

A Resiliência cibernética nas redes 5G brasileiras poderá ser mantida em qual prazo?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	52	44,4%
Médio prazo 10 anos	47	40,2%
Longo prazo 20 anos	01	15,4%
Total de participantes	117	100%

11. O(a) senhor(a) acredita que as autoridades competentes supracitadas conseguem orientar adequadamente as instituições públicas e privadas, e a população brasileira em geral, sobre como se manter preparada para agir em caso de um ataque/incidente cibernético sobre alguma infraestrutura crítica (IC) brasileira?

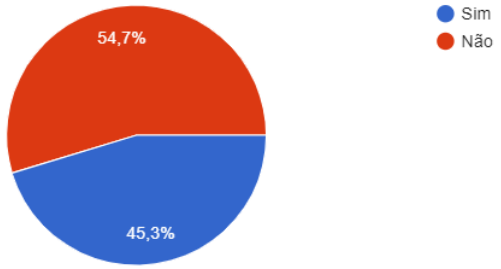

Figura 4.11: As autoridades competentes conseguem orientar medidas contra ataques/incidentes cibernéticos no 5G [74].

Tabela 4.11: As autoridades competentes conseguem orientar medidas contra ataques/incidentes cibernéticos no 5G

As autoridades competentes conseguem orientar medidas contra ataques/incidentes cibernéticos no 5G atualmente?	**Quantidade**	**Porcentagem**
Sim	64	54,7%
Não	53	45,3%
Total de participantes	117	100%

12. O(a) senhor(a) acredita ser possível o emprego dual do 5G nas áreas militares supracitadas, a despeito dos altos investimentos financeiros necessários para realizar as ligações por fibras ópticas entre as câmeras fixas (*fish eye*) e/ou articuladas (*speed dome*), bem como a disponibilização do sinal 5G replicado internamente em alguns setores estratégicos do QGEx e do QG Complexo do CMP/11ª RM?

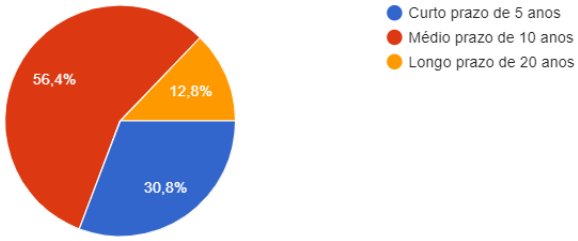

Figura 4.12: Prazos para disponibilizar o sinal 5G no QGEx e no QG Cmdo CMP/11ª RM [74].

Tabela 4.12: Prazos para disponibilizar o sinal 5G no QGEx e no QG Cmdo CMP/11ª RM

Qual seria o prazo viável para emprego do 5G no QGEx e QG CMP/11ª RM?	**Quantidade**	**Porcentagem**
Curto prazo 5 anos	36	30,8%
Médio prazo 10 anos	66	56,4%
Longo prazo 20 anos	15	12,8%
Total de participantes	117	100%

13. Senhor(a) participante, ao finalizar o preenchimento desse Questionário, que visa esclarecer e qualificar o "Emprego dual – civil e militar – do 5G na Defesa brasileira", na sua opinião qual é o grau de importância da pesquisa científica sobre todo o assunto abordado?

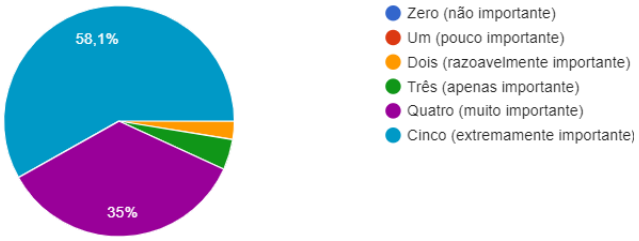

Figura 4.13: Grau de importância dessa pesquisa científica sobre todo o assunto abordado [74].

Tabela 4.13: Grau de importância dessa pesquisa científica sobre todo o assunto abordado

Qual é o grau de importância dessa pesquisa científica sobre todo o assunto abordado?	**Quantidade**	**Porcentagem**
Cinco (extremamente importante)	68	58,1%
Quatro (muito importante)	41	35%
Três (apenas importante)	5	4,3%
Dois (razoavelmente importante)	3	2,6%
Um (pouco importante)	0	0%
Zero (não importante)	0	0%
Total de participantes	117	100%

4.1.3 DISCUSSÕES DO QUESTIONÁRIO *ON-LINE*

A principal contribuição desse Questionário *On-line* na pesquisa realizada neste trabalho é que serviu de base para um relatório independente que será encaminhado para o Escritório de Projetos do Exército (EPEx), orgânico do Estado-Maior do Exército (EME), via o canal de comando do Departamento de Ciência e Tecnologia (DCT) logo após a publicação dessa dissertação na UnB. As observações e as respostas dos militares participantes foram de grande valia para demonstrar os resultados da pesquisa aos atores responsáveis pela definição e implantação do 5G junto ao Exército num futuro próximo.

Das 13 (treze) questões encaminhadas no questionário e pelas respostas dos 117 (cento e dezessete) participantes voluntários, verificou-se os pontos chaves respondidos:

- 27,3% (32 militares) do Graf 4.1 trabalham em Grandes Comandos Operacionais (C Mil A) e Grandes Comandos Logísticos e Administrativos (RM) ficando mais próximos das autoridades decisoras e envolvidos diretamente nas operações lidam com o C²;
- 33,3% (39 militares) do Graf 4.2 configuram ou operam equipamentos para o tráfego de informações diversas centradas em redes (ROD, SISCOMIS, EBNet, Intranet, Internet, VoIP, Servidores, Roteadores, Fibras Ópticas, etc) e lidam diretamente com as Com;
- 52,1% (61 militares) do Graf 4.3 acreditam que o Brasil obterá vantagens estratégicas na Defesa com o Ecossistema 5G Brasil sobre os 10 países fronteiriços na América do Sul no curto prazo de 5 anos;
- 46,2% (54 militares) do Graf 4.4 acreditam que o Ecossistema 5G Brasil no médio prazo de 10 anos possibilitará os desenvolvimentos nacionais tecnológico, social e econômico estimados pela Anatel, MCTIC, SEPEC e PNUD;
- 52,1% (61 militares) do Graf 4.5 acreditam nas melhorias do 5G brasileiro nos Projetos Estratégicos das FA (Nuclear, Cibernético e Espacial) no curto médio prazo de 10 anos;
- 46,2% (54 militares) do Graf 4.6 acreditam que o 5G brasileiro possibilitará benefícios aos sistemas de Defesa (Com, C², CS, Armto, Log, etc) das FA no curto prazo de 5 anos;
- 93,2% (109 militares) do Graf 4.7 acreditam que o Brasil poderá sofrer ataques cibernéticos nas redes 5G brasileiras no curto prazo de 5 anos;
- 57,3% (67 militares) do Graf 4.8 acreditam que o Com D Ciber e a ENaDCiber conseguirão capacitar militares das FA contra ameaças do 5G no médio prazo de 10 anos;
- 51,3% (60 militares) do do Graf 4.9 acreditam que o incentivo à pesquisa científica do 5G poderá ampliar a capacidade da Segurança Cibernética brasileira no médio prazo de 10 anos;
- 44,4% (52 militares) do Graf 4.10 acreditam que a Resiliência Cibernética nas redes 5G brasileiras poderá ser mantida no médio prazo de 10 anos;
- 54,7% (64 militares) do Graf 4.11 acreditam que as autoridades competentes conseguem orientar medidas contra ataques/incidentes cibernéticos no 5G atualmente;

- (xii) 56,4% (66 militares) do Graf 4.12 acreditam que o emprego do 5G no QGEx e QG CMP/11ª RM será viável no médio prazo de 10 anos; e
- 58,1% (68 militares) do Graf 4.13 consideraram o Grau de importância Cinco (extremamente importante) para essa pesquisa científica sobre todo o assunto abordado no Questionário Online.

Por todo, o exposto nesse Questionário *on-line*, pode-se concluir que a maioria do universo de 117 militares entrevistados, mais de 40% responderam que as novas tecnologias derivadas dos 3 serviços (eMBB, mMTC, e URLLC) do Ecossistema 5G Brasil, poderão ocasionar muitos benefícios à nação brasileira, à defesa e à segurança nacional, pois:

(i) 52,1% (61 militares) do Graf 4.3 acreditam nas vantagens estratégicas na Defesa brasileira no curto prazo de 5 anos, em relação aos 10 (dez) países vizinhos lindeiros na América do Sul, pelos seguintes motivos: por causa da quase totalidade da implantação do Ecossistema 5G Brasil nas grandes e médias cidades, além das principais rodovias federais nos próximos 5 anos, segundo os marcos previstos no Edital inicial da Anatel conforme [107], [152], e [23].

(ii) 46,2% (54 militares) do Graf 4.4 acreditam que o Ecossistema 5G Brasil no médio prazo de 10 anos ensejará vantagens estratégicas para o Brasil com o desenvolvimento econômico na geração de empregos diretos das operadoras vencedoras dos leilões da Anatel e empregos indiretos nos outros setores da economia brasileira [106].

Pois segundo dados da ITU, um aumento estimado de 10% na penetração da Internet móvel no Brasil potencializa o aumento do PIB anual em 1,2%, ao passo que um aumento de 10% na digitalização de um país pode incrementar ao PIB anual em 1,9% [106], enquanto que as Nações Unidas preveem que o uso de soluções 5G pode representar um benefício de R$ 590 bilhões por ano para a economia brasileira, e somente pela demanda potencial de software a expectativa total R$ 101 bilhões até 2031 [112].

Além disso as redes 5G poderão ser utilizadas diretamente no Agronegócio brasileiro, aumentando ainda mais sua eficiência, eficácia, e efetividade nas produções de grãos, café, algodão, para as empresas exportadoras, como estimam [26], [27].

A melhoria das redes móveis de comunicação celular 5G no Brasil se tornarão mais acessíveis economicamente com a redução dos impostos e o custo total de aquisição móvel **TCMO** termo em inglês para *total cost of mobile ownership* calculado pela proporção da renda mensal para 20% da população localizada nas faixas mais baixas de distribuição de renda (pacote de dados de 1GB) segundo [106], assim o Ecossistema 5G Brasil poderá possibilitar grande parte da inclusão digital popular esperada pela ITU com o lançamento do 5G Global em 2015 [22];

(iii) 52,1% (61 militares) do Graf 4.5 acreditam nas melhorias do 5G brasileiro nos Projetos Estratégicos das FA (Nuclear, Cibernético e Espacial) no curto médio prazo de 10 anos, tendo em vista as médias históricas de investimentos do Governo nas FA. Segundo o Livro Branco da Defesa Nacional versão de 2012 retrata que o Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres (PROTEGER) é o projeto do EB responsável literalmente proteger as 90% das Infraestruturas Críticas (IC) em terra, responsáveis por 56% da matriz energética e 96% do PIB do País. Já no [67] versa que o Brasil ocupou a 12ª colocação de 17 países com o maior volume de investimentos neste setor foi de

R$ 136 bilhões com total de 2% do PIB do ano de 2018, o qual chegou a marca de R$ 6,83 trilhões[1]; e

(iv) 93,2% (109 militares) do Graf 4.7 acreditam que o Brasil poderá sofrer ataques cibernéticos nas redes 5G brasileiras no curto prazo de 5 anos. Realmente existe essa possibilidade e o MD procura defender as IC de ataques cibernéticos por meio de operações realizadas pelo C D Ciber, sob supervisão do Com D Ciber, CERT.br e GSI.

4.2 SIMULAÇÃO DO *SOFTWARE HTZ WARFARE*

Para gerar a simulação da área de cobertura do sinal 5G com dados reais das ERBs locais no SMU, acessados por meio do *site* da Anatel [154], primeiro foi realizado um estudo na Área de Operações (áreas estratégicas) no SMU.

O Centro de Operações do Comando Militar do Planalto (C Op/CMP) é o setor responsável do CMP em planejar, coordenar e executar as ações de defesa e de seguranças pública e patrimonial das instalações físicas nas áreas estratégicas do SMU, além de realizar o C4ISTR (Comando e Controle, Comunicações, Computador, Inteligência, Vigilância, Aquisição de Alvos e Reconhecimento) para apoiar o processo de tomada de decisão do Cmt CMP, conhecido como **Ciclo OODA "Observar, Orientar, Decidir e Atuar"** [65].

As áreas estratégicas do SMU com os objetivos do Plano de Operações Hipotético Cerrado (POHC) estão ilustradas na Figura 4.14 – Áreas Estratégicas delimitadas SMU com Objetivos a seguir.

Figura 4.14: Áreas Estratégicas delimitadas SMU com Objetivos [74]

Para o leitor ter uma noção melhor das dimensões e características reais dessas áreas estratégicas defendidas pelas tropas do CMP, já organizadas no POHC. Visualiza-se uma imagem real produzida pelo *drone Mavic 2 Enterprise* no mês de dezembro de 2022, conforme ilustra a Figura 4.15 – Vista aérea das áreas estratégicas do SMU abaixo.

[1]Em [153] o PIB brasileiro cresceu 2,9% em 2022 e fechou o ano de 2022 em R$ 9,9 trilhões.

Figura 4.15: Vista aérea das áreas estratégicas do SMU [74]

Antes de realizar a simulação do sinal 5G nas áreas estratégicas do SMU, primeiro foi necessário realizar o levantamento de inteligência da área de cobertura do sinal 5G real no SMU. Assim, por meio da página eletrônica da operadora de telefonia móvel Claro DF <https://www.claro.com.br/mapa-de-cobertura>, obteve-se essa informação em dezembro de 2022, conforme demonstra a Figura 4.16 – Área de cobertura real do sinal 5G da operadora Claro, na região do SMU, em dezembro de 2022 a seguir.

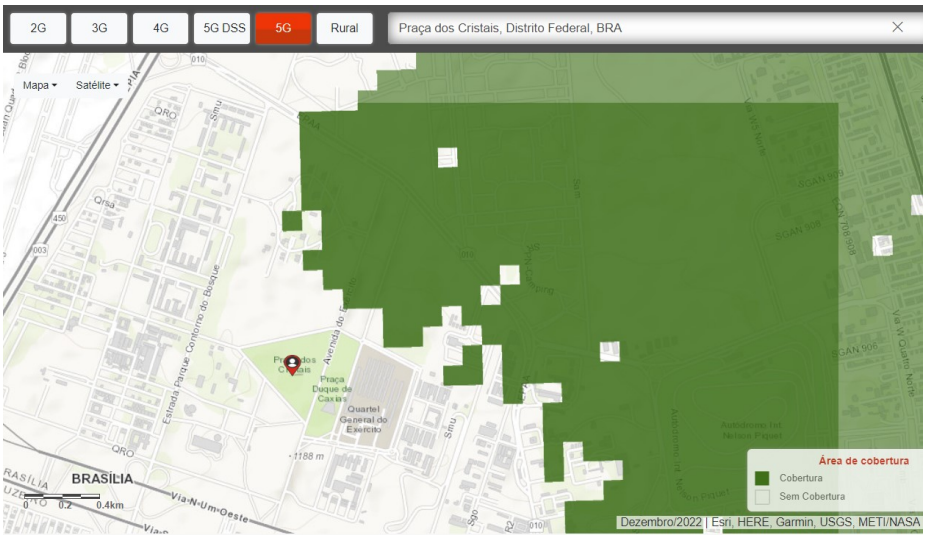

Figura 4.16: Área de cobertura real do sinal 5G da operadora Claro DF na região do SMU em dezembro de 2022 [74]

A partir das análises das imagens das Fig 4.14, Fig 4.15 e Fig 4.16, estima-se que área de cobertura do sinal 5G simulado será do tipo Macrocélula de sistema celular, a fim de contemplar o sinal 5G próprio do EB, realizando interseções úteis nas áreas de bordas dos sinais 5G da Operadora Claro DF no SMU. Ressalta-se que as áreas de instalação das Estações Rádio Base (ERBs) seriam nos aquartelamentos para aumentar a segurança das mesmas contra vandalismos ou furtos de cabos de cobre, além de manter a garantia do sinal 5G em todo o SMU quando aglutinado com o sinal 5G da Claro DF.

Dessa forma, com o estudo do terreno e das áreas sem sinais 5G fornecidos pela Claro DF, foi possível realizar os planejamentos das melhores posições para instalação de 18 (dezoito) torres das ERB 5G com

(*conteiner/shelter* composto por transceptores, cabos, conectores, banco de baterias, sistema de ar condicionado, sistema de para-raios e suas antenas ortogonais de painel plano) no SMU, foi utilizado o *software HTZ Warfare*[2].

O Centro de Instrução de Guerra Eletrônica (CIGE) realiza as instruções desse *software HTZ Warfare* para os oficiais e praças participantes dos cursos de GE/G Ciber anualmente em Brasília/DF. E também realiza seus planejamentos reais de emprego dos equipamentos de CEMA em apoio às operações do EB, para as tropas do 1º Batalhão de Guerra Eletrônica (1º BGE) distribuídas por todo o território brasileiro.

Para gerar a área de cobertura do sinal simulado 5G no *software HTZ Warfare* foram escolhidos 18 (dezoito) pontos geográficos para implantação das ERBs para o sinal 5G no SMU, segundo descreve a Tabela 4.14 – Coordenadas geográficas das 18 ERBs simuladas para a cobertura 5G no SMU a seguir.

Tabela 4.14: Coordenadas geográficas das 18 ERBs simuladas para a cobertura 5G no SMU

Locais	**Latitude**	**Longitude**
Ponto 1 – 32º GAC	15º45'46"S	47º55'26"O
Ponto 2 – 3º Esqd C Mec	15º45'52.53"S	47º55'28.60"O
Ponto 3 – Portaria Oeste VMG	15º45'54"S	47º55'24.62"O
Ponto 4 – Portaria Leste VMG	15º45'60"S	47º55'06.61"O
Ponto 5 – BGP	15º46'00"S	47º55'30"O
Ponto 6 – BPEB	15º46'12.08"S	47º55'33.40"O
Ponto 7 – 11º D Sup	15º46'20"S	47º55'40.20"O
Ponto 8 – Torre Central (Praça)	15º46'22"S	47º55'17.29"O
Ponto 9 – Torre 1 (Praça)	15º46'19.81"S	47º55'25.28"O
Ponto 10 – Torre 2 (Praça)	15º46'17.20"S	47º55'11.46"O
Ponto 11 – Torre 3 (Praça)	15º46'29.56"S	47º55'15.81"O
Ponto 12 – Torre 4 (Praça)	15º46'17.39"S	47º55'05.40"O
Ponto 13 – QGEx 1 (Oeste)	15º46'25.53"S	47º55'06.55"O
Ponto 14 – QGEx 2 (Sul)	15º46'30.21"S	47º55'05.05"O
Ponto 15 – QGEx 3 (Leste)	15º46'25.06"S	47º55'57.84"O
Ponto 16 – CMP 1 (Norte)	15º46'41.38"S	47º55'11"O
Ponto 17 – CMP 2 (Leste)	15º47'01"S	47º55'03.54"O
Ponto 18 – CMP 3 (Oeste)	15º46'44.54"S	47º55'44.46"O

Fonte: [74]

Os locais exatos de cada ERB implantada pelo *software HTZ Warfare* nas áreas estratégicas do SMU estão demonstrados na Figura 4.17 – Posições das ERBs no SMU implantadas pelo *software HTZ Warfare* abaixo.

[2]Em [155] a empresa francesa ATDI desenvolvedora do *software HTZ Warfare* disponibiliza um filmete com as principais funcionalidades, por meio da URL: <https://atdi.com/products-and-solutions/htz-warfare/>. Obs.: Clicar sobre o ícone do vídeo de 1'13"localizado no canto direito no meio da página para visualização.

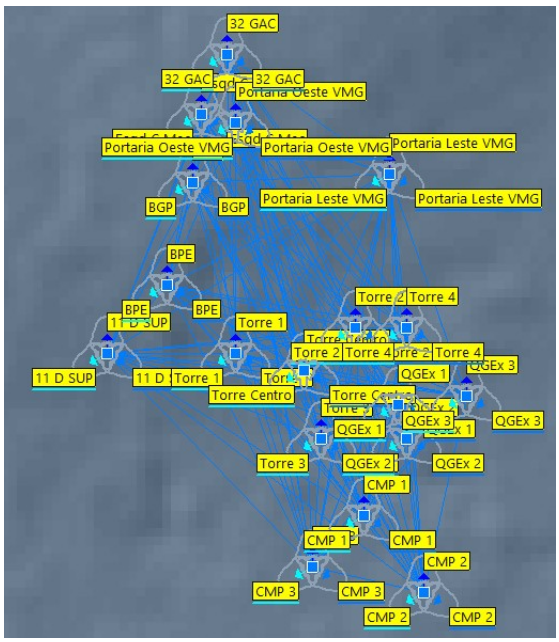

Figura 4.17: Posição das ERB simuladas pelo *HTZ Warfare* na região do SMU [74]

Posteriormente dentro do *software HTZ Warfare* foram configurados os parâmetros dos equipamentos das ERBs, para realizar a simulação do sinal 5G nas áreas desprovidas do sinal 5G real da Claro DF, conforme a Tabela 4.15 a seguir:

Tabela 4.15: Requisitos e parâmetros configurados para gerar a área de cobertura 5G simulada no *HTZ Warfare*

Requisito	**Parâmetro**
Altura da antena de transmissão (HTx)	35 m
Altura da antena de recepção (hRx)	1,5 m
Ganho da antena de transmissão (GTx)	15 dBi[3]
Ganho da antena de recepção (GRx)	15 dBi
Frequência da antena de transmissão (Tx)	3.500 MHz
Frequência da antena de recepção (Rx)	3.520 MHz
Banda utilizada Tx/Rx	80 MHz
Tipo da antena de transmissão	MU-MIMO
Setor da antena de transmissão	120º
Potência da antena de transmissão	50 W
Modulação da antena de transmissão	OFDM
Polarização da antena de transmissão	Vertical
Modelo de propagação do sinal	Padrão
Zona de Fresnel	Padrão

Fonte: [74]

Das informações da Figura 4.17 e da Tabela 4.15 foram implantadas 18 ERBs hipotéticas no *software HTZ Warfare* para gerar a cobertura do sinal 5G nas áreas de estratégicas do SMU que não estavam contempladas pelo sinal 5G real da Claro DF, a saber:

1. Regiões da Av. Duque de Caxias (sentido Norte-Sul): 1) 32º GAC; 2) 3º Esqd C Mec; 5) BGP; 6)

BPEB; 7) 11º D Sup;

2. Regiões da Vila Militar dos Generais (VMG) e Av. do Exército e Av. Duque de Caxias: 3) Portaria Oeste VMG e 4) Portaria Leste VMG;

3. Regiões exclusivas da Praça Cívica (Cristais): 8) Torre Central; 9) Torre 1; 10) Torre 2; 11) Torre 3; 12) Torre 4; e

4. Regiões do QGEx, QG CMP/11ª RM, e Av. do Exército: 13) Bloco A do QGEx (QGEx 1); 14) Bloco J do QGEx (QGEx 2); 15) Bloco H do QGEx (QGEx 3); 16) Torre N do CMP (CMP 1); 17) Ginásio Vera Cruz do CMP (CMP 2); 18) Torre S do CMP (CMP 3).

Como resultado das configurações inseridas no *software HTZ Warfare* pelas áreas não atendidas pela cobertura real da operadora Claro vista na Figura 4.16, gerou-se a simulação da área de cobertura do sinal 5G nas regiões estratégicas do SMU, conforme demonstra o produto final com a Figura 4.18 – Áreas de coberturas dos sinais simulados 5G no SMU a seguir.

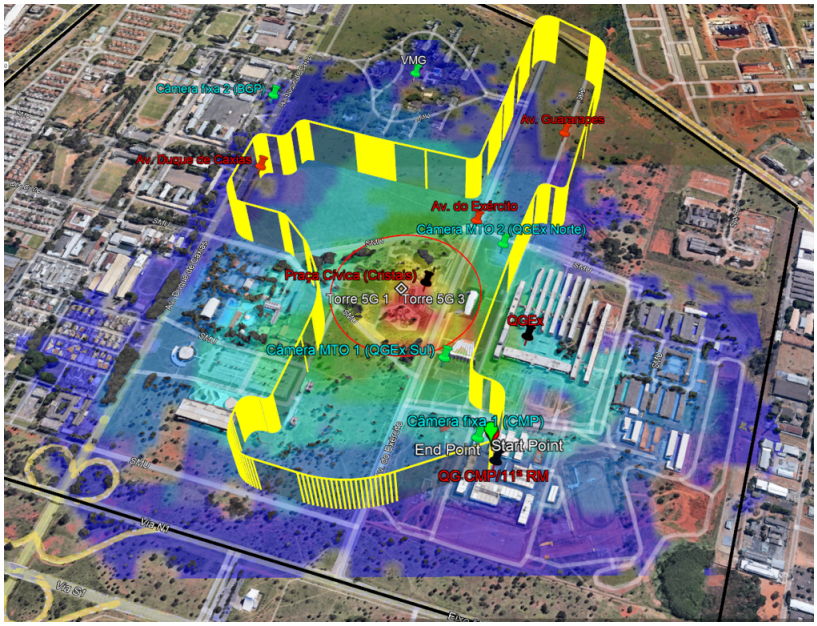

Figura 4.18: Áreas de coberturas dos sinais simulados 5G no SMU [74]

O *software HTZ Warfare* disponibiliza uma escala de cores em forma de rodapé na tela da simulação gerada, conforme demonstra a Figura 4.19 – Escala dos níveis dos sinais gerados no *software HTZ Warfare* a seguir.

Figura 4.19: Escala dos níveis dos sinais gerados no *software HTZ Warfare* [74]

Para o melhor entendimento do código de cores apresentado nas Figuras 4.18 e 4.19 do sinal simulado 5G no SMU gerado pelo *software HTZ Warfare*, foi criada a Tabela 4.16 – Legenda dos níveis dos sinais coloridos (*Clutters*) expressos nas áreas de coberturas 5G no SMU abaixo.

Tabela 4.16: Legenda dos níveis de sinais coloridos (*Clutters*) expressos nas áreas de coberturas 5G no SMU

Cores no simulador	**Nível do sinal dBuV/m**	**Nível do sinal dBm**
Azul escuro	79	-69
Azul médio	82	-66
Azul claro	84	-64
Verde claro	87	-61
Verde médio	89	-59
Verde escuro	91	-57
Amarela	94	-54
Laranja	99	-49
Vermelha	102	-46
Marrom	118	-30
Bege	129	-19

Fonte: [155]

Das assertivas acima, das análises das imagens das Figuras 4.16, 4.17 e 4.18 e das informações das Tabelas 4.15 e 4.16, as quais resultaram na imagem da Figura 4.18, infere-se que as áreas de coberturas mais próximas das ERBs nas cores Bege (129 dBuV/m ou -19 dBm) e Vermelha (-46 dBm) estão com os níveis de sinal 5G mais fortes e os níveis de ruídos mais fracos para os dispositivos de TIC presentes nessas áreas, por exemplo: *smartphones, tablets, laptops, drones* e câmeras WiFi, poderão ser integrados ao Servidor *Videowall* do C Op/CMP via Internet com maior velocidade de tráfego de dados *Download (DL) e Upload (UL)*) com a melhor qualidade do sinal 5G na região.

Enquanto que nas áreas de coberturas mais distantes das ERBs nas cores Verde claro (87 dBuV/m e -61 dBm) e Azul escuro (79 dBuV/m e -69 dBm) estão com os níveis de sinal 5G mais fracos para os dispositivos de TIC, o que é plenamente aceitável e esperado, devido às condições de propagação, modulação do sinal 5G e influências de diversos fatores ambientais (irradiação solar, temperatura, umidade, pressão atmosférica, altitude, relevo, vegetação, e trânsito no local) no SMU.

O critério que deve ser considerado na operação dos equipamentos de TIC é Relação Sinal-Ruído, do inglês (*Signal-to-Noise Ratio*) (SNR), que é uma medida relativa da potência do sinal recebido em um dispositivo de TIC, ou seja, é a informação transmitida mais o ruído [2].

Essa SNR costuma ser calculada em unidades de decibéis (dB), que é uma unidade de medida padronizada em função do cálculo de 20 (vinte) vezes a razão do logaritmo de base 10 da potência do sinal recebido à amplitude do ruído, dada pela fórmula:

Q(dB) = 20 log (V1/V2):

(**Q**) é a quantidade numérica da medida calculada em dB (decibel);

(**V1**) é resistência inicial do sistema; e

(**V2**) é resistência final do sistema

Da fórmula **Q(dB) = 20 log (V1/V2)** são calculados os valores lineares usando as resistências (V1/V2),

Tabela 4.17: Correspondência entre valores dB e valores Lineares

Q(dB)	**Linear V1/V2**
120	1.000.000
90	31 600
60	1 000
30	31,6
20	10
10	3,16
6	2
3	1,414
0	1
-3	0,707
-6	0,5
-10	0,316
-20	0,1
-30	0,0316
-60	0,001
-120	0,000001

Fonte: Adaptado de [157]

obtém-se os valores em dB, conforme a Tabela 4.17 – Correspondência entre valores dB e valores Lineares acima.

Os valores em decibéis (dB) são usados para se calcular diversos parâmetros nas telecomunicações, como a Relação Sinal-Ruído (*Signal-to-Noise Ratio* (SNR)) e a Taxa de Erro de Bits (*Bit Error Rate* (BER)).

Uma SNR é a razão entre o sinal emitido e seus ruído presente em um sistema eletrônico (telecomunicações, som, imagem, etc). Ou seja, uma SNR alta facilita ainda mais para o destinatário extrair o nível do sinal na informação recebida com um certo nível de ruído de fundo. Por exemplo: uma antena de recepção (Rx) com ganho de 20 dB significa que a mesma consegue captar 100 vezes mais o sinal recebido com a informação sobre o nível do ruído presente na informação transmitida sobre uma portadora de outra antena de transmissão (Tx). Ou seja, o sinal recebido (Rx) foi amplificado 100 vezes em relação ao sinal transmitido (Tx) [157].

Enquanto que uma atenuação de -3 dB em uma antena de transmissão (Tx) significa que o sinal transmitido por ela perdeu 2 vezes energia em relação ao sinal transmitido de outra antena (Tx) sem essa atenuação. Ou seja, o sinal foi transmitido pela antena (Tx) com metade da energia produzida pelo rádio liberada para essa antena [157].

Por fim, de acordo com as Tabelas 4.16 e 4.17 ainda existem boas possibilidades de exploração dos

equipamentos nessa nova área de cobertura do 5G no SMU, principalmente na área central da Praça Cívica nas áreas das cores Bege e Vermelha, pois dispõem dos melhores níveis do sinal 5G. Considerando-se que a maioria dos equipamentos celulares e dispositivos de TIC operam corretamente com limiares de sensibilidade (SNR) de até -100 dBm, estes poderão operar com algumas falhas com até -120 dBm.

4.3 POSSIBILIDADES DO EMPREGO MILITAR 5G NA DEFESA E SEGURANÇA BRASILEIRAS

A 10ª Conferência de Sistemas e Tecnologia Militar 2021 ocorreu de 23 a 26 de novembro de 2021, em Brasília/DF, no Estádio Nacional de Brasília Mané Garrincha. Contou com representantes das indústrias nacionais de defesa; autoridades diplomáticas e do governo; políticos; militares das Forças Armadas; integrantes da Segurança Pública; pesquisadores; estudiosos; jornalistas especializados; visitantes; e abordou diversas pesquisas e propostas sobre o emprego do 5G na esfera militar.

A Anatel sob coordenação da ITU estipulou as faixas de frequências para exploração comercial e governamental no Brasil [23], [27], [107]: (i) 700 MHz; (ii) 2,3 GHz; (iii) 3,5 GHz; e (iv) 26 GHz.

De acordo com [26] consideram-se as características de Cobertura, Capacidade e Latência das Redes Móveis do **Projeto 5G Brasil**, as quais estão sintetizadas dentro de cada faixa do espectro eletromagnético (EEM) distribuído para o Brasil pela Anatel, conforme demonstradas na Figura 4.20 – Diagrama de Cobertura, Capacidade e Latência das Redes Móveis 5G brasileiras a seguir.

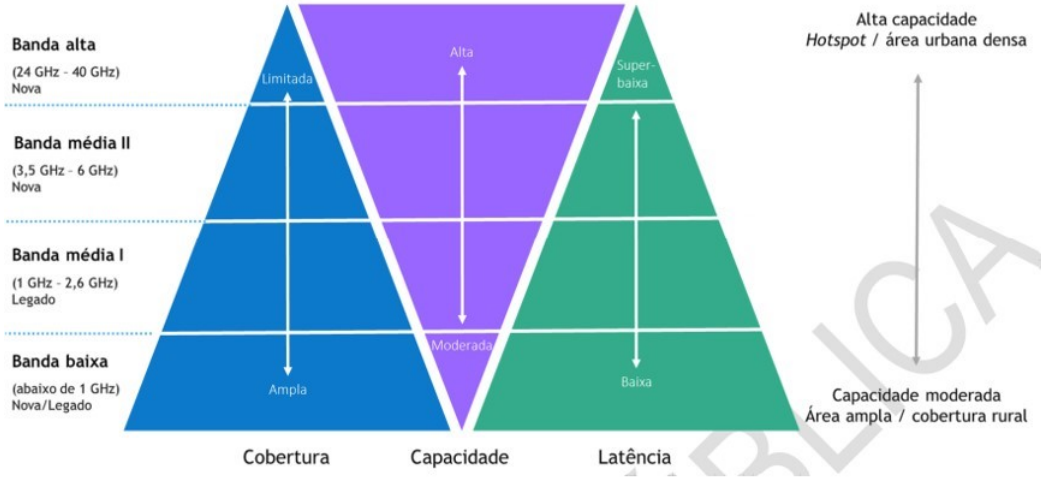

Figura 4.20: Diagrama de Cobertura, Capacidade e Latência das Redes Móveis 5G brasileiras [26]

A partir da análise da Figura 4.20 acima, obtemos a aplicabilidade nos contextos das diferentes faixas de radiofrequências que devem atender aos requisitos múltiplos designados pela ITU e Anatel para o Ecossistema 5G, focando nas qualidades das faixas do EEM para cada aplicação: eMBB, mMTC e URLLC [26], tais como:

(i) **Banda baixa** (abaixo de 1 GHz) Nova/Legado (e.g. 700 MHz) mais dedicada ao uso para Banda Larga

Móvel aprimorada/extrema (eMBB/xMBB), segundo [15], [11] (5G NR 2021) com uso amplo e onipresente abrange uma gama de casos de outros usos com diferentes desafios, incluindo aumento de antenas (*Hotspots*) para cobertura de áreas amplas, permitindo altas taxas de dados na capacidade de grande volume no tráfego de dados (1 Gbps *download* (DL) e 100 Mbps *upload* (UL)), alta densidade de usuários simultâneos e necessidade de capacidade muito alta de mobilidade em velocidades acima de 300 Km/h, e uma experiência de usuário perfeita com videogames e filmes 4K/8K Realidade Virtual (RV) e Realidade Aumentada (RA). O cenário da Banda Larga Móvel aprimorada/extrema é visto como a comunicação centrada no ser humano dentro do 5G;

(ii) **Banda média I** (1 GHz – 2,6 GHz) Legado (e.g. 2,3 GHz);

(iii) **Banda média II** (3,5 GHz – 6 GHz) Nova (e.g. 3,8 GHz); e

(iv) **Banda alta** (24 GHz - 40 GHz) Nova (e.g. 26 GHz).

Observa-se que as faixas de frequências infra 6 GHz são as mais baixas e oferecem ampla cobertura, porém com baixa disponibilidade de largura de banda. Enquanto que as faixas de frequências supra 6 GHz são as mais altas e oferecem grandes taxas de transmissão, grande confiabilidade e baixa latência, porém com área de cobertura muito menor chegando aos tamanhos das pequenas células (micro células, pico células e femto células).

De acordo com [15] as células pequenas (*Small Cells*) dão origem às outras células cada vez menores, fazendo com que as antenas saiam dos topos dos prédios altos ou colinas e desçam para o topo de prédios mais baixos ou para as laterais de prédios altos e, finalmente, para postes de iluminação e cabines de transporte públicos, às quais formam as pico células. Com a diminuição no tamanho da pequena célula ocorre também a redução nos níveis de potência irradiada das Estações Rádio Base (ERB) que chegam nos usuários móveis (UM).

O resumo com as características dos tipos das pequenas células estão descritas na Tabela 4.18 – Tipos de Pequenas Células (*Small Cells*) do Ecossistema 5G abaixo.

Da análise da descrição da Tabela 4.18 abaixo, infere-se que essas pequenas células são configuradas sob demanda e constituem uma rede sem fio de pequenas células cooperativas que possuem uma infinidade de conexões de alta velocidade para a rede móvel por meio do *Backhaul* [15].

Projeta-se a codificação de uma rede com ferramentas de sobreposição de redes, para fornecer comunicações robustas e mais econômicas para oferecer suporte aos serviços do 5G [15]. Por exemplo: as pico células são úteis nas ruas das cidades em áreas congestionadas, ao longo de rodovias e dentro de grandes edifícios públicos/privados. Agora, estas pequenas células quando instaladas dentro de construções (edifícios, aeroportos, universidades, etc) são denominadas de femto células e, podem ser abertas para todos os usuários, ou apenas para um seleto grupo de usuários pré-autorizados, denominados assinantes. Esse processo de aumentar a capacidade de tráfego numa área usando pequenas células é denominado de **densificação da rede**.

Mas existem limites de densificação de redes em áreas por causa da eficiência espectral máxima em cada frequência usada. Por exemplo na tecnologia 5G com Ondas milimétricas na banda da frequência de 60 GHz (57 GHz – 64 GHz) com Feixes Direcionais 3D as pequenas células correspondem a 50 pequenas

Tabela 4.18: Tipos de Pequenas Células (*Small Cells*) do Ecossistema 5G

Tipo	**Típica implantação**	**Usuários simultâneos suportados**	**Ambiente fechado**	**Ambiente aberto**	**Alcance**
Femto	Principalmente em ambientes residenciais e corporativos	Residencial: 4–8 usuários. Corporativo: 16–32 usuários	10–100 mW	0,2–1W	Dezenas de metros
Pico	Espaços públicos (interiores/exteriores; aeroportos, shopping centers, estações de trem)	64–128 usuários	100–250 mW	1–5 W	Dezenas de metros
Micro	Áreas urbanas para preencher lacunas de cobertura macro	sem valor	128–2568 usuários	5–10 W	Poucas centenas de metros
Metro	Áreas urbanas para fornecer capacidade adicional	> 250 usuários	sem valor	10–20 W	Centenas de metros
WiFi	Ambientes residenciais, de escritório e corporativos	< 50 usuários	20–100 mW	0,2–1 W	Poucas dezenas de metros

Fonte: Adaptado de [15]

células por Km2 [15]. Na referência [158] é mostrado que quase 400 Gbps/Km2 de capacidade podem ser alcançados mesmo com esquemas simples de modulação/codificação.

Já as grandes células externas são denominadas de macrocélulas (*macro cells*) e servem para suportar usuários de alta mobilidade e proporcionar maior alcance do sinal do centro para as bordas externas, conforme demonstra a Figura 4.21 – Diagrama de uma Rede 5G RAN completa da Ericsson nos EUA a seguir.

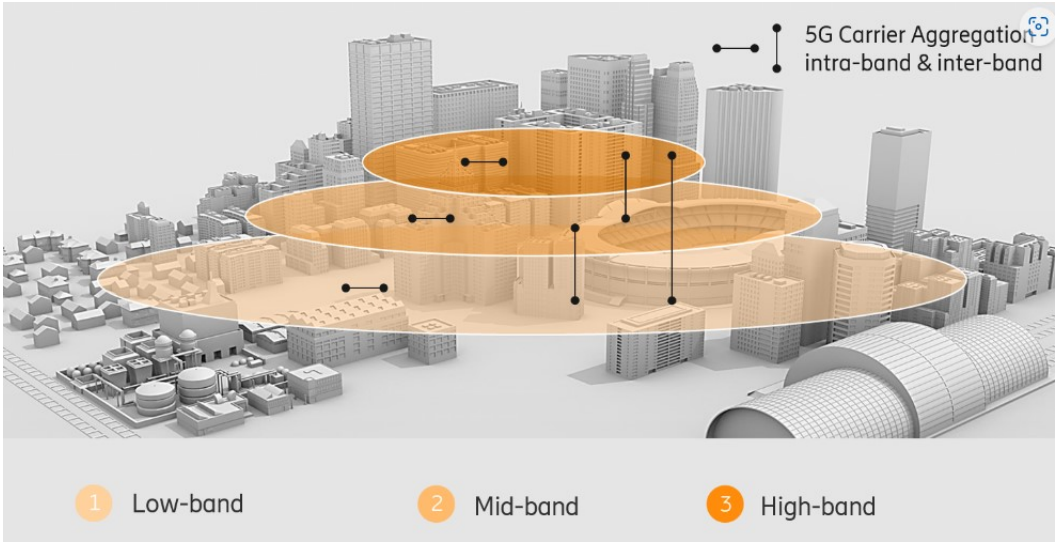

Figura 4.21: Diagrama de uma Rede 5G RAN completa da Ericsson nos EUA [159]

Da análise da Figura 4.21 acima, segundo a Ericsson, nos EUA, com o Compartilhamento Dinâmico de Espectro (*Dynamic Spectrum Sharing*) (DSS) a Banda Baixa (*Low-band*) (Nr 1) garante cobertura e penetração interna, a Banda média (*Mid-band*) (Nr 2) garante cobertura e capacidade em áreas Metropolitanas, e a Banda Alta (*High-band*) (Nr 3) garante serviços em áreas específicas.

Ainda, de acordo com [15] a densidade das macro células na rede varia dependendo de uma série de fatores, como objetivos de cobertura e a densidade de tráfego pelo número de usuários simultâneos. Na Europa e na América do Norte a densidade celular nos centros urbanos pode chegar a 5 células por km2, enquanto que na região da Ásia-Pacífico pode chegar de 20–30 células por Km², devido à demanda de tráfego significativamente maior do que na Europa e América do Norte (EUA, Canadá e México).

De acordo com [160] a arquitetura do 5G 3GPP está baseada em "Tecnologias Avançadas", enquanto que [161] propõe o termo "Tecnologias Chaves", as quais são as diversas inovações tecnológicas (e.g. Onda milimétrica, MIMO massivo, Redes Heterogêneas, SDN, NFV, Comunicação D2D) sobre o padrão atual das de redes móveis de comunicações sem fio do *4G LTE-Advanced*, tais como:

1. **5G *New Radio* (5G NR) nos Sistemas de Comunicações Estratégicos do MD e das FA (MB, EB e FAB)**: esta tecnologia de acesso foi concebida para a interface aérea do 5G. Existem duas gamas de frequências, altas e baixas, que o 5G NR usará para suportar altas taxas de dados e a reutilização intensiva de frequências por meio do *Backhauling*, assim como do *Fronthauling* usadas nas redes de fibras ópticas metropolitanas das diversas ERBs espalhadas nos *Clusters* dos sistemas 5G e dos sistemas legados 4G/3G. Com esse 5G NR será possível estabelecer diversas redes rádio virtualizadas e com diversos serviços para as Organizações Militares (OM) adotantes.

2. **Redes Heterogêneas (*HetNets*) em Bases Militares/Hospitais Militares/Escolas Militares**: segundo [3] o conceito de Redes Heterogêneas é usado para explicar que o 5G proporciona o uso concomitante das diversas tecnologias legadas do 4G/3G, pois o 5G abrange a multiplicidade de arquiteturas, camadas e tipos de tecnologias de Rádio de Acesso à Rede (5G RAN), como as novas tecnologias do Rádio de Acesso Tecnológico (5G RAT) [22], Rádio de Acesso por Rede-Nuvem (*Cloud-RAN*) [3] e do *5G New Radio* (5G NR) [18].

   Elas também podem ser consideradas multicamadas [15] pois utilizam as pequenas células (*small cells*) de baixo consumo de energia elétrica e maior eficiência espectral do EEM nas ERBs, as quais podem ser classificadas como: micro, pico e femto células [8].

   Elas possibilitam reutilizar as frequências das ERBs já implementadas nas gerações anteriores 4G/3G nas cidades por meio do *Fronthaul* via comunicação cabeada (fibra óptica ou cabo coaxial de cobre) ou via aérea tipo micro-ondas. Dentro da mesma célula pequena ocorre a comunicação das Unidades Rádio Remotas do 5G NR (*Remote Radio Units* (RRUs[4])) para as Unidades de Bandas Bases Digitais das antenas (*Digital Baseband Units* (BBUs[5])), geralmente via fibra óptica e cabos coaxiais de cobre (sempre em dupla) dentro da ERB, e também via enlaces de micro-ondas, conforme demonstra a

[4]Em [14] as Unidades de Rádio Remotas (RRUs) convertem as informações do sinal digital fornecidos pelas BBUs através de um cabo de fibra óptica para as antenas. Essas RRUs também são necessárias para amplificar o sinal de RF gerado para níveis entre 10 – 200 W, dependendo da largura de banda da operadora e da faixa das células desejadas.

[5]Em [14] as BBUs são responsáveis pelo gerenciamento geral de uma célula e pela geração e decodificação do sinal da BBU para 2G, 3G e 4G.

Figura 4.22 – Esquema de ligações *Fronthaul* entre RRUs e BBUs via fibra óptica na ERB e *Backhaul* via fibra óptica entre BBUs de ERBs diferentes (foras da figura) abaixo.

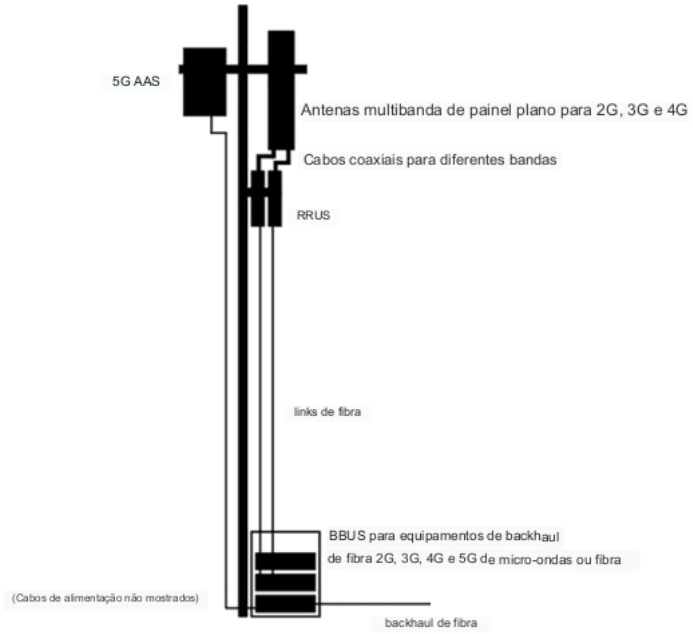

Figura 4.22: Esquema de ligações *Fronthaul* entre RRUs e BBUs via fibra óptica na ERB e *Backhaul* via fibra óptica entre BBUs de ERBs diferentes (foras da figura) [14]

Também dentro das diversas ERBs presentes nas Redes Heterogêneas ocorrem a comunicação por meio do *Backhaul*, que é a conexão entre as BBUs das ERB com a Estação de Comutação (*Optical Management Entily*), as quais podem ocorrer via cabos de fibra óptica, cabos coaxiais de cobre e enlaces de micro-ondas dentro das macrocélulas, devido às redes de fibras ópticas já estarem instaladas para os sistemas legados 4G/3G (áreas metropolitanas) e 2G (áreas rurais), conforme demonstra a Figura 4.23 – Interligação *Backhaul* das Macrocélulas com as Microcélulas no Ecossistema 5G a seguir.

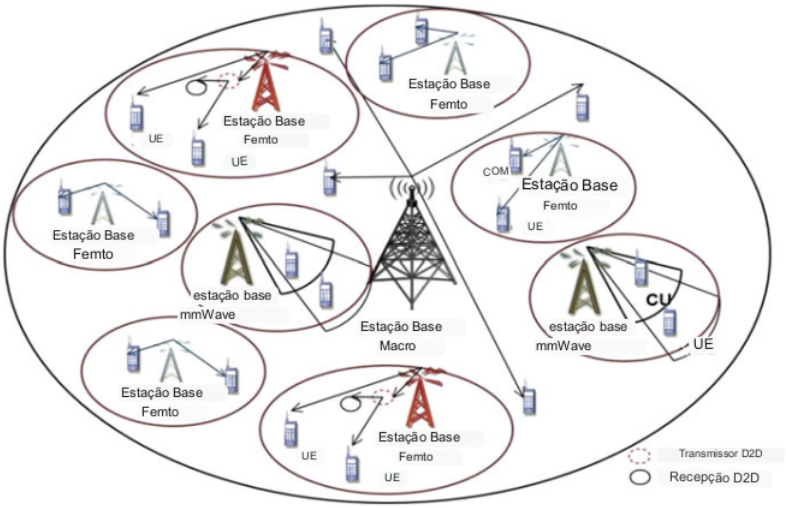

Figura 4.23: Interligação *Backhaul* das Macrocélulas com as Microcélulas no Ecossistema 5G [21]

3. **Ondas mm nos Sistemas de Telecomunicações Satelitais e Sistemas de Comunicações Terrestres para Treinamentos e Operações das FA (MB, EB e FAB)**: derivadas das faixas de frequências de 30 GHz – 300 GHz [14] as Ondas mm são utilizadas para melhorar o desempenho das Redes Heterogêneas em termos de altas taxas de tráfego (DL/UL) de dados, baixas/super baixas latências e variáveis áreas de coberturas do sinal desde pequenas células até macrocélulas [18]. A WRC-19 liberou as faixas de frequências Ondas mm de 24.25 GHz – 27.5 GHz, 50.4 GHz – 52.6 GHz e 81 GHz – 86 GHz [14]. No entanto, na transmissão de dados via Ondas mm, estas podem sofrer muitas perdas de pacotes devido aos sinais serem mais propensos às interferências ambientais quando eles ultrapassam objetos físicos (absorção e refração) e também quando ocorrem perdas de potência no multipercurso (reflexão e difração) ou quando sofrem o efeito Doppler em áreas urbanas muito movimentadas, isto quando comparadas às Ondas centimétricas utilizadas n 4G-LTE, WiMAX (IEE 802.16) e WiFi (2,4 GHz, 5 GHz e 6 GHz) [3], [8], [14].

4. **Comunicações D2D (comunicações de Dispositivos para Dispositivos) nas Bases Logísticas e Parques de Manutenção** – são definidas como dois nós que se comunicam diretamente sem atravessar uma ERB ou uma rede central, assim elas podem ocorrer nas frequências dos celulares 5G ou de faixas do espectro tipo WiFi muito usados para controle de mercadorias, produtos e veículos em estoque. Essa tecnologia é ideal para realizar o controle automático do suprimento das OM de Logística, por meio de robôs e de veículos autônomos (*drones*, carros, etc).

5. **Redes Definidas por Software (SDN) estabelecidas nos Grandes Comandos Operacionais nas Áreas de Operações de Adestramento e nas Áreas de Operações reais**: esta abordagem de gerenciamento de Redes permite a configuração de uma Rede Dinâmica e programação eficiente para obter maior flexibilidade de uso de frequências e de níveis de alcance distintos, com maior solução de problemas de acesso em comparação com a configuração descentralizada e complexa das Redes de dados tradicionais (e.g. *Ethernet, Mesh e WiFi*).

6. **Virtualização de Funções de Rede (NFV) nas Redes Heterogêneas**: esta é uma abordagem de Rede Avançada que permite dispositivos de rede baseados em software que funcionam como máquinas virtuais nos servidores para substituir dispendiosos dispositivos de *hardwares* dedicados para determina função na rede, como roteadores e *firewalls*. A NFV pode alcançar melhor escalabilidade, elasticidade e adaptabilidade em redes de alto desempenho, com custos mais baixos de manutenção, em comparação com as tecnologias das redes tradicionais (e.g. *Ethernet, Mesh e Wi-Fi*).

7. **Fatiamento da Rede em Áreas de Postos de Comando**: esta é a forma de arquitetura de Rede Virtual Fatiada em camadas de acesso. Tem os mesmos princípios daqueles por detrás das SDN e NFV em uma Rede fixa. CPorém, com o Fatiamento da Rede surgem diversas redes virtuais em cima de uma infraestrutura física comum e compartilhada para diferentes aplicativos, conforme demonstra a Figura 4.24 – Fatiamento da Rede no Ecossistema 5G abaixo.

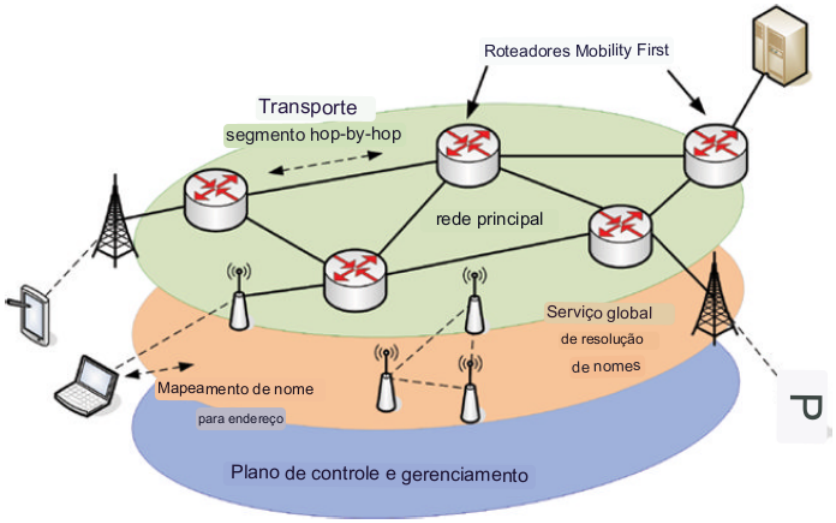

Figura 4.24: Fatiamento da Rede no Ecossistema 5G [15]

8. **Antenas Ortogonais em Arranjos com OFDMA para Sítios de Antenas em Operações militares**: antenas especiais contendo tecnologias de Feixes Direcionais Analógicos, Digitais e Híbridos (*Beamformings Analogic, Digital and Hybrid*) e acessos de Usuários Massivos–Múltipla Entrada e Múltipla Saída (*Massive Users–Multiple Input Multiple Output (MU-MIMO)*). As tecnologias de multiplexação dos 5G RAN que usam Multiplexação por Divisão Ortogonal de Frequência de Acesso (OFDMA) estão conseguindo recompor as portadoras com os pacotes (*bits*) na informação e as Antenas Ortogonais Painéis Planas com conjuntos de 64, 128, 256, 512, 1.024 e até 4.028 microantenas conseguem maior eficiência espectral do EEM com menor gasto de energia elétrica. Estão sendo usadas tecnologias MU-MIMO com Feixes Direcionais (analógico, híbrido e digital) para suprir as atenuações das Ondas mm no Ambiente Operacional [162]. Um estudo da GSMA apontou as frequências de 3,5 GHz, 26 GHz, 40 GHz e 66–71 GHz importantes para o Brasil utilizar no 5G [26].

   Abaixo a Figura 4.25 – Esquema contento uma Antena Ortogonal Painel Planar com 128 microantenas com tecnologias MU-MIMO (8x2 MIMO e 16x2 MIMO) com Direcionamento de Feixes (analógico, digital e híbrido) demonstra o aprimoramento do sinal 5G entre a antena e o aparelho do usuário.

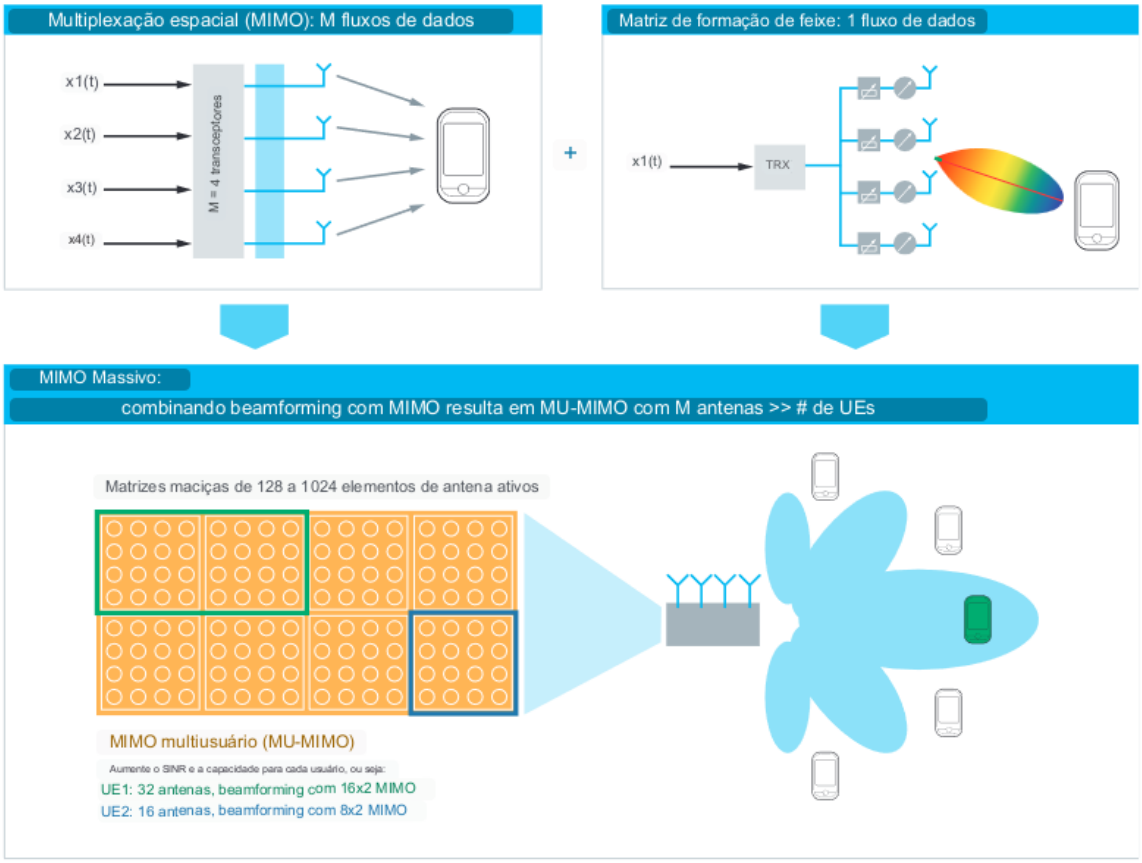

Figura 4.25: Esquema contento uma Antena Ortogonal Painel Planar com 128 microantenas com tecnologias MU-MIMO (8x2 MIMO e 16x2 MIMO) com Direcionamento de Feixes (Analógico, Digital e Híbrido) [162]

A [163] previu melhorias do 5G 3GPP em relação ao padrão do 4G LTE-A no ano 2018, que foram se confirmando pelos lançamentos (*releases*) 15 a 17, pela ITU, a cada ano de 2015 até 2022, a saber:

(i) incremento na taxa real de tráfego de 1 até 20 Gbps;

(ii) maior largura de banda por unidade de área 1.000 vezes maior;

(iii) alto número de dispositivos conectados com densidade 100 vezes maior (IoT);

(iv) percepção de 99% pelo usuário;

(v) cobertura total para 100% disponibilidade de conectividade;

(vi) redução de 90% no consumo de energia em dispositivos de baixa potência;

(vii) lançamento de baterias de longa duração, estimadas até 10 anos de vida útil; e

(viii) baixas/super baixas latências na ordem de 1 ms.

Das assertivas acima, infere-se que o Ecossistema 5G Global possibilitou algumas melhorias na Defesa dos países estrangeiros estudados, assim como o nosso **Ecossistema 5G Brasil** poderá possibilitar na Defesa e Segurança brasileiras as seguintes melhorias:

1. **Empregar câmeras com Inteligência Artificial (IA) e Aprendizado de Máquina (ML) na Segurança Orgânica de OM**: nas vigilâncias públicas e nos setores responsáveis pelas defesa e segurança das infraestruturas críticas: geração/transmissão/distribuição de energia elétrica derivadas do petróleo e de outras fontes renováveis (hidrelétrica, eólica, solar, ondas do mar, etc);nas estações de tratamento de água/esgoto, nas telecomunicações, nos setores financeiro/bancário, no controle do tráfego urbano nas cidades e estradas com IA, controle dos transportes (aquático, terrestre e aéreo) urbanos, na produção industrial/fabril com robótica e IoT, na distribuição e logística de produtos realizados automaticamente, nas áreas de segurança alimentar (agronegócio e extrativismo vegetal) no controle de dispositivos de análise de solo, rios, plantações, vigilância do perímetro das propriedades com drones e controle de rebanhos com dispositivos RFI fixados nos animais.

2. **Empregar exames de *drones* para Inteligência pelo EB**: para observação, filmagem e acompanhamento de Agentes Perturbadores da Ordem Pública (APOP) nas cidades e nas estradas de acesso, visando acompanhar em tempo real os deslocamentos das Organizações Criminosas (ORCRIM) durante as operações de repressão aos ilícitos transnacionais nas áreas das fronteiras terrestres e marítimas brasileiras.

3. **Empregar exames de *drones* ofensivos pela FAB**: para realizar ataques cinéticos com mísseis, foguetes ou granadas contra alvos estratégicos militares, infraestruturas críticas inimigas e também contra tropas inimigas lotadas no território amigo.

4. **Empregar Aeronaves Remotamente Pilotadas (ARP) como plataformas aéreas de comunicações pelas FA (MB, EB e FAB)**: para fornecer comunicações móveis de alta velocidade e imagens *FullHD* ao vivo em operações militares, do tipo Operação Ágata na faixa da fronteira terrestre brasileira das regiões Sul e Centro Oeste, e operações federais delegadas do tipo Intervenção Militar, como ocorreu no RJ nos anos de 2018 a 2020, quando as FA assumiram o combate direto contra as Organizações Criminosas (OrCrim) tutelando as Polícias Federal, Civil e Militar do RJ.

5. **Empregar Veículos Hiper Planados (HGV) na FAB**: no território nacional, deve-se estimular o emprego de aeronaves em altitudes mais baixas até 3.000 pés (cerca de 1.000 m) para evitarem os sistemas de defesa antiaérea inimigos, a fim de fornecer o sinal de 5G para as tropas em solo e, consequentemente, realizar a coleta/busca de dados estratégicos nos países vizinhos às fronteiras brasileiras durante as campanhas de Inteligência, preferencialmente desde a situação de Paz, pré-conflito e, principalmente, na situação de Guerra.

6. **Empregar robôs com sistemas de armas automáticas**: para realizarem a desativação/destruição de explosivos e/ou recolhimento de agentes químicos, biológicos, radiológicos e nucleares deixados em invólucros suspeitos em vias públicas, em locais fechados tipo estádios/ginásios de esportes ou locais de aglomeração de pessoas em atividades ao ar livre como em *shows* em praias e parques.

7. **Empregar Inteligência Artificial (IA) e Aprendizado de Máquina (ML) nas Bases Logísticas Inteligentes das FA (MB, EB, e FAB)**: para incrementar um controle de estoque automatizado com Identificador por Frequência de Rádio (RFID) colado nos Materiais de Emprego Militar (MEMN), fornecer suprimentos em todas as classes automaticamente, prover dados médios de planejamento em Nuvem Corporativa para o MD e para cada FS (MB, EB e FAB) acessarem pela ROD, proporcionar

o controle das frotas de navios, aeronaves e veículos terrestres, realizar a manutenção com maior escala de serviço e distribuição com eficácia, eficiência e efetividade desde a situação de Paz.

8. **Empregar IA e ML nos Hospitais de Campanha Inteligentes**: possibilitar uma comunicação massiva entre os diversos equipamentos hospitalares ligados em *HetNets*. E utilizar Redes de Área Corporal Médica (*Medical Body Area Network* (MBAN) [3]) para monitorar pacientes nos leitos do hospital e também pacientes na ambulância de emergência com microdispositivos subcultâneos implantados operando na banda de 2,4 GHz. Acredita-se que a Telemedicina no Campo de Batalha poupará um número maior de vidas dos militares feridos em combate pela agilidade nas cirurgias remotas realizadas por médicos cirurgiões especialistas civis e/ou militares, será um melhor emprego das tropas de saúde com rapidez.

9. **Empregar equipamentos vestíveis de Internet das Coisas para o Campo de Batalha (IoBT) nos Adestramentos e nas Operações reais**: equipamentos individuais e coletivos, armamentos e dispositivos de IoTC [125] visando aumentar as capacidades no Projeto Estratégico COBRA (Combatente Brasileiro) desenvolvido pelo EB atualmente em parceria com algumas Indústrias Nacionais de Defesa brasileiras.

10. **Empregar sistemas de comunicações mais seguros nos Grandes Comandos e nas Grandes Unidades com Redes Neurais, IA, ML e *Blockchain***: para atender aos níveis Operacional e Móvel Tim com antenas direcionais ortogonais especiais do tipo Ondas Milimétricas, a fim de entregar maior capacidade de taxas de dados (*bits*) e com antenas setoriais e tecnologias de Feixes direcionais tipo Antenas Ortogonais Planas MU-MIMO (*Beamforming*[6]), visando fugir das ações da CEMA inimiga realizadas contra a interface aérea do 5G, favorecerá o sigilo das tropas em deslocamento para as áreas de conflitos, assim como facilitará as Com durante o Ataque Coordenado e a Perseguição nas Operações Ofensivas e facilitará as Com sigilosas durante as Ações Defensivas e de Segurança de Área de Retaguarda.

11. **Empregar equipamentos de Realidade Aumentada (RA) e de Realidade Virtual (RV) nos Adestramentos e Operações reais**: para realizar os treinamentos e adestramentos nas escolas de formações militares da MB, EB e FAB. Por meio de simuladores virtuais de veículos aquáticos, terrestres e aéreos, como também na simulação viva dos alunos com o uso de armamentos coletivos e individuais em situações críticas de combate (tipo um *paintball virtual*, certificar o adestramento das tropas de cadetes e de alunos com redução no consumo de munições reais e de insumos de manutenção reais de viaturas, aeronaves e embarcações caso fossem empregados os meios reais.

12. **Empregar a Computação Confiável por meio da *Blockchain*) nos diversos órgãos do Sistema Brasileiro de Inteligência[7] (SISBIN)**: para realizar a criptografia/decriptografia das comunicações

[6]Em [4] descreve que *Beamforming* é uma das tecnologias chave do 5G NR, pois com Múltiplo Acesso por Divisão de Frequências Ortogonais (OFDMA) e MU–MIMO das antenas é possível superar o desvanecimento mais grave na propagação de ondas milimétricas.

[7][164] o SISBIN é formado pelos Sistema de Inteligência de Defesa (SINDE) e Sistema de Inteligência Operacional (SIOP). O SINDE é responsável em planejar e executar a Atividade de Inteligência de Defesa, visando assessorar o processo decisório do Ministério da Defesa (MD) e auxiliar na elaboração do Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA) de cada C Mil A. Enquanto que o SIOP é responsável em planejar e executar a Atividade de Inteligência Operacional, visando assessorar o processo decisório das Operações Conjuntas (Op Cj), desde o tempo de Paz, bem como manter um banco de dados que sirva de base para os Planejamentos Operacionais e para os Comandos Operacionais, quando ativados.

digitais entre os diversos órgãos de Inteligência do SISBIN responsáveis pela Defesa e Segurança brasileiras, tais como: GSI/PR, MD, FA (MB, EB e FAB), MJ (PF, PRF e FN), PM, CBM, e demais Agências Nacionais Governamentais (RFB, IBAMA, Defesa civil, entre outros órgãos da APF).

Em síntese dos exemplos supracitados existem diversas Tecnologias Avançadas/Tecnologias Chaves derivadas do Ecossistema 5G atual que podem ser incrementadas na Defesa e Segurança brasileiras. Os equipamentos de IoBT, HetNet, SDN, NFV, Redes Neurais, Redes Não Terrestres (RNT), Aprendizado de Máquina (ML), Inteligência Artificial (IA), Computação em Nuvem, Antenas Ortogonais e Rádios de Ondas mm, Mineração de dados com outros sistemas de aplicações distribuídas e equipamentos de TIC para o Estado Brasileiro.

De acordo com [75] o **Ecossistema 5G Brasil** poderia ser implementado junto ao SISFRON para a defesa brasileira tanto nas cidades da Faixa de Fronteira dos Estados das regiões Centro-Oeste e Sul, como nas áreas rurais interiores do Brasil com o uso satelital, com canais de frequências na faixa de 26 GHz (24,3 GHz – 27,5 GHz) para entregar comunicações (VoIP/Dados) e sinal de Internet para as OM das FA e para as repartições públicas como: (i) universidades; (ii) escolas; (iii) postos de saúde; (iv) hospitais; (v) prefeituras; (vi) estradas; (vii) praças e parques de lazer; e (viii) estádios e ginásios de esportes.

O Ecossistema 5G Brasil também pode ser empregado nas regiões urbanas, semiurbanas e rurais com canais de frequências nas faixas infra 6 GHz (e.g. 700 MHz) com maiores áreas de cobertura e grande capacidade de comunicação de borda (eMBB), enquanto que as frequências intra 6 GHz (2,3 – 3,5 GHz) possibilitarão capacidades equilibradas nas áreas de cobertura e acessos de diversos dispositivos eletrônicos simultâneos (mMTC) para atuarem na segurança pública de instituições e prédios públicos com sistemas de câmeras de vigilância IP com IA e sistemas de alarmes inteligentes com ML.

Na Defesa podem ser usados com sistemas de vigilância com sensores diversos (radares terrestres, aéreos e navais) com maiores velocidades de respostas, bases inteligentes com automação industrial e robótica, emprego de *drones* autônomos para monitoramento dos campos de instrução e dos perímetros externos em torno dos aquartelamentos, assim como para o monitoramento de estradas e vias de acesso com câmeras IP de alta resolução para dar o alerta antecipado, além de *drones* e veículos autônomos de resgate para situações de busca e salvamento de tropas isoladas em áreas de difícil acesso humano ou de risco de morte iminente.

Das assertivas acima e de acordo com [124], [125], [128], [130], [161], conclui-se que as várias tecnologias do 5G baseadas nos 3 serviços (Banda Larga Móvel aprimorada (eMBB), Comunicações Tipo Máquina massivas (mMTC) e Comunicações Ultra-Confiáveis e Baixa Latência (URLLC)) possibilitarão a melhoria de diversas aplicações para “Missão Crítica” na coleta de dados em tempo real com sensores diversos, nas comunicações pervasivas e onipresentes em áreas civis e áreas militares, desenvolvidas para a Defesa nacional, favorecendo a Segurança pública e o desenvolvimento geral do Brasil.

4.4 LIMITAÇÕES DO EMPREGO MILITAR DO 5G NA DEFESA E SEGURANÇA BRASILEIRAS

De acordo com [160] a base da arquitetura 5G deve contar com novos modelos de confiança adotados em diferentes aplicações na arquitetura do 5G RAN (*Radio Access Network*), em tradução literal Rádio de Acesso à Rede, tais como: (i) função de gestão de acesso e mobilidade (AMF); (ii) função de gestão de sessão (SMF); (iii) gestão unificada de dados (UDM); (iv) função de servidor de autenticação (AUSF); e (v) função de controle de políticas (PCF). Esses novos modelos de confiança podem afetar significativamente o projeto do mecanismo de segurança e os novos modelos de entrega de serviço 5G trarão novas vulnerabilidades de segurança e privacidade devido ao aumento dos vetores de ataque.

Segundo estudos próprios da ITU apontaram algumas limitações e desafios no emprego do 5G atualmente, tais como:

1. **EEM é um recurso escasso, muito valioso financeiramente (U$ e R$)**: há intensa competição das operadoras na compra de faixas disponibilizadas pela ITU, por exemplo nos níveis: regional, nacional e internacional. Dado que o espectro radioelétrico está dividido em faixas de frequências atribuídas a diferentes serviços de radiocomunicações, onde cada faixa deve ser utilizada apenas pelos serviços atribuídos, com condição técnica estabelecida para que possam coexistir entre si, sem criar interferências prejudiciais aos serviços adjacentes pré-definidos pela ITU.

2. **Necessidade de gastos com o maior uso do EEM licitado pela Anatel**: a necessidade de aumentar a densificação de antenas nas áreas do 5G, com aquisição de tecnologias com maior eficiência espectral como as Antenas Ortogonais para Ondas milimétricas com feixes direcionais eletrônicos (*Beamforming*) e altas capacidades de processamentos MU-MIMO, em quantidades muito maiores dos sistemas 3G/4G já implantados, por causa da capacidade aumentada de usuários móveis simultâneos e das taxas de dados habilitadas pelo 5G em até Gbps.

3. **Consumo de parte do EEM de bandas de frequências acima de 24 GHz, que representam desafios técnicos consideráveis**: por causa das características intrínsecas de propagação das Ondas milimétricas (*mmWaves*) que sofrem atenuações mais facilmente no meio de propagação por: absorção, refração, difração, reflexão e perdas no caminho. Essas ondas de rádio se propagam em distâncias muito mais curtas do que as bandas de frequências médias entre 1 – 6 GHz e das bandas de frequência abaixo de 1 GHz, exigindo um número muito maior de antenas e maior proximidade da ERB para realizar uma cobertura eficiente nas áreas definidas.

4. **A cobertura de uma determinada área exigirá um número significativamente maior de estações rádio base (ERB)**: esse fator aumenta a complexidade da infraestrutura, incluindo a necessidade de implantação de equipamentos de rádio em instalações viárias aéreas e subterrâneas nas localidades, tais como: semáforos, postes de iluminação, postes de alimentação de energia elétrica, estações de ônibus e de metrô, telhados, *outdoors*, bueiros, etc.

5. **Os enlaces de conexão 5G entre as ERB com a Rede Central (*Core Net*) dependem tanto de tecnologias de fibra óptica, quanto tecnologias sem fio (*Wifi, Mesh, WiMax*)**: é necessário um

trabalho considerável para implementar serviços de fibra óptica e garantir a disponibilidade de soluções de reuso das frequências com *Fronthauling e Backhauling* sem fio com capacidades suficientes para realizarem as comunicações entre as macro células e as micro células. Podem ser utilizados também enlaces de micro-ondas e enlaces satelitais e, potencialmente, outros sistemas de Estações de Plataforma de Alta Altitude (*High Altitude Platform Station (HAPS)*) em balões atmosféricos ou Aeronaves Remotamente Pilotadas (ARP), os quais poderão ser implantados nas cidades grandes ou áreas semiurbanas mais povoadas.

6. **Exigência de regulamentações internacionais e nacionais, que precisam ser adotadas e aplicadas globalmente e nacionalmente**: a fim de evitarem a interferência mútua entre os serviços do 5G, visando criar um ecossistema móvel viável para o futuro da humanidade, reduzir os preços dos serviços por meio das economias escaláveis nos mercados Global e Nacional, e permitir a interoperabilidade e o *roaming* entre os equipamentos dos usuários de diversas redes.

De acordo com [165] a arquitetura do 5G prevê outros desafios para serem vencidos, tais como a autointerferência dos equipamentos durante o uso *Full-Duplex* (FD) e o combate aos desvanecimentos de larga escala (sombreamento pelo relevo, vegetação, prédios, etc) e desvanecimento de pequena escala (comportamento aleatório das componentes do sinal que chegam ao receptor em curtas distâncias ou pequenos intervalos de tempo) e perdas no multipercurso (*multipath fading*) (vários mecanismos de propagação gerados pelo ambiente, geralmente reflexão e difração) das Ondas milimétricas (*mmWaves*) interagindo nos objetos e nos meios de propagação, conforme demonstra a Tabela 4.19 – Taxas de atenuações em dB do sinal sem fio 5G contra materiais durante a sua propagação a seguir.

Tabela 4.19: Taxas de atenuações em dB do sinal sem fio 5G contra objetos durante a sua propagação

Taxas de atenuação na propagação	**Materiais**
3 dB[8]	Janela
3 a 5 dB	Placa de gesso/*drywall*
4 a 6 dB	Parede de bloco
6 dB	Parede de vidro e estrutura de metal
6 a 10 dB	Porta de metal
6 a 15 dB	Parede de concreto

Segundo [159], [91] uma forma de solucionar parte desse problema de desvanecimento das Ondas milimétricas no espaço físico é aumentar a quantidade dos arranjos de antenas MU-MIMO (*Multi-User Multiple-Input Multiple-Output*), a quantidade de antenas com feixes direcionais (*Beamforming*) e aumentar o reuso das frequências (*Fronthaul*[9]) nas fibras ópticas de ligação entre as ERB locais do tipo multimodo, e aumentar também o reuso (*Backhaul*[10]) das frequências usadas nas plataformas aéreas das ERB

[9]Em [11], [150] *Fronthaul*: é a interface física de fibra óptica em pares (para haver redundância nas bandas de frequências do rádio 5G) ou por um enlace de micro-ondas, que realizam a ligação entre a Unidade de Banda Base Digital (BBU) na parte inferior do gabinete da Estação Rádio Base (ERB) e o cabeçote da Unidade de Rádio Remoto (RRU) na parte superior do mastro próximo da Antena Multibanda de Painel Plana MU–MIMO [14]. Ambos equipamentos RRU e BBU integram a Rede de Acesso Rádio em Nuvem (*Cloud-RAN*) da célula da ERB [166].

[10]Em [15], [150] *Backhaul*: é o reuso de frequências necessário para conectar as pequenas células (*small cells*) à rede central do sistema 5G, internet e outros serviços da rede. As conexões podem ser realizadas por meio das fibras ópticas subterrâneas ou por meio de micro-ondas na interface aérea do rádio 5G usado na ERB.

(a) 

Figura 4.26: Calçada com equipamento 5G [167]

(b) 

Figura 4.27: Poste de iluminação pública com equipamento 5G RAN [167]

(c) 

Figura 4.28: Semáforo com equipamento rádio 5G RAN [167]

[167] conforme demonstram a Figura 4.26 – Calçada com equipamento rádio 5G RAN, a Figura 4.27 – Poste de Luz com equipamento rádio 5G RAN e a Figura 4.28 – Semáforo com equipamento rádio 5G RAN acima.

Em 2020, o ex-presidente estadunidense Donald Trump acusou as empresas chinesas Huawei e ZTE, grandes líderes globais de fabricação, instalação e operação de equipamentos e serviços 5G, de colaborarem com a espionagem eletrônica do atual governo chinês liderado pelo Presidente Xi Jiping, pois havia muitas suspeitas dessas empresas repassarem dados sigilosos de seus clientes estrangeiros, principalmente dados dos EUA [168].

Essa desconfiança de Donald Trump tem fundamento por causa do **Poder Cibernético Chinês** [11] estar

[11] Em [169] na sua obra intitulada *CHINA'S CYBER POWER* (2016), a China evoluiu muito rapidamente tecnologicamente nas últimas 2 décadas e utiliza o seu Poder Cibernético principalmente contra os EUA realizando espionagem e atividades de Guerra Cibernética (exploração, defesa e ataque).

dominando o século XXI, devido aos avanços tecnológicos chineses nas últimas 2 décadas, conquistando áreas antes exploradas somente pelos EUA e Rússia. Atualmente a China detém as maiores indústrias produtoras de processadores, microchips e outros insumos microeletrônicos necessários para diversas aplicações humanas. Além disso, as empresas chinesas são obrigadas por lei a repassarem quaisquer informações de interesse do governo chinês.

Isso resultou na publicação da **Lei de Equipamentos Seguros**, aprovada no Senado norte-americano em 28 de outubro de 2021 [170]. Na sanção do atual Presidente da República dos EUA, Joe Biden, mais 14 empresas chinesas foram incluídas na "Lista Negra Comercial dos EUA" iniciada pelo ex-Presidente Donald Trump sobre os produtos e serviços chineses oferecidos nos EUA (e.g. Huawei, Xiaomi, ZTE, Alibaba, Tencent, e Baidu). Segundo [168] no governo Trump eram 31 empresas chinesas nessa lista, mas foi ampliada no governo Biden para o total de 59. Aplicativos chineses como *TikTok* e *WeChat* foram proibidos temporariamente pelas autoridades da Comissão Federal de Comunicações (*Federal Communications Commission*) nos EUA por suspeitas de espionagem, pois representavam ameaça à segurança nacional EUA, já que muitos chineses residentes nos EUA e seus descendentes estadunidenses continuaram usando para se comunicarem com os seus parentes chineses moradores na China.

Conforme divulgado em [171] a Comissão Federal de Comunicações (FCC) dos EUA proibiu todas as vendas de novos dispositivos de telecomunicações Huawei e ZTE nos EUA em novembro de 2022, por motivos de segurança nacional, de acordo com o comunicado da presidente da FCC Jessica Rosenworcel: "Essas novas regras são uma parte importante de nossas ações contínuas para proteger o povo americano de ameaças à segurança nacional envolvendo telecomunicações".

De acordo com [172], oficial da Marinha dos EUA (*Navy*) no seu artigo científico: "Cibersegurança: A Próxima Ameaça para a Segurança Nacional", publicado no Corpo da Marinha dos Estados Unidos (USMC, 2011), as ameaças de ataques cibernéticos causam uma orientação do ambiente cibernético através da Segurança Cibernética, porque cada nível de uma infraestrutura ciberfísica é formada por: (i) software operacional; (ii) pessoas; (iii) informações; e (iv) suscetível a falhas de segurança por ataque, infiltração ou acidente. Sims citou ainda que: "As ameaças cibernéticas são assimétricas porque permitem que poucos recursos realizem ataques em massas".

Segundo [48] que escreveu na Revista Política Hoje, no ano de 2017:

> **Emissões eletromagnéticas para comunicação, não importa se seja por rádio, internet ou *data link*, em termos físicos é a mesma, diferenciando o nível de frequência (bandas) em que ocorre. O ciberespaço e as emissões eletromagnéticas hoje são os principais meios de transmitir informações e conhecimento, sejam elas individuais, coletivas, civis ou militares. Na realidade podemos afirmar que as redes de computadores e de comunicação, no século XXI, tornaram-se a mesma coisa. Há uma ampla convergência tecnológica entre computadores, comunicações, equipamentos eletrônicos, software e criptografia."** (Grifo nosso)

Das assertivas acima, infere-se que as redes móveis 5G também apresentam vulnerabilidades técnicas inerentes às suas características físicas no EEM, principalmente nas faixas infra e médias do 6 Ghz, que podem ser exploradas em ações de Guerra Cibernética e/ou Guerra Eletrônica mais facilmente do que as faixas supra 6 GHz. Contudo, com o avançar tecnológico em um futuro próximo até as faixas de frequências supra 6 GHz ficarão vulneráveis aos enxames de *drones* com IA capazes e especializados em cumprir um rol de missões de Inteligência: (i) Sinais (SIGINT) composta por Fontes de Sinais de

Comunicações (COMINT) e Fontes de Sinais de Eletrônica (ELINT); (ii) Fontes Cibernéticas; (iii) Fontes Acústicas; e (iv) Fontes de Imagens (IMINT).

Finalmente, estima-se que no futuro próximo as redes móveis do Ecossistema 5G Brasil poderão sofrer ataques cibernéticos de agentes internos e externos do Brasil, assim como já ocorre com os EUA, tendo em vista o aumento considerável de equipamentos de TIC (*laptops, smartphones, tablets, switchs, access point*, servidores, roteadores, etc) que estarão ligados nas redes móveis 5G e na computação em Nuvem 5G, além dos dispositivos da Internet das Coisas (IoT) ligados nas redes internas *WiFi*, redes *Mesh* e redes *ZigBee* fornecidas pelos sinais do 5G nas residências (*indoor*), como também os equipamentos que fornecerem os sinais 5G nas redes externas (*outdoor*) por meio dos *Hotspots* instalados em praças, postes de luz, semáforos, telhados de coretos, pontos de ônibus e metrôs; e nas vias urbanas, bueiros, telhados de lojas, etc.

4.5 ARQUITETURA CONCEITUAL DE SISTEMA DE 5G TÁTICO EB

O denominado **Sistema 5G Tático EB** é um Sistema de Comunicação 5G desenvolvido pela Operadora de Telefonia Celular Tim DF, embarcado em uma viatura Furgão Mercedes Benz Sprinter 413, o qual está em operação regular desde o ano de 2020, justaposto ao Forte Caxias Quartel General do Exército (QGEx), no Setor Militar Urbano, no Distrito Federal (DF).

Até o segundo bimestre de 2023 permaneceu ativado na área Leste interna do Pátio de Formaturas do QGEx, mas no mês de maio seguiu para a área Leste externa do QGEx, visando aumentar a sua área de cobertura e não interferir nas redes 5G das outras operadoras Claro e Vivo com ERBs já instaladas nos telhados dos blocos do QGEx.

O seu emprego no SMU foi primordial para estabelecer 2 pequenas células (*small cells*) de aproximadamente 250 m de raio com sinal 5G, formadas por 3 conjuntos (Cj) Rad 5G NR embarcados no interior do Furgão MB Sprint 413 ligados nas 3 Antenas Ortogonais Painéis Planos MU–MIMO de 120º cada, nas regiões da Cúpula da Concha Acústica e da Praça Cívica, onde se encontravam a maioria dos manifestantes no último bimestre de 2022.

Esse **Sistema 5G Tático EB** ficou estacionado e segurado pela guarda armada do Grupo Ômega do QGEx, estabelecido na Av. Guararapes, em frente ao Bloco A, do Gabinete do Gab Cmt Ex, conforme simulado o raio de ação de cor vermelha na Figura 4.29 – Área da Cobertura do sinal 5G no SMU do *HTZ Warfare* com 18 ERBs e 2 Sistemas 5G Tático EB no SMU abaixo.

Figura 4.29: Área da Cobertura do sinal 5G no SMU do *HTZ Warfare* com 18 ERBs e 2 Sistemas 5G Tático EB no SMU [74]

Das assertivas acima e da análise da Figura 4.29, estima-se que o Objetivo Geral deste trabalho foi atingido, considerando-se uma proposta de arquitetura conceitual de 5G Tático para ser empregada pelo EB em operações militares, que na simulação se ateve ao espaço geográfico do SMU, mas que poderá ser empregado em outras localidades brasileiras, segundo planejamento prévio do MD e COTER.

A propósito, esse **Sistema 5G Tático EB** foi empregado em dupla com pleno êxito na **Operação Posse 2023**, no dia 1º de janeiro de 2023, durante aos atos cerimoniais e posteriormente nas festividades dos *Shows* populares na Esplanada dos Ministérios.

Os Sistemas 5G Táticos EB foram dispostos em diagonal entre si, sendo que o primeiro foi mobiliado na borda do gramado da Esplanada dos Ministérios, próximo ao local do *Show* da posse do atual Presidente da República, Luiz Inácio Lula da Silva, enquanto que o segundo ficou mobiliado na frente dos Ministérios da Infraestrutura e Turismo, conforme demonstra a Figura 4.30 – Croqui dos Sistemas 5G Táticos EB na Operação Posse 2023 na Esplanada dos Ministérios abaixo.

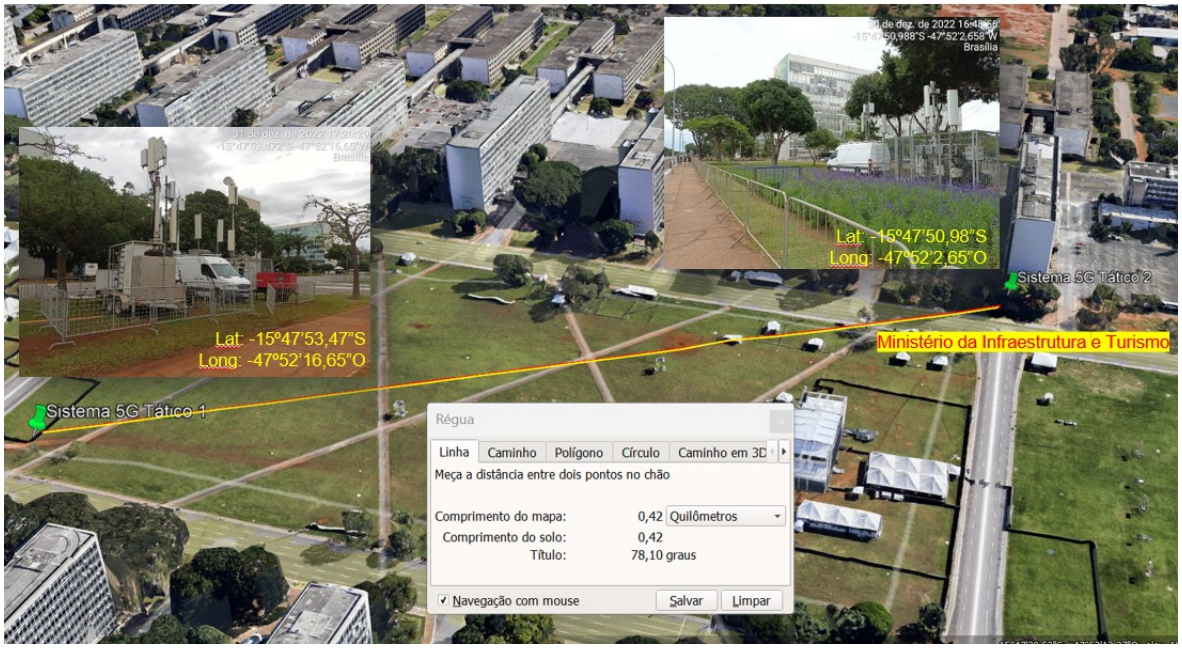

Figura 4.30: Croqui dos Sistemas 5G Táticos EB na Operação Posse 2023 na Esplanada dos Ministérios [74]

A seguir uma imagem detalhada do **Sistema 5G Tático EB 1** mobiliado na região Oeste da Esplanada dos Ministérios, especificamente na borda do gramado onde ocorreram os espetáculos populares no dia da Posse Presidencial, conforme demonstra a Figura 4.31 – Sistema 5G Tático EB na região Oeste da Esplanada dos Ministérios.

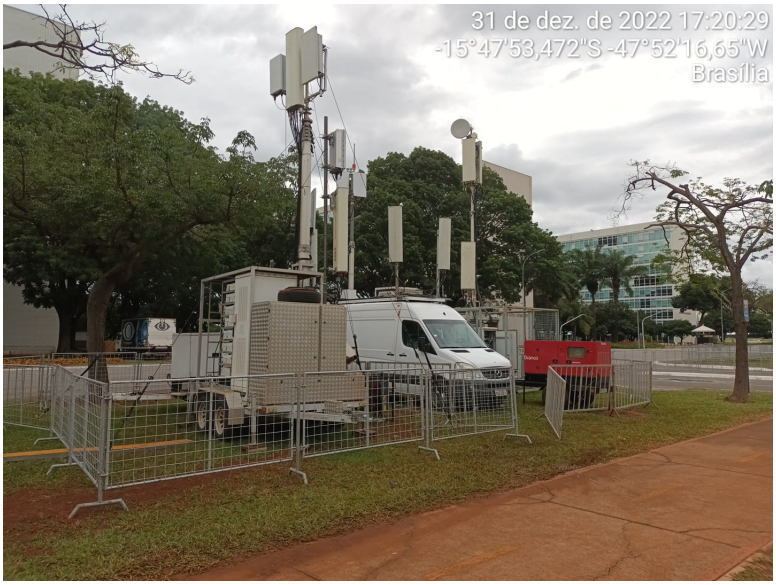

Figura 4.31: Sistema 5G Tático EB 1 na região Oeste da Esplanada dos Ministérios no dia 1º JAN 23 [149]

Abaixo uma imagem detalhada do **Sistema 5G Tático EB 2** mobiliado na região Leste da Esplanada dos Ministérios, especificamente na frente dos Ministérios da Infraestrutura e Turismo, conforme demonstra a Figura 4.31 – Sistema 5G Tático EB na região Leste da Esplanada dos Ministérios.

Figura 4.32: Sistema 5G Tático EB 2 na região Leste da Esplanada dos Ministérios no dia 1º JAN 23 [149]

Esse modelo de arquitetura presente no **Sistema 5G Tático EB** foi proposto conceitualmente para o EB utilizar nas operações por todo o Brasil, tendo em vista seu baixo custo de produção em torno de R$ 732.826,00 (Setecentos e trinta e dois mil, oitocentos e vinte e seis reais) valor de 2012.

Por fim, ao corrigirmos o valor total de 2012, obtém-se hoje um valor de aproximadamente R$ 1 milhão (Hum milhão de reais) segundo [149], conclui-se que esse sistema é relativamente mais vantajoso financeiramente quando comparado aos outros sistemas de comunicações militares adquiridos pelo Comando Logístico (COLOG) do EB. Por exemplo: hoje uma Estação Terrestre Transportável do SISCOMIS custa em torno de U$ 300,000.00 (Trezentos mil dólares) e aproximadamente R$ 1,44 milhão de reais com o câmbio do U$ 1.00 a R$ 4,80, de meados de julho de 2023.

5 CONCLUSÃO E TRABALHOS FUTUROS

5.1 CONCLUSÃO

O Brasil é o 5º maior país do mundo em extensão territorial com seus 8.510.417,771 Km² [173]. Também é o maior país da América do Sul e ocupa 43,7% do continente sul-americano. Existem cerca de 207.750.291 habitantes, segundo o censo de 25 de dezembro de 2022, realizado pelo Instituto Brasileiro de Geografia e Estatística (IBGE) [174].

Realmente o Brasil é um país com dimensões continentais e detém um enorme potencial exploratório dos recursos minerais estratégicos presentes nas áreas da Amazônia Legal e da Amazônia Azul, tais como: (i) Minerais (Ouro, Terras Raras, Nióbio, Grafite, Urânio, Ferro, Manganês, etc); (ii) Fontes de energia renováveis, Gás natural e Petróleo [175]; (iii) além da riquíssima Biodiversidade (Fauna e Flora) presentes nos 6 Biomas[1] no território brasileiro [176], [178]. E, ainda, dispõe de extensa área marítima denominada Amazônia Azul (AAz) [179], tão rica em biodiversidade e recursos minerais no seu subsolo e solo presente no Oceano Atlântico Sul (OAS), quanto as riquezas existentes na Amazônia Verde. E todos esses patrimônios humano e físicos brasileiros devem ser resguardados e protegidos para serem explorados de forma sustentável e exclusiva pelas gerações futuras de brasileiros [51], [61], [67], [68].

Atualmente, o Brasil é a 9ª maior economia global entre os 10 países mais ricos divulgados em 2023, considerando-se o PIB de U$ 1,8 trilhões. Em 2022 o País ficou com superávit comercial acima da média mundial e obteve desempenho econômico melhor do que a Rússia e África do Sul, países participantes do BRICS [180].

E para se manter entre os líderes globais é necessário conquistar e manter os seus Objetivos Nacionais Permanentes (ONP), estabelecer uma política-externa conciliadora com os demais países buscando alianças político-econômicas e a manutenção dos recursos naturais estratégicos nacionais por meio da Defesa externa e Segurança nacional [67].

Esse trabalho abordou na Seção **1 INTRODUÇÃO** um arcabouço legal que ampara o emprego do **Poder Nacional**[2] e do **Poder Cibernético**[3] brasileiros contra outros Estados-Nação, que porventura venham ameaçar a nossa soberania e segurança nacional.

O Brasil dispõe de 23.119 Km de fronteiras, destas 15.719 Km são terrestres junto de 11 Estados brasileiros [182], e adjunto aos 9 países sulamericanos e um território ultramarino da França [67] limítrofes [183] e 7.400 Km são de costa litorânea junto ao Oceano Atlântico Sul (OAS) [184].

[1]Em [176] descreve que o Brasil contém rica flora com cerca de 56 mil espécies de plantas superiores; e rica fauna com 3 mil espécies de peixes de água doce, 517 espécies de anfíbios, 1.677 espécies de aves, 517 espécies de mamíferos e milhões de espécies de insetos, segundo dados do Ministério do Meio Ambiente e Convenção Internacional [177].

[2]Em [67] descreve o Poder Nacional: é a capacidade disposta da nação para alcançar e manter seus Objetivos Nacionais Permanentes, em sintonia com a vontade nacional, baseadas em 5 expressões: (i) política; (ii) econômica; (iii) psicossocial; (iv) militar; e (v) científico-tecnológica.

[3]Em [181] descreve o Poder Cibernético: é a capacidade de uma nação empregar suas capacidades na Segurança, Defesa e Guerra cibernéticas para obter vantagens e influenciar eventos em outros ambientes operacionais e/ou outros instrumentos de poder.

E as FA brasileiras desempenham a Defesa nacional, diuturnamente, nas Faixa de Fronteira Marítima (5,7 milhões Km² na Amazônia Azul) no Oceano Atlântico Sul e Faixa de Fronteira Terrestre (2.357.850 Km²) na América do Sul [182], empregando diversos Meios de Emprego Militar (MEM) e de tropas militares especializadas para cumprirem as missões planejadas nos Níveis Político, Estratégico, Operacional e Tático [70]. As ações de patrulhamento e de combate aos ilícitos federais cometidos nessas áreas dão responsabilidade do Governo federal em realizar a Defesa externa e a Segurança nacional para manter o *status quo* de normalidade da soberania[4] e a situação de Paz no Brasil [61].

O Sistema Brasileiro de Inteligência (SISBIN), a Estrutura Militar de Defesa (Etta Mi D), e o Sistema Militar de Comando e Controle (SISMC²) são empregados para direcionar os atores da Defesa brasileira a promoverem as estratégias de **Proteção, Dissuasão e Projeção de Poder**, empregando diversas tecnologias duais[5] – civil e militar – do MD e das FA (MB, EB e FAB) [51], [67], [68].

A Dimensão Informacional do Ambiente Operacional se vale da Internet e do EEM (licenciado e não licenciado) orgânicos nas Redes Heterogêneas atuais para promover o denominado ***hacking* cognitivo** [6] [65], que considera o uso maciço de tecnologias presentes no espaço cibernético [186] para atacar a sociedade e modificar a opinião pública com propagandas direcionadas (*micromarketing*), explorando recursos de psicologia, ciências sociais e divergências políticas entre as instituições governamentais, e usando a desinformação nas instituições não governamentais e mídia, visando a alcançar objetivos estratégicos nas Operações de Informação [65].

De acordo com [40] é necessário controlar a narrativa do conflito com Operações de Informação. Porque a atuação da F Ter na Dimensão Informacional deverá contribuir notadamente para moldar as percepções da população e da mídia [65]. E as ações cibernéticas (ataque, defesa e exploração) devem ser cuidadosamente sincronizadas com as operações reais, visando apoiar a manobra em todas as fases da campanha na Guerra [37].

Ressalta-se neste trabalho que além da situação de Guerra em um país, a qual pode causar destruições das Infraestruturas Críticas (IC) e inúmeras mortes de civis e de militares nos combates, como está ocorrendo na atual Guerra Russo-Ucraniana [187], outras situações inusitadas podem afetar gravemente a soberania nacional e modificar o *status quo* da normalidade na situação de Paz, causando a mudança para a situação de Crise [39], como exemplo concreto disso, atravessamos o período da pandemia de COVID-19 entre os anos 2020–2023.

[4]Em [67] Soberania: é o âmago citado no Art. 1º da Constituição da República Federativa do Brasil. Ela é inalienável, é indivisível e é imprescritível. E deve ser exercida pela vontade geral da população brasileira e ser preservada em nome das futuras gerações e da prosperidade do País. É uma ordem inigualável, a qual não deve ser submetida a qualquer outra ordem.

[5]Em 3.9 SisMC²: são empregadas diversas tecnologias duais utilizadas na defesa e segurança nacional: (i) satélites dos SISCOMIS, SGDC-1 e SisGAAz; (ii) redes de comunicação cabeadas e sem fio na ROD, nas redes de telefonia VoIP das FA (RETELMA, RITEx e RTCAer) e nas redes de dados corporativas das FA (RECIM, EBNet, INTRAER); (iii) veículos de combate (aéreos, terrestres, fluviais e marítimos) no patrulhamento das fronteiras marítimas, terrestres e aéreas; (iv) radares, câmeras infravermelho e sensores especiais no SisGAAz (MB), no SISFRON (EB) e no SIPAM (FAB); (v) VANT (*drone*) empregados nas operações sob coordenação do MD mas emprego direto das FA: Ágata, Timbó, Verde Brasil, Acolhida e Garantia de Votação e Apuração; (vi) emprego de armamentos não-letal e letal nos adestramentos conjuntos das FA realizados anualmente; e (vii) Comando e Controle (C²) eficiente, eficaz e efetivo realizado pelo SIPLOM no MD.

[6]Em [185] informa que está surgindo uma nova era de *hackers* cognitivos que objetivam a propaganda digital através de robôs digitais *bots* programados com IA para poderem alterar o condicionamento social, como do Partido Comunista Chinês que busca influenciar a plataforma de mídia social chinesa TikTok para o mundo. O *hacking* cognitivo pode ainda espalhar notícias falsas (*fake news*) que podem desestabilizar campanhas presidenciais estrangeiras.

Se por um lado ainda existe a Guerra Russo-Ucraniana que forçou os litigiosos a usarem tecnologias duais presentes no Ecossistema 5G nos combates da Guerra Ominidirecional, por meio de Enxames de *drones* para atividades de **C4ISTAR**, missões de "ataque suicida"contra alvos inimigos e também na comunicação em Redes não Terrestres (RNT) usando a faixa de 52,6 GHz – 71 GHz [188], conforme lançamento Rel-17 com topologias fixadas em Plataformas de Alta Altitude e constelações de Satélites de Baixa Órbita da Terra (*Low Earth Orbit* (LEO)) de 500 Km até 1.500 Km de altitude da superfície terrestre [189]. Por exemplo: uso da Internet Espacial, estabelecida via rede satelital da empresa *Star Link* na Ucrânia está usando a Estação Terrena da Polônia para realizar as retransmissões do sinal 5G entre os diversos satélites no céu e direcionando com até 1 Gbps para o solo, atendendo a áreas isoladas nas fronteiras com a Rússia, áreas rurais e áreas urbanas destruídas pelos ataques russos [190].

Por outro lado a pandemia de COVID-19 determinou a aceleração forçada na implantação do 5G Global pelos Governos, segundo o relatado no Fórum Econômico Mundial [83], onde 84% dos empregadores aceleraram a digitalização nos processos de trabalhos em suas empresas, e destes 83% forneceram mais oportunidades para seus funcionários trabalharem remotamente de suas casas entre 2020–2023.

De acordo com [12] conforme publicado no *Future Jobs Survey 2020 – October 2020* [129] após o choque agudo do período da COVID-19 em 2020, as inflações em 2021 atingiram níveis inéditos em quase 40 anos em muitas economias mundiais, impulsionadas pelas altas subidas dos preços das *commodities*, interrupções na cadeia de suprimentos relacionadas à pandemia, políticas monetárias expansivas, apoios fiscais às empresas, pagamentos de auxílios emergenciais aos trabalhadores isolados na pandemia, e aumento na demanda de serviços sobre compras de bens de consumo.

De acordo com os 3 (três) serviços do Ecossistema 5G Brasil abordados nesse trabalho (eMBB, mMTC e URLLC) e suas Tecnologias Chaves [11] ou **Tecnologias Futuras** [16]; em breve propiciarão o desenvolvimento econômico, científico, social e a evolução da Internet Banda Larga no território brasileiro [112], [106]. Até 2030, o 5G atenderá aos 5.570 municípios e promoverá a inclusão digital nas instituições públicas de Ensino Básico (Creches, Ensinos Fundamental e Médio) do Programa Conectiva e fornecerá incremento nas infraestruturas das redes do PAIS [107], [27], [108] e [98].

Este trabalho priorizou discutir a Segurança Cibernética no Ecossistema 5G Brasil, pois a Informação é a matéria prima na Dimensão Informacional, principalmente no 5º Domínio, denominado Espaço Cibernético, que transcende os 6 Domínios (Marítimo, Terrestre, Aéreo, Espacial, Cibernético, e Eletromagnético) do Ambiente Operacional, na Era da Informação [65], [40].

Ressalta-se, ainda, neste trabalho que a arquitetura conceitual dual proposta com o **Sistema 5G Tático EB** embarcado na Viatura Mercedes Benz 413 poderia atender plenamente às necessidades de C4ISTAR das FA brasileiras em operações, propiciando comunicação de dados com altas taxas e velocidades de DL/UL na banda larga móvel da eMBB, como meio principal empregado nas Operações Conjuntas[7] coordenadas pelo MD, nas Faixas de Fronteira terrestre e também nas Operações Singulares das FA brasileiras no acionamento para Op GLO.

[7]Em [39] define as operações conjuntas (Op Cj) como aquelas operações que empregam meios ponderáveis de mais de uma Força Singular (MB, EB, e FAB), sob um comando único (pode ser de qualquer Força Armada) com Estado-Maior Conjunto contendo os representantes das 3 FA, tendo propósitos interdependentes ou complementares. É realizada no nível operacional,cuja integração das Forças é fundamental com C² e Com sob um único comando.

Como exemplo disso a Operação Ágata Amazônia[8] [191] é coordenada pelo MD e executada pelas FA (MB, EB, e FAB) em cooperação com diversos órgãos federais (PF, IBAMA, FUNAI, etc) e estadual do Amazonas (PCAM) realizaram ações de combate ao garimpo ilegal, ameaça aos indígenas e destruição do Meio-Ambiente pelo metal pesado mercúrio nas águas, terras e fauna amazonense. Foram destruídas cerca de 29 balsas que poderiam gerar lucro de até R$ 23,2 milhões por mês aos criminosos federais. Nesta Op Ágata poderia ser usado o Sistema 5G Tático fornecendo os sinal 5G nas localidades ribeirinhas, pois é um sistema de comunicações flexível e que pode ser transportado tanto por navios do Comando do 9º Distrito Naval (Cmdo 9º DN) da MB (Manaus/AM) e balsas da 12ª Região Militar (12ª RM) do EB (Manaus/AM), como por aeronaves KC-390 do Sétimo Esquadrão de Transporte Aéreo (7º ETA) da FAB (Manaus/AM), pois foram realizadas ações de Assistência Hospitalar e Ações Cívico-Sociais para a população ribeirinha e indígena da Amazônia Ocidental.

Das assertivas acima e da Figura 4.29 – Área da Cobertura 5G final no SMU contendo as 18 ERBs do HTZ Warfare e juntamente das 2 viaturas do **Sistema 5G Tático EB**, conclui-se que o Objetivo Geral deste trabalho foi atingido com a proposta conceitual de uma arquitetura de 5G Tático para ser empregada pelo EB na Defesa nacional.

Por todo o exposto, das assertivas acima e de acordo com [65]:

> **"Nos conflitos modernos, a informação é tão importante quanto o efeito letal para determinar os resultados da campanha militar."** (Grifo nosso)

5.2 TRABALHOS FUTUROS

Em 2019, na WRC-19, foi enfatizada na ***Connected 2030 Agenda*** publicada em [85], em tradução livre "Agenda 2030 Conectada", os 5 (cinco) Objetivos de Desenvolvimento Sustentável (ODS) para o 5G Global [12], [85]: (i) Objetivo 1 – Crescimento; (ii) Objetivo 2 – Inclusividade; (iii) Objetivo 3 – Sustentabilidade; (iv) Objetivo 4 – Inovação; e (v) Objetivo 5 – Parceria.

De acordo com [12], [21], [86], [88], [129], [189] já surgiram novas tecnologias baseadas nas **Redes Móveis da 6ª Geração**, conforme a Agenda 2030 da ITU [85], a fim de atender às necessidades específicas da Indústria 4.0 e da Sociedade 5.0 [21].

Em [87] estima que o 6G seja implantado no mundo no período de 2030-2035 e fique dedicado ao conceito "Tudo Ligado". Por exemplo: a Finlândia anunciou seu programa "6 Genesis"para o desenvolvimento de um Ecossistema 6G completo.

A ITU-Telecomunicações (ITU-T) criou o *Focus Group NET-20230 (FG NET-2030)* em 2018, em tradução literal "Grupo Foco Rede 2030", o qual está concentrado na exploração das novas tecnologias para os sistemas 6G para além de 2030 [79].

[8]Em [191] Operação Ágata do Comando Conjunto Uiara é formada pela Agência Brasileira de Inteligência (ABIN), Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM), Fundação Nacional dos Povos Indígenas (FUNAI), Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA), Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), Polícia Civil do Amazonas (PCAM), Polícia Federal (PF) e Secretaria Especial de Saúde Indígena (SESAI).

A Conferência de Radiocomunicação Mundial da ITU 2023 (*ITU World Radiocommunication Conference 2023* (WRC-23)) em Dubai, Emirados Árabes Unidos, será realizada de 20 de novembro de 2023 até 15 de dezembro de 2023, onde serão discutidos o futuro das telecomunicações móveis internacionais (IMT) incluindo o tema do 6G, conforme a *Resolution 1399 (C20) – Agenda of the World Radiocommunication Conference (WRC-23)* documento de 5 páginas contendo os assuntos abordados na Reunião Preparatória.

Já o documento denominado *Informe de la RPC sobre cuestiones técnicas, operacionales y de reglamentación/procedimiento que deben examinarse en la Conferencia Mundial de Radiocomunicaciones de 2023* contém 1.214 páginas nessa versão no idioma espanhol, descrevendo diversos assuntos que serão abordados na WRC-23, os quais já foram iniciados na WRC-19, tais como: (i) regulação da faixa de frequência 4.800 – 4.990 MHz para áreas terrestres nacionais e serviços móveis internacionais para navegações aéreas e marítimas; (ii) considerar a identificação das bandas de frequências 3.300 – 3.400 MHz, 3.600 – 3.800 MHz, 6.425 – 7.025 MHz, 7.025 – 7.125 MHz e 10,0 GHz – 10,5 GHz as IMT; (iii) considerar as faixas de frequências 3.600 – 3.800 MHz para o serviço móvel da Região 1[9].

Segundo [129] espera-se que as redes da próxima geração 6G sejam associadas com larguras de banda elevadas e frequências em Terahertz (até 3THz) e taxas de dados elevadas até 1Tbps, isso permitirá várias aplicações que incluem altas taxas de transferência de dados com o conceito da nova **Comunicação Verde** (*Green Comunication*) baseada em alguns fatores, tais como [12]:

(i) ser sustentável (promover o desenvolvimento econômico junto da conservação ambiental);

(ii) ser limpa (usar energia elétrica de fontes renováveis e de baixo impacto ambiental, reduzindo a emissão de carbono na atmosfera);

(iii) usar frequências do EEM da **Luz Visível** por meio da *Optical Wireless Communication (OWC)*, em tradução literal Comunicação Óptica Sem Fio;

(iv) ter uma rede centrada no ser humano (super rápida, descentralizada, inteligentes e cognitivas);

(v) ser onipresente; e (vi) pronta para possibilitar uma nova multiplicidade de serviços que unem o mundo físico e cibernético para apoiar o surgimento de uma nova sociedade denominada Sociedade 5.0.

Dessa forma, como sugestões de trabalhos futuros, poderão ser pesquisados os seguintes temas:

1. **O futuro das Redes de Comunicação 6G sem fio para estabelecer a Comunicação, Navegação, Sensoriamento e Serviços (CONASENSE)**: suas aplicações na ciência estão sendo estudadas com muita intensidade hoje, mas os cientistas e autores E. F. Nichols e J. D. Tear publicaram o artigo científico intitulado ***"Joining the Infra-red and Electric Wave Espectra"***, no ano de 1923, nos EUA, em tradução literal do inglês para o português: "Unindo os espectros do infravermelho e das ondas elétricas"[192]. Atualmente os Raios T são usados para realizara a análise de imagens humanas na medicina e também análise de objetos na engenharia de materiais, pois as ondas não-ionizantes[10]

[9]Em [19] Região 1 da ITU: é formada pelos continentes Europeu, Africano, e Asiático (incluindo países pertencentes antiga União Soviética), Mongólia e o Oriente Médio a oeste do Golfo Pérsico, incluindo o Iraque.

[10]Em [5] **radiações não ionizantes**: não provocam os efeitos permanentes na matéria, contudo tem capacidade de realizar alterações temporárias na organização eletrônica, as quais são cessadas naturalmente quando os elétrons retornam ao seu estado

interagem com as matérias sem danificar suas estruturas moleculares. No EEM, a radiação Terahertz (THz), também denominadas de Ondas T, está localizada entre as faixas das Micro-ondas e do Infravermelho, entre 300 GHz e 3 THz, com comprimentos de ondas de 1.000 a 100 micrômetros [192].

2. **Rede sem Fio Inteligente e Cognitiva: usará Aprendizado de Máquina (*Machine Learning*) (ML) e Inteligência Artificial (IA)**: implantadas na borda e no núcleo da Rede 6G para processar grande quantidade de dados no chamado *Big Data*. Por exemplo: poderão ser trocados e gerados dados por Comunicações Máquina a Máquina, Internet Industrial das Coisas (IIoT), Comunicações Holográficas (Vídeo 3D), Internet de NanoCoisas (IoNT), e CONASENSE. Portanto, o 6G opera com base na consciência do contexto.

3. **Redes não Terrestres (RNT) também denominada de Internet do Espaço (*Space Internet*)** [193], [194], [189]: são compostas por Sistemas Espaciais (SE) formados por Satélites ou Constelações de Satélites de 4 tipos de órbitas terrestres distintas: (i) Órbita Terrestre Baixa (LEO) até 1.500 Km de altura; (ii) Órbita Terrestre Média (MEO) de 1.500 Km até 20.000 Km de altura; (iii) Órbita Terrestre Geossíncrona (GEO) até 36.000 Km; e (iv) (*Highly Elliptical Orbit*(HEO)) posicionado de 1.000 Km a 39.000 Km de de altura, com revolução de 12 horas de período elíptico em torno da Terra. No Brasil, o Comando da Aeronáutica (COMAER) implementou o Programa Estratégico de Sistemas Espaciais (PESE) (MD20-S-01) em 2017 [193], a fim de desenvolver os Sistemas Espaciais (Segmento Orbital e Segmento de Infraestrutura de Operação Terrestre) priorizando as necessidades do MD e das FA, além de disponibilizar Produtos de uso predominantemente dual (civil – militar) para entidades públicas e privadas que aderirem aos projetos do PESE.

4. **Internet Tática (IT)** [129]: é considerada também Internet Ativa, pois habilita sensações táteis e hápticas[11] para interação homem-máquina. Alguns requisitos da (IT): (i) latência ultrabaixa, menor que 5 milissegundos; (ii) perda ultrabaixa é quase intolerável a perda de pacotes; (iii) largura de banda ultra alta, possibilita vídeo de 360º graus até hologramas; (iv) alimentação Realidade Virtual (VR) com 5 Gbps e Hologramas com Tbps; (v) sincronização rigorosa, com diferentes entradas sensoriais por causa das reações do cérebro humano, por exemplo: tátil é 1 ms, visual: 10 ms e áudio: 100 ms. Logo o retorno em tempo real de diferentes entradas deve ser sincronizado corretamente; (vi) níveis diferenciados de priorização de fluxos com base em sua relevância imediata.

5. **Comunicações de Tipo Holográfico (HTC)** [12]: nos últimos anos a tecnologia de exibição holográfica conseguiu avançar muito, desde exibições de campo de luz até diferentes tipos holografias. As aplicações holográficas podem se tornar realidade na Indústria (controle de objeto real cpor meio do objeto virtual), na Medicina com imagem 3D, na Comunicação com entrega Personalizada, e na Telepresença Interativa.

inicial anterior à ionização. As radiações não ionizantes estão distribuídas desde as ondas de rádio (de 10^5 Hz a 10^{10} Hz), micro-ondas (de 10^{10} Hz a 10^{12} Hz), infravermelha (ondas de calor) de 10^{12} Hz a 10^{14} Hz), luz visível (para o ser humano, vai de $4,3.10^{14}$ Hz a $7,5.10^{14}$ Hz) até as ondas ultravioleta (entre $7,5.10^{14}$ Hz e 3.10^{16} Hz). Desta forma, a energia associada aos fótons de cada radiação é que determina o seu caráter ionizante ou não.

[11] Em [195] **Háptica**: significa ter a capacidade de desenhar em silhuetas com os dedos. Origem: grego haptikós, -ê, -ón.

Referências Bibliográficas

1 TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores. Tradução: Daniel Vieira*. [S.l.]: São Paulo: Pearson Prentice Hall, 2011.

2 KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet. *São Paulo: Person*, v. 28, 2006.

3 BEARD, C.; STALLINGS, W. *Wireless communication networks and systems*. [S.l.]: Pearson, 2015.

4 JÚNIOR, O. T. Exploração da diversidade de polarização por meio da álgebra de quatérnions na melhoria de sistemas mimo-ofdm.

5 SALÍCIO, C. U.; CASTRO, P. A. A. D. O espectro eletromagnético e as interações de cada faixa espectral com a matéria. *Física Ótica (Periódicos de Internet) disponível em:< https://edisciplinas. usp. br/mod/resource/view. php*, 2016.

6 FLICKENGER, R. *Redes sem fio no mundo em desenvolvimento: um guia prático para o planejamento e a construção de uma infra-estrutura de telecomunicações*. [S.l.]: Hacker Friendly LLC, Seattle, WA, US, 2008.

7 UNION, I. T. *About International Telecommunication Union (ITU)*. : ITU Committed to connecting the world, 2023. Disponível em: <https://www.itu.int/en/about/Pages/default.aspx>.

8 FRENZEL, L. *Electronics Explained: Fundamentals for Engineers, Technicians, and Makers*. [S.l.]: Newnes, 2017.

9 GEORGE, C. et al. *DISTRIBUTED SYSTEMS Concepts and Design 5th Ed*. [S.l.]: Addison-Wesley, 2012.

10 MATOS, L. J. de. *SISTEMAS MÓVEIS e PLANEJAMENTO CELULAR*. : UFF/TCE/TET, 2011. Disponível em: <https://pt.scribd.com/document/211825710/Apostila-de-Sistemas-Moveis-2012-1-LENI>.

11 OSSEIRAN, A.; MONSERRAT, J. F.; MARSCH, P. *5G mobile and wireless communications technology*. [S.l.]: Cambridge University Press, 2016.

12 HENRIQUE, P. S. R.; PRASAD, R. *6G: The Road to the Future Wireless Technologies 2030*. [S.l.]: CRC Press, 2022.

13 LIYANAGE, M. et al. *A comprehensive guide to 5G security*. [S.l.]: Wiley Online Library, 2018.

14 SAUTER, M. *From GSM to LTE-advanced Pro and 5G: An introduction to mobile networks and mobile broadband*. [S.l.]: John Wiley & Sons, 2017.

15 RODRIGUEZ, J. *Fundamentals of 5G mobile networks*. [S.l.]: John Wiley & Sons, 2015.

16 ITU. *5G Basics*. Switzerland, Geneva: ITU Telecommunication Standardization Sector (ITU–T), 2017. 1 – 1469 p. Disponível em: <https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-IMT-2017-1-PDF-E.pdf>.

17 ALEXIOU, A. et al. *5G wireless technologies*. [S.l.]: Institution of Engineering and Technology, 2017.

18 DAHLMAN, E.; PARKVALL, S.; SKOLD, J. *5G NR: The next generation wireless access technology*. [S.l.]: Academic Press, 2020.

19 FMUSER. *Regiões ITU*. : FMUSER International Group INC., 2020. Disponível em: <https://pt.fmuser.net/content/?7695.html>.

20 BLUETOOTH. *2023 Bluetooth® Market Update – New trends and forecasts now available*. : Bluetooth, 2023.

21 MATIN, M. A. *A Glimpse Beyond 5G in Wireless Networks*. [S.l.]: Springer Nature, 2022.

22 SERIES, M. Imt vision–framework and overall objectives of the future development of imt for 2020 and beyond. *Recommendation ITU*, Electronic Publication Geneva, Switzerland, v. 2083, n. 0, 2015. Disponível em: <https://www.itu.int/rec/R-REC-M.2083-0-201509-I>.

23 COMUNICAÇÕES, M. das. *Espaço 5G*. Agência Nacional de Telecomunicações (Anatel), 2022. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/5G>.

24 TELEBRASIL5GBRASIL. *Ecossistema 5G Brasil: agentes*. Brasília/DF: , 2018. Disponível em: <https://5gbrasil.telebrasil.org.br/ecossistema/agentes>.

25 BRASIL, T. G. *Painéis com Definições, Plano de Ação, Eventos e Comissões Temáticas*. Brasília/DF: [s.n.], 2018. Disponível em: <https://5gbrasil.telebrasil.org.br/>.

26 BRASIL. *ESTRATÉGIA BRASILEIRA DE REDES DE QUINTA GERAÇÃO (5G) Versão para consulta pública*. Brasília/DF: Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), 2019. 1 – 36 p. Disponível em: <https://antigo.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/estrategia5g/Documento-base-da-Estrategia-Brasileira-de-5G.pdf>.

27 TELECOMUNICAçõES, A. N. de. *Anatel atualiza o Plano Estrutural de Redes de Telecomunicações – PERT 2019 – 2024*. Brasília/DF: Agência Nacional de Telecomunicações (Anatel), 2021. Disponível em: <https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/7838beeae0e7f5837d491fd26413cb46>.

28 TELECO. *Redes 5G II: Órgãos Regulamentadores e Organizações Envolvidas*. : Teleco Inteligência em Telecomunicações, 2023. Disponível em: <https://www.teleco.com.br/tutoriais/tutorialredes5g2/pagina_3.asp>.

29 SERIES, M. Recommendation itu-r m.2150-1 detailed specifications of the terrestrial radio interfaces of international mobile telecommunications-2020 (imt-2020). *Recommendation ITU*, Electronic Publication Geneva, Switzerland, 2022. Disponível em: <https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-1-202202-I!!PDF-E.pdf>.

30 NYAGADZA, B. et al. Digital technologies, fourth industrial revolution (4ir) & global value chains (gvcs) nexus with emerging economies' future industrial innovation dynamics. *Cogent Economics & Finance*, Taylor & Francis, v. 10, n. 1, p. 2014654, 2022.

31 ROJAS, C. N. et al. Society 5.0: A japanese concept for a superintelligent society. *Sustainability*, MDPI, v. 13, n. 12, p. 6567, 2021.

32 KLIMBURG, A.; TIRMAA-KLAAR, H. Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the eu. European Parliamentary Research Service (EPRS), 2011.

33 INKSTER, N. *China's Cyber Power*. [S.l.]: Routledge, 2018.

34 SCORSIM, E. *A tecnologia competitiva de 5G da Huawei nas redes de comunicações*. : Direito da Comunicação, 2020. Disponível em: <https://direitodacomunicacao.com/br/a-tecnologia-competitiva-de-5g-da-huawei-nas-redes-de-comunicacoes-de-5g-o-alvo-da-geoestrategica-da-lawfare-imp>.

35 FARHADI, A.; SANDERS, R. P.; MASYS, A. *The Great Power Competition Volume 3: Cyberspace: The Fifth Domain*. [S.l.]: Springer Nature, 2022.

36 WONG, E. Usa versus china: A new era of great power competition, but without boundaries. *The New York Times*, v. 26, 2019.

37 BRASIL. Doutrina militar de defesa cibernética (md31-m-07). MINISTÉRIO DA DEFESA, Brasília/DF, p. 1 – 38, nov 2014. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf>.

38 SILVA, J. C. B. L. da. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. *Revista da Escola de Guerra Naval*, Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos, v. 20, n. 1, p. 193, 2014.

39 BRASIL. *Manual de Campanha EB70-MC-10.223 Operações*. Brasília/DF: Ministério da Defesa, 2017. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/1/848/3/EB70-MC-10.223-\%20Opera\%C3\%A7\%C3\%B5es>.

40 VISACRO, A. *A guerra na Era da Informação*. [S.l.]: Editora Contexto, 2018.

41 RIBEIRO, R. d. Q. B.; RIBEIRO, S. F. Guerra de informação. *Revista Agulhas Negras*, v. 5, n. 6, p. 135–148, 2021.

42 KLIMBURG, A.; MIRTL, P. Cyberspace and governance-a primer. AUT, 2012.

43 AMERICA, U. S. of. Field manual fm 3-12 cyberspace operations and electromagnetic warfare. Headquarters, Department of the Army, Washington, DC, p. 1 – 162, ago 2021. Disponível em: <https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713>.

44 BORAH, C. K. Cyber war: the next threat to national security and what to do about it? by richard a. clarke and robert k. knake. *Strategic Analysis*, Taylor & Francis, p. 458 – 460, nov 2015. Disponível em: <https://doi.org/10.1080/09700161.2015.1047221>.

45 PARKS, R. C.; DUGGAN, D. P. Principles of cyberwarfare. *IEEE Security & Privacy*, IEEE, v. 9, n. 5, p. 30–35, 2011.

46 SCHMITT, M. N. Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, Cambridge University Press, v. 84, n. 846, p. 365–399, 2002.

47 NUNES, L. A. R. Guerra cibernética e o direito internacional: aplicabilidade do jus ad bellum e do jus in bello. Escola Superior de Guerra (Campus Rio de Janeiro), 2015.

48 NETO, R. B. G. Guerra cibernética/guerra eletrónica-conceitos, desafios e espaços de interação. *Revista Política Hoje*, v. 26, n. 1, p. 201–217, 2017.

49 BRASIL. *A GUERRA OMNIDIMENSIONAL: NOVAS CONCEPÇÕES DO PENSAMENTO ESTRATÉGICO MILITAR*. Brasília/DF: Revista da Escola Superior de Guerra, 2012. 55 – 68 p. Disponível em: <https://revista.esg.br/index.php/revistadaesg/article/view/225/200>.

50 BRASIL. *Cartilha de Gestão de Segurança da Informação*. Brasília/DF: Gabinete de Segurança Institucional (GSI), 2022. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/cartilha-de-gestao-de-seguranca-da-informacao/CartilhadeSegurancaInformao.pdf>.

51 BRASIL. *ESTRATÉGIA NACIONAL DE DEFESA (END)*. Brasília, DF: Ministério da Defesa (MD), 2020. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf>.

52 BRASIL. *Segurança de Infraestruturas Críticas (SIC)*. Brasília/DF: Gabinete de Segurança Institucional, 2022. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic>.

53 BRASIL. *PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022*. Brasília/DF: Presidência da República (PR), 2022. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf>.

54 VIANNA, E. W. Segurança da informação digital: proposta de modelo para a ciber proteção nacional. 2019.

55 STANDARDS, N. I. of; TECHNOLOGY. *NIST Special Publication 800-12 Revision 1 – An Introduction to Information Security*. Gaithersburg, MD, 2017. Disponível em: <https://doi.org/10.6028/NIST.SP.800-12r1>.

56 ISO. *ISO/IEC 27001 Information security management systems Requirements*. International Organization for Standardization (ISO), 2022. Disponível em: <https://www.iso.org/standard/27001>.

57 BRASIL. *DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas*. Brasília/DF: Presidência da República (PR), 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>.

58 BRASIL. *DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional*. Brasília/DF: Presidência da República (PR), 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>.

59 BRASIL. *DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020. Aprova a Estratégia Nacional de Segurança Cibernética*. Brasília/DF: Presidência da República (PR), 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>.

60 VIANNA, E. W.; SOUSA, R. T. B. de. Ciber proteção: a segurança dos sistemas de informação no espaço cibernético. *Revista Ibero-Americana de Ciência da Informação*, v. 10, n. 1, p. 110–131, 2017.

61 BRASIL. *CONSTITUIÇÃO da República Federativa do Brasil*. Brasília, DF: Supremo Tribunal Federal (STF, 2023. Disponível em: <https://www.stf.jus.br/arquivo/cms/legislacaoConstituicao/anexo/CF.pdf>.

62 BRASIL. *Manual de Campanha GUERRA CIBERNÉTICA (EB70-MC-10.232)*. [S.l.]: Exército Brasileiro (EB), 2017.

63 GOMES, M. G. F. M.; CORDEIRO, S. S.; PINHEIRO, W. A. A guerra cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de comando e controle (c2). *Revista Militar de Ciência e Tecnologia, Rio de Janeiro*, v. 33, n. 2, p. 11–18, 2016.

64 VASCONCELLOS, A. A. U. Ameaças cibernéticas à segurança nacional e os impactos nas expressões do poder nacional: paradoxo entre passado, presente e futuro. Escola Superior de Guerra, Rio de Janeiro/RJ, 2017. Disponível em: <https://repositorio.esg.br/handle/123456789/777>.

65 BRASIL. *Manual de Fundamentos EB20-MF-07.101 CONCEITO OPERACIONAL DO EXÉRCITO BRASILEIRO OPERAÇÕES DE CONVERGÊNCIA 2040*. Brasília/DF: Exército Brasileiro (EB), 2023. Disponível em: <http://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=181261464&act=sep>.

66 BRASIL. *Manual de Fundamentos Doutrina Militar Terrestre EB20-MF-10.102*. Brasília/DF: Ministério da Defesa, 2019. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/4760/1/EB20-MF-10.102.pdf>.

67 BRASIL. *Livro Branco de Defesa Nacional (LBDN)*. Brasília/DF: Ministério da Defesa, 2021. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf>.

68 BRASIL. *POLÍTICA NACIONAL DE DEFESA (PND)*. Brasília, DF: Ministério da Defesa (MD), 2020. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf>.

69 BRASIL. *LEI COMPLEMENTAR Nº 97, DE 9 DE JUNHO DE 1999*. Brasília/DF: Presidência da República, 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm>.

70 BRASIL. *Doutrina Militar de Defesa – MD51-M-04*. Brasília/DF: Ministério da Defesa, 2007. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/135/1/MD51_M04.pdf>.

71 BRASIL. *DECRETO Nº 8.903, DE 16 DE NOVEMBRO DE 2016. Institui o Programa de Proteção Integrada de Fronteiras e organiza a atuação de unidades da administração pública federal para sua execução*. Brasília/DF: Presidência da República, 2016. Disponível em: <https://www.planalto.gov.br/cciVil_03/_Ato2015-2018/2016/Decreto/D8903.htm>.

72 BRASIL. *PLANO ESTRATÉGICO DO EXÉRCITO 2020-2023 (EB 10-P-01.007)*. http://www.ceadex.eb.mil.br/images/legislacao/XI/plano_estrategico_do_exercito_2020-2023.pdf: Estado-Maior do Exército, 2020.

73 BARROS, S. S.; ROSA, F. G. M. G.; RIBEIRO, E. M. Princípios e técnicas para elaboração de textos acadêmicos. Superintendência de Educação a Distância, 2017. Disponível em: <https://educapes.capes.gov.br/bitstream/capes/174974/4/eBook_Principios_e_Tecnicas_para_Elaboracao_de_Textos_Academicos-Especializacao_em_Gestao_de_Pessoas_UFBA.pdf>.

74 OLIVEIRA, R. C. F. de. *Criador das Figuras e Tabelas dessa dissertação*. Brasília/DF: Universidade de Brasília (UnB), 2023.

75 OLIVEIRA, R. C. F. de; NZE, G. D. A.; DIAS, U. S. Emprego dual-civil e militar-do 5g na defesa brasileira: uma proposta para o sisfron, sob domínio do exército. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. E49, p. 599–615, 2022.

76 NUNES, P. D. R. R. *Alunos do PPEE apresentam seus traballhos na MICRADS'22*. Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE, 2022. Disponível em: <https://rafael.rabelo.org/2022/07/20/alunos-do-ppee-apresentam-artigos-no-micrads22/>.

77 RISTI. *Edições – Edições regulares, em Português e Espanhol*. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: <http://www.risti.xyz/index.php/pt-pt/edicoes>.

78 GSMA. *The Mobile Economy 2022*. GSMA Intelligence, 2022. Disponível em: <https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf>.

79 ITU. *Focus Group on Technologies for Network 2030*. International Telecommunication Union, 2023. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx>.

80 LI, R. e. o. Rumo a uma nova internet para o ano de 2030 e para além. In: . [S.l.: s.n.].

81 GSMA. *Road to 5G: Introduction and Migration*. Global System for Mobile Communications Association (GSMA), 2018. Disponível em: <https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf>.

82 GSMA. *5G Spectrum GSMA Public Policy Position*. GSMA Latin America, 2020. Disponível em: <https://www.gsma.com/latinamerica/resources/5g-spectrum-gsma-public-policy-position-2/>.

83 ITU-T. *Global Connectivity Report 2022 – Achieving universal and meaningful connectivity in the Decade of Action*. ITU 2023, 2022. Disponível em: <https://www.itu.int/hub/publication/d-ind-global-01-2022/>.

84 ITU. *Pandemic in the Internet Age: communications industry responses*. International Telecommunication Union (ITU), 2020. Disponível em: <https://reg4covid.itu.int/wp-content/uploads/2020/06/ITU_COVID-19_and_Telecom-ICT.pdf>.

85 ITU. *Connect 2030 Agenda*. International Telecommunication Union, 2023. Disponível em: <https://www.itu.int/highlights-report-activities/connect2030/>.

86 ITU. *Network 2030 – A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond*. International Telecommunication Union, 2023. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf>.

87 DOGRA, A.; JHA, R. K.; JAIN, S. A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies. *IEEE Access*, IEEE, v. 9, p. 67512–67547, 2020.

88 GALAL, H.; O'HALLORAN, D. The impact of 5g: Creating new value across industries and society. In: *World Economic Forum Whitepaper*. Switzerland: [s.n.], 2020. Disponível em: <https://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf>.

89 MOURAD, A. et al. A baseline roadmap for advanced wireless research beyond 5g. *Electronics*, MDPI, v. 9, n. 2, p. 351, 2020.

90 RIBEIRO, J. A. J. *TP103 - José Antonio Justino Ribeiro Documentos*. Santa Rita do Sapucaí/MG: Instituto Nacional de Telecomunicações -– Inatel, 2012. Disponível em: <https://www.inatel.br/biblioteca/todo-docman/material-didatico/pos-graduacao/1-semestre-2012/turma-80-92-sao-paulo/tp103-jose-antonio-justino-ribeiro-2>.

91 SCHWAR, R. . *Desmistificando o 5G – Coexistência do 5G NR com o LTE com base no compartilhamento dinâmico de espectro (DSS)*. ROHDE&SCHWARZ, 2023. Disponível em: <https://www.rohde-schwarz.com/br/knowledge-center/videos/desmistificando-o-5g-coexist-ncia-do-5g-nr-com-o-lte-com-base-no-compartilhamento-din-mico-de-espectro-dss-video
251220-726978.html>.

92 SUKINI, T. et al. International journal of psychosocial rehabilitation, vol. 24, issue 02, 2020 red betel leaf (piper crocatum) tea efication in overcoming leucorhea. *International Journal of Psychosocial Rehabilitation*, v. 24, n. 02, 2020.

93 BRASIL. *Guia dos 7º Jogos Mundiais Militares apresenta os principais destaques do Brasil em todos os dias da competição*. REDE DO ESPORTE, 2019. Disponível em: <http://rededoesporte.gov.br/pt-br/noticias/guia-dos-7o-jogos-mundiais-militares-apresenta-os-principais-destaque-do-brasil-em-todos-os-dias-da-competicao>.

94 WELLE, D. *Franceses suspeitam ter contraído coronavírus em outubro*. DW Made for minds, 2020. Disponível em: <https://www.dw.com/pt-br/atletas-franceses-suspeitam-ter-contra\%C3\%ADdo-coronav\%C3\%ADrus-em-outubro-na-china/a-53348305>.

95 SIRIWARDHANA, Y. et al. The role of 5g for digital healthcare against covid-19 pandemic: Opportunities and challenges. *Ict Express*, Elsevier, v. 7, n. 2, p. 244–252, 2021.

96 STRABELLI, T. M. V.; UIP, D. E. *COVID-19 e o Coração*. [S.l.]: SciELO Brasil, 2020. 598–600 p.

97 EBC. *OMS declara fim da emergência em saúde por covid-19*. Brasília/DF: Agência Brasil, 2023. Disponível em: <https://agenciabrasil.ebc.com.br/saude/noticia/2023-05/oms-declara-fim-da-emergencia-em-saude-por-covid-19>.

98 BRASIL. *RELATÓRIO DE AVALIAÇÃO DAS POLÍTICAS PÚBLICAS RELATIVAS À IMPLANTAÇÃO DAS REDES MÓVEIS DE QUINTA GERAÇÃO (5G)*. Senado Federal, 2022. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2022/09/21/relatorio_redes.pdf>.

99 BRASIL. *CORONAVÍRUS BRASIL (dados até 26/04/2023)*. Brasília/DF: Ministério da Saúde, 2023. Disponível em: <https://covid.saude.gov.br>.

100 COMUNICAÇÕES, M. das. *Relatório analítico do impacto da pandemia de COVID-19 no setor de telecomunicações do Brasil (2ª edição)*. Brasília/DF: Agência Nacional de Telecomunicações (Anatel), 2021. 1 – 56 p. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5BitmjawIrUf6lt6H5yefTqyMayOylzRWIKE7CzLQ2BN9zlRTAUIDIhNvEkBlalNBGhEwfZfmi9-_Z0xYmPVzG>.

101 ERICSSON. *5G Advanced: Evolution towards 6G*. Ericsson White Paper BNEW-22:024836 Uen, 2022. Disponível em: <https://www.ericsson.com/49e389/assets/local/reports-papers/white-papers/5g-advanced-evolution-towards-6g.pdf>.

102 AMERICAS, G. *5G Americas White Papers*. : The Voice of 5G & LTE for the Americas, 2023. Disponível em: <https://www.5gamericas.org/white-papers/>.

103 LOPES, C. H. de S. Sistemas fiwi 5g nr baseados em fronthauls de fibra óptica e fso. 2020.

104 BRASIL. *Brasil é eleito para Conselho da União Internacional de Telecomunicações (UIT)*. : Ministério das Comunicações, 2022.

105 (ANACOM), A. N. das C. *Agropecuária*. [S.l.]: Portal 5G, 2023.

106 GSMA. ***O caminho para um Brasil digital*** *Agenda para 2023-2026*. GSMA Latin America, 2022. Disponível em: <https://www.gsma.com/latinamerica/wp-content/uploads/2022/09/O-caminho-para-um-Brasil-digital_GSMA-2022.pdf>.

107 COMUNICAÇÕES, M. das. *Anatel publica edital do leilão do 5G*. Brasília/DF: Agência Nacional de Telecomunicações (Anatel), 2022. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-publica-edital-do-leilao-do-5g>.

108 BRASIL. *RELATÓRIO DO LEILÃO 5G – AMPLIAÇÃO DA BANDA LARGA/CONECVITIDADE*. Brasília/DF: Câmara dos Deputados, 2021. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/subcomissoes/Subcomissoes\%20Especiais/2021/subcomissao-especial-5g/relatorio-do-leilao-5g-ampliacao-da-banda-larga-conectividade-deputado-vitor-lippi>.

109 SOUZA, E. et al. An open source simulation tool for sharing and compatibility studies between 5g and other radiocommunication systems. In: IEEE. *2017 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)*. [S.l.], 2017. p. 1–5.

110 ITU. *WRC-19 identifies additional frequency bands for 5G*. ITU News, 2023. Disponível em: <https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/>.

111 BRASIL. *5G é ativado em todas as capitais brasileiras*. Brasília/DF: Ministério das Comunicações, 2022. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2022/outubro/5g-e-ativado-em-todas-as-capitais-brasileiras>.

112 BRASIL, N. U. *Levantamento sobre 5G no Brasil indica importante benefício para economia no país*. Brasília/DF: Nações Unidas Brasil, 2021. Disponível em: <https://brasil.un.org/pt-br/178976-levantamento-sobre-5g-no-brasil-indica-importante-benef\%C3\%ADcio-para-economia-no-pa\%C3\%ADs>.

113 SILVA, L. A. D. Securing 5g: Nato's role in collaborative risk assessment and mitigation. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Virginia Tech, p. 74, 2020.

114 KASPERSKY. *O que é uma Ameaça Persistente Avançada (APT)?* AO Kaspersky Lab, 2023. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/advanced-persistent-threats>.

115 TOTVS. *Entenda o que é SCADA e o seu papel dentro da indústria*. 2023. Disponível em: <https://www.totvs.com/blog/gestao-industrial/scada/>.

116 GUEDES, R. *APT: Ameaça Persistente Avançada*. DCiber, 2023. Disponível em: <https://dciber.org/apt-ameaca-persistente-avancada/>.

117 NSA-CISA. Potential threats to 5g network slicing. In: . [s.n.], 2021. p. 1–12. Disponível em: <https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL\%20THREATS\%20TO\%205G\%20NETWORK\%20SLICING_508C_FINAL.PDF>.

118 (CGI.BR), C. G. da Internet no B. *Cartilha de Seguranc¸a para Internet, versão 4.0*. Comitê Gestor da Internet no Brasil (CERT.br) São Paulo, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>.

119 FREITAS, W. *Tipos de ameaças à segurança cibernética – Maneiras de proteção cibernética*. Acadi-TI, 2019. Disponível em: <https://acaditi.com.br/tipos-de-ameacas-a-seguranca-cibernetica-maneiras-de-protecao-cibernetica/>.

120 SEGURADO, A. *Ataque cibernético: tipos de ameaças e 4 dicas para evitar*. B2BStack, 2022. Disponível em: <https://blog.b2bstack.com.br/ataque-cibernetico/>.

121 BITDEFENDER. *Bitdefender Antivirus Free for Windows keeps you safe, even against today's constantly changing e-threats*. 2023. Disponível em: <https://www.bitdefender.com/solutions/free.html>.

122 BRASIL. *Resolução nº 740, de 21 de dezembro de 2020*. Brasília/DF: Agência Nacional de Telecomunicações (Anatel), 2020. Disponível em: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020>.

123 DESENVOLVIMENTO;, B. I. de; AMERICANOS, O. dos E. *Relatório de Cibersegurança 2020: riscos, avanços e o caminho a seguir na América Latina e Caribe*. : Banco Interamericano de Desenvolvimento (BID), 2020. Disponível em: <https://publications.iadb.org/pt/relatorio-de-ciberseguranca-2020-riscos-avancos-e-o-caminho-seguir-na-america-latina-e-caribe>.

124 HARVEY, J. F.; STEER, M. B.; RAPPAPORT, T. S. Exploiting high millimeter wave bands for military communications, applications, and design. *IEEE Access*, IEEE, v. 7, p. 52350–52359, 2019.

125 SHARMA, P. K. et al. Wearable computing for defence automation: Opportunities and challenges in 5g network. *IEEE Access*, IEEE, v. 8, p. 65993–66002, 2020.

126 PEDRO, J. M. G. G. O impacto das redes 5g na segurança e defesa nacional. IUM, 2021.

127 WADE, D. 5g network information technology and military information communication data services. Feb 2021.

128 BASTOS, L. et al. Potential of 5g technologies for military application. In: IEEE. *2021 International Conference on Military Communication and Information Systems (ICMCIS)*. [S.l.], 2021. p. 1–8.

129 LI, R. Network 2030 and new ip. *IEEE CNSM*, 2019.

130 FERREIRA, J. R. da A. Aplicabilidade da tecnologia 5g para uso dos órgãos de segurança pública. *O Comunicante*, v. 10, n. 1, p. 43–49, 2020.

131 NAKAGAWA, M. *FERRAMENTA: ANÁLISE SWOT (CLÁSSICO)*. : Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), 2020. Disponível em: <https://www.sebrae.com.br/Sebrae/Portal\%20Sebrae/Anexos/ME_Analise-Swot.PDF>.

132 BRASIL. *LEI COMPLEMENTAR Nº 117, DE 2 DE SETEMBRO DE 2004*. Brasília/DF: Câmara dos Deputados, 2004. Disponível em: <https://www2.camara.leg.br/legin/fed/leicom/2004/leicomplementar-117-2-setembro-2004-533982-publicacaooriginal-17852-pl.html>.

133 BRASIL. *LEI COMPLEMENTAR Nº 136, DE 25 DE AGOSTO DE 2010*. Brasília/DF: Presidência da República, 2010. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm>.

134 BRASIL. *DECRETO Nº 9.819, DE 3 DE JUNHO DE 2019. Dispõe sobre a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo.* Brasília/DF: Presidência da República, 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9819.htm>.

135 BRASIL. *A Participação do Exército na Segurança dos Grandes Eventos – O LEGADO*. Brasília/DF: Exército Brasileiro (EB), 2018. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/1/1130/1/Grandes\%20Eventos_O\%20Legado.pdf>.

136 BRASIL. *Manual de Fundamentos – O Exército Brasileiro (EB20-MF-10.101)*. Exército Brasileiro (EB), 2014. Disponível em: <https://www.eb.mil.br/documents/10138/6563889/Manual+-+O+Ex\%C3\%A9rcito+Brasileiro/09a8b0d2-81d0-4a69-a6ea-0af9a53eaf45>.

137 BRASIL. *A Companhia de Comando e Controle (Cia C2)do Batalhão de Apoio às Operações Especiais (B Ap Op Esp)*. Comando de Operações Especiais (C Op Esp), 2021. Disponível em: <http://www.copesp.eb.mil.br/index.php/editoria-b/baoe/445-a-cia-de-comando-e-controle-do-b-ap-op-esp>.

138 BRASIL. *PARECER n. 00484/2019/CONJUR-MD/CGU/AGU*. Brasília/DF: Advocacia Geral da União, 2019. Disponível em: <https://ponte.org/wp-content/uploads/2020/04/parecer-2019-0000025959.pdf>.

139 BRASIL. *Decreto-lei no 3.437, de 17 de julho de 1941*. Brasília/DF: Presidência da República, 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/1937-1946/del3437.htm>.

140 SIGNIFICADOS. *Eficácia, eficiência e efetividade*. : 7Graus, 2023. Disponível em: <https://www.significados.com.br/eficacia-eficiencia-e-efetividade/>.

141 STELLE, C. A.; MARIA, M. A. C.; HOKAMA, M. L. *Um Estudo sobre a EBNet*. Escola de Aperfeicoamento de Oficiais (EsAEx), 2005. Disponível em: <https://docplayer.com.br/1480563-Um-estudo-sobre-a-ebnet.html>.

142 BRASIL. *Conceito de Operações do Sistema Militar de Comando e Controle (CONOPS SISMC²)*. Brasília/DF: Ministério da Defesa (MD), 2016. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/doutrina_militar/lista_de_publicacoes/md31a_sa_02a_conopsa_sismca_1a_eda_2015.pdf>.

143 BRASIL. *PORTARIA Nº 029-DCT, DE 23 DE JULHO DE 2009*. Brasília/DF: EXÉRCITO BRASILEIRO, 2009. Disponível em: <http://www.sgex.eb.mil.br/sg8/005_normas/01_normas_diversas/08_departamento_de_ciencia_e_tecnologia/port_n_029_dct_23jul2009.html>.

144 BRASILEIRO, E. *Localização dos CT (Centros de Telemática) e CTA (Centros de Telemática de Área)*. Centro Integrado de Telemática do Exército (CITEx), 2015. Disponível em: <http://www.citex.eb.mil.br/index.php/editoria-e>.

145 BRASILEIRO, E. *Programa Estratégico Gestão de Tecnologia da Informação e Comunicações*. Departamento de Ciência e Tecnologia (DCT), 2019. Disponível em: <http://www.dct.eb.mil.br/ultimasnoticias/programa-estrategico-gestao-de-tecnologia-da-informacao-e-comunicacoes>.

146 BRASIL. *Amazônia Legal*. Brasília/DF: Instituto Brasileiro de Geografia e Estatística (IBGE), 2021. Disponível em: <https://www.ibge.gov.br/geociencias/cartas-e-mapas/mapas-regionais/15819-amazonia-legal.html>.

147 STARTSE. *Como Shenzhen se tornou o principal centro de inovação do oriente*. [S.l.]: https://www.startse.com/artigos/como-shenzhen-se-tornou-o-principal-centro-de-inovacao-do-oriente/, 2023.

148 DJI. *Drones com câmera*. 2022. Disponível em: <https://www.dji.com/br/mavic-2>.

149 ALBUQUERQUE, R. F. de. *Conversa explicativa sobre o Site Móvel 5G embarcado na viatura VAN Mercedes Benz, da operadora de telefonia móvel Tim DF*. Brasília/DF: [s.n.], 2022.

150 FIGUEIREDO, F. A. P. de. *Arquitetura de Redes de Acesso de Rádio em Nuvem: Em direção a redes móveis 5G*. ReseachGate, 2020. Disponível em: <https://www.researchgate.net/profile/Felipe-Pereira-De-Figueiredo/publication/346722837_Arquitetura_de_Redes_de_Acesso_de_Radio_em_Nuvem_Em_direcao_a_redes_moveis_5G/links/5fcfb16392851c00f85f07c6/Arquitetura-de-Redes-de-Acesso-de-Radio-em-Nuvem-Em-direcao-a-redes-moveis-5G.pdf>.

151 OLIVEIRA, R. C. F. de. *O emprego dual – civil e militar – do Ecossistema na Defesa brasileira*. Brasília/DF: Google Formulário, 2022. Disponível em: <http://forms.gle/yWvSQMbYkbZ38Aat9>.

152 BAIGORRI, R. D. C. C. *Edital de Radiofrequências – Faixas de 700 MHz – 2,3 GHz – 3,5 GHz – 26 GHz*. Brasília/DF: Agência Nacional de Telecomunicações (Anatel), 2018. Disponível em: <Palestra>.

153 BRASIL. *PIB cresce 2,9% em 2022 e fecha o ano em R$ 9,9 trilhões*. Agência Brasil (EBC), 2023. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2023-03/pib-cresce-29-em-2022-e-fecha-o-ano-em-r-99-trilhoes>.

154 BRASIL. *Recuperação de Frequências*. Agência Nacional de Telecomunicações (Anatel), 2022. Disponível em: <https://sistemas.anatel.gov.br/stel/Consultas/RecuperacaoFrequencias/tela.asp?SISQSmodulo=9896>.

155 ATDI. *HTZ Warfare – Modelling all radio communications technologies between 8 KHz to 1 THz*. 2022. Disponível em: <https://atdi.com/products-and-solutions/htz-warfare/>.

156 RIBEIRO, J. A. J. *ANTENAS E PROPAGAÇÃO*. [S.l.]: Instituto Nacional de Telecomunicações (Inatel), 2010.

157 UFPR. *O dB , (decibel) e outras unidades logarítmicas: dBA, Neper, dBr, dBm, dBw, dBk, dBm0, dBu, dBsr, VU, dB, dBV/m, dBp, dBi, dBd, S unit, dBFS*. : [s.n.], 2020. Disponível em: <http://www.eletrica.ufpr.br/armando/index_arquivos/dB.pdf>.

158 ABOUELSEOUD, M.; CHARLTON, G. System level performance of millimeter-wave access link for outdoor coverage. In: IEEE. *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. [S.l.], 2013. p. 4146–4151.

159 TOMBAZ, S. *Dynamic Spectrum Sharing*. Ericsson, 2021. Disponível em: <https://www.itu.int/en/ITU-D/Conferences/GSR/2020/Documents/2020-08-26_ITU_Spectrum-Planning-for-Emerging-Technologies_Ericsson.pdf>.

160 FANG, D.; QIAN, Y. 5g wireless security and privacy: Architecture and flexible mechanisms. *IEEE vehicular technology magazine*, IEEE, v. 15, n. 2, p. 58–64, 2020.

161 BHARDWAJ, A. 5g for military communications. *Procedia Computer Science*, Elsevier, v. 171, p. 2665–2674, 2020.

162 SCHWARZ, R. . Massive mimo eight things to consider when testing antenna arrays. Rohde & Schwarz/5G, Munich, 2022. Disponível em: <https://www.rohde-schwarz.com/premiumdownload/
L1liN0RPN2NzNXVhL3JSL0FITXN2SmIyT0pzcGI1cXZPN0NVRXloSFZsL0VrWUFlYURSNDZDWnp1UDB6WjR5

163 INTELLIGENCE, G. The 5g guide: A reference for operators. *GSMA, April*, 2019.

164 BRASIL. *Doutrina de Operações Conjuntas — MD30-M-01/Volumes 1 e 2*. Brasília/DF: Ministério da Defesa (MD), 2020. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf>.

165 EL-SHORBAGY, A.-m. 5g technology and the future of architecture. *Procedia Computer Science*, Elsevier, v. 182, p. 121–131, 2021.

166 LIYANAGE, M. et al. *A comprehensive guide to 5G security*. [S.l.]: Wiley Online Library, 2018.

167 OLIVEIRA, L. A.; ALENCAR, M. S.; LOPES, W. T. A. Evolução da arquitetura de redes móveis rumo ao 5g. *Revista de Tecnologia da Informação e Comunicação*, v. 8, n. 2, p. 43–50, 2018.

168 CRUZ, S. C. V. E.; BOJIKIAN, N. M. P. De trump a biden.

169 INKSTER, N. *China's Cyber Power*. Routledge, 2018. Disponível em: <https://www.iiss.org/publications/adelphi/2016/chinas-cyber-power>.

170 NEGóCIOS, P. E. e G. *Biden sanciona lei que reforça restrições dos EUA a chinesas Huawei e ZTE*. Editora Globo, 2021. Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2021/11/epoca-negocios-biden-sanciona-lei-que-reforca-restricoes-dos-eua-a-chinesas-huawei-e-zte.html>.

171 REUTERS. *EUA proíbem vendas de equipamentos Huawei e ZTE alegando risco à segurança nacional*. Infomoney, 2022. Disponível em: <https://www.infomoney.com.br/negocios/eua-proibem-vendas-de-equipamentos-huawei-e-zte-alegando-risco-a-seguranca-nacional/>.

172 SIMS, J. W. *Cybersecurity: The Next Threat to National Security*. [S.l.], 2011. Disponível em: <https://apps.dtic.mil/sti/citations/ADA601238>.

173 BRASIL. *Cidades e Estados*. Brasília, DF: Instituto Brasileiro de Geografia e Estatística. IBGE, 2022. Disponível em: <https://www.ibge.gov.br/cidades-e-estados>.

174 BRASIL. *Prévia da população calculada com base nos resultados do Censo Demográfico 2022 até 25 de dezembro de 2022*. Brasília, DF: Instituto Brasileiro de Geografia e Estatística, IBGE, 2023. Disponível em: <https://ftp.ibge.gov.br/Censos/Censo_Demografico_2022/Previa_da_Populacao/POP2022_Brasil_e_UFs.pdf>.

175 BRASIL. *A Vertente Econômica da Amazônia Azul*. Brasília/DF: Marinha do Brasil (MB), 2019. Disponível em: <https://www.mar.mil.br/hotsites/amazonia_azul/vertente-economica.html>.

176 BRITO, F. *Corredores ecológicos: uma estratégia integradora na gestão de ecossistemas*. [S.l.]: Editora da UFSC, 2012.

177 BRASIL, O. O corredor central da mata atlântica: uma nova escala de conservação da biodiversidade. *Ministério do Meio Ambiente, Conservação Internacional e Fundação SOS Mata Atlântica*, 2006.

178 BRASIL. *Biomas*. Brasília/DF: Ministério do Meio Ambiente e Mudança do Clima, 2023. Disponível em: <https://www.gov.br/mma/pt-br/assuntos/ecossistemas-1/biomas>.

179 BRASIL. *Amazônia Azul (AAz)*. Brasília/DF: Marinha do Brasil (MB), 2019. Disponível em: <https://www.mar.mil.br/hotsites/amazonia_azul/sobre.html>.

180 BLOG, G. I. *Veja quais são as maiores economias do mundo em 2023 e o posicionamento do Brasil*. : Genial Investimentos Corretora de Valores Mobiliários S.A., 2023. Disponível em: <https://blog.genialinvestimentos.com.br/maiores-economias-do-mundo-e-posicionamento-do-brasil/>.

181 JR, J. S. N. *Cyber Power*. [S.l.], 2010.

182 NACIONAL, M. da I. *FAIXA DE FRONTEIRA Programa de Promoção do Desenvolvimento da Faixa de Fronteira (PDFF)*. Brasília/DF: Secretaria de Programas Regionais (SPR), 2009. Disponível em: <https://antigo.mdr.gov.br/images/stories/ArquivosSNPU/Biblioteca/publicacoes/cartilha-faixa-de-fronteira.pdf>.

183 BRASIL. *FRONTEIRAS TERRESTRES*. Brasília/DF: Fundação Alexandre de Gusmão (FUNAG), 2009. Disponível em: <https://antigo.mdr.gov.br/images/stories/ArquivosSNPU/Biblioteca/publicacoes/cartilha-faixa-de-fronteira.pdf>.

184 BRASIL. *SisGAAz: Proteção e Monitoramento das Águas Jurisdicionais Brasileiras*. Brasília/DF: Marinha do Brasil (MB), 2020. Disponível em: <https://www.marinha.mil.br/sisgaaz-protecao-e-monitoramento-das-aguas-jurisdicionais-brasileiras>.

185 SOLUTIONS, M. *O HACKING COGNITIVO TEM UM PODER COMO "NUNCA ANTES"*. MyCena Limited, 2023. Disponível em: <https://mycena.co/pt/o-hacking-cognitivo-tem-um-poder-como-nunca-antes/>.

186 CYBENKO, G. V.; GIANI, A.; THAYER, P. T. Cognitive hacking and the value of information. In: . [S.l.: s.n.], 2004.

187 BRASIL, B. N. *Guerra na Ucrânia: 240 mil já morreram no conflito, dizem EUA*. Gabinete de Segurança Institucional, 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-63582629>.

188 ERICSSON. *5G EVOLUTION TOWARD 5G ADVANCED: An overview of 3GPP releases 17 and 18*. ERICSSON TECHNOLOGY REVIEW, 2021. Disponível em: <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-evolution-toward-5g-advanced>.

189 JIANG, S. New ip networking for network 2030. In: *Fifth ITU Workshop on Network*. [S.l.: s.n.], 2019. v. 2030.

190 SPACE, T. *Starlink traz nova esperança para o acesso à Internet na Ucrânia*. TS2 Space Sp. z o.o., 2023. Disponível em: <https://ts2.space/pt/starlink-traz-nova-esperanca-para-o-acesso-a-internet-na-ucrania/>.

191 NOTÍCIAS, A. M. de. *Operação das Forças Armadas impõe prejuízo de 49 milhões ao garimpo ilegal*. Manaus/AM: DEFESA NET, 2023. Disponível em: <https://www.defesanet.com.br/front/noticia/1051815/operacao-das-forcas-armadas-impoe-prejuizo-de-49-milhoes-ao-garimpo-ilegal/>.

192 SANTOS, C. A. dos. *A hora e a vez da radiação terahertz?* INSTITUTO CIÊNCIA HOJE, 2023. Disponível em: <https://cienciahoje.org.br/coluna/a-hora-e-a-vez-da-radiacao-terahertz/>.

193 BRASIL. *PROGRAMA ESTRATÉGICO DE SISTEMAS ESPACIAIS (PESE) (MD20-S-01)*. Ministério da Defesa (MD), 2018. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md20a_sa_01a_programaa_estrategicoa_dea_sistemasa_espaciaisa_pesea_ed-2018.pdf>.

194 XAVIER, P. *LEO, MEO e GEO: como podemos explicar os diferentes tipos de órbita?* Viasat, 2023. Disponível em: <https://news.viasat.com/pt-br/blog/leo-meo-e-geo-como-podemos-explicar-os-diferentes-tipos-de-orbita>.

195 DICIONÁRIO, P. *Háptica*. Priberam Informática, 2023. Disponível em: <https://dicionario.priberam.org/h\%C3\%A1ptica>.