ESCOLA DE GUERRA NAVAL

CC (T) Erica Dias de Souza

A IMPLEMENTAÇÃO DO 5G NO SETOR DE DEFESA E SUA INFLUÊNCIA NO MODUS OPERANDI DA GUERRA CIBERNÉTICA

Rio de Janeiro

2021

CC (T) Erica Dias de Souza

A IMPLEMENTAÇÃO DO 5G NO SETOR DE DEFESA E SUA INFLUÊNCIA NO MODUS OPERANDI DA GUERRA CIBERNÉTICA

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CC Miguel Henrique Alexandre Dias Alves

Rio de Janeiro

Escola de Guerra Naval

2021

AGRADECIMENTOS

A Deus, por me dar forças para continuar diante dos obstáculos encontrados ao longo do curso. Sem Ele não seria possível.

À minha filha que, apesar de em sua tenra idade não entender as minhas ausências, foi a motivação para a realização deste trabalho.

Ao meu orientador, CC Miguel Alves, pela consideração, paciência e respeito com que conduziu a orientação deste trabalho, sempre de forma segura e objetiva, me incentivando a continuar.

RESUMO

A Guerra Cibernética faz parte do novo contexto de guerra dos países. O uso do espaço cibernético como meio dissuasório e como interface para os diversos dispositivos militares vem se tornando uma realidade. E, tecnologias disruptivas como o 5G têm ganhado um vasto campo na área de Defesa, onde muitas aplicações são projetadas e testadas para uso militar. Os diversos cenários de uso previstos no 5G para suprir as exigências dos mais variados setores, tais como conectividade massiva, velocidades ultrarrápidas e conexão altamente confiável para serviços de missão crítica, têm gerado demandas de novos serviços, permitindo um aumento considerável de dispositivos conectados. Neste contexto, esta monografia discorrerá sobre os conceitos e princípios da Guerra Cibernética, destacando, também, as potencialidades e disrupções do 5G, de forma que o leitor compreenda as diversas aplicações viáveis de serem implementadas na área de Defesa, visto que as soluções projetadas pretendem trazer inovações e rapidez no trato das informações, influenciando e melhorando a tomada de decisões e as condições dos soldados no campo de batalha. Desta forma, será realizada uma análise sobre como o 5G influenciará a Guerra Cibernética, que terá seu espaço permeado de aplicações militares, prospectando um cenário de ataque mais intenso, afetando diretamente o seu m*odus operandi*.

Palavras-chave: 5G. Aplicações militares. Defesa. Guerra Cibernética. IoMT.

SUMÁRIO

1 INTRODUÇÃO

As grandes guerras ensinaram como a logística para sustentá-las era de difícil execução. As tecnologias utilizadas à época precisavam, em sua maioria, ser transportadas para as regiões de conflito, assim como os militares, demandando esforço, tempo e aparatos de segurança, tornando os custos elevados. Ademais, o alcance dos alvos não era preciso, ocasionando grandes danos materiais e humanos muitas vezes desnecessários, arruinando economias como no caso da 1ª Guerra Mundial.

A devastação econômica dos países participantes da Grande Guerra acabou por se tornar a fagulha que culminou na 2ª Guerra Mundial, igualmente devastadora, conhecida por ser o maior conflito armado da história. Os ensinamentos obtidos nestas e noutras guerras que se sucederam fizeram com que os países se adaptassem, buscando restringir os meios cinéticos, direcionando suas capacidades para uma modalidade de guerra menos custosa, porém, potencialmente danosa e com escopo mais previsível.

A Guerra Cibernética, também conhecida como a "Guerra do Futuro", passou a ser uma opção vantajosa para as diversas nações, visto que o emprego das forças humanas que antes se expunham nas linhas de frente das batalhas, deixando milhões de vítimas, passaram a estar protegidas sob um anonimato intencional, além de gerar economia de meios, rapidez e precisão de objetivos. É a guerra sem fronteiras, onde tornou-se difícil prever a chegada do inimigo, alcançando um dos fatores mais valiosos para atingi-lo: o efeito surpresa.

Com a instituição do Direito Internacional dos Conflitos Armados (DICA), que procurou de certa forma "humanizar" a guerra, o estímulo a novos meios que pudessem alcançar os objetivos das nações sem, no entanto, afetar de maneira significativa vidas humanas, fez com que a Guerra Contemporânea exigisse mais que armamentos, moldando seus ataques com o uso de tecnologias avançadas. Desta forma, o 5^0 Domínio[1] da Guerra tornou-se o ícone de uma intervenção profícua de alcance global.

O rápido desenvolvimento de novas tecnologias culminou, então, no favorecimento do espaço cibernético como um meio de guerra. Assim como a internet em seus primórdios, com a incipiente *Advanced Research Projects Agency Network* (Arpanet)[2] criada para fins militares, novas tecnologias disruptivas inevitavelmente vêm sendo

1 São considerados domínios de Guerra os espaços terrestre, naval, aéreo, espacial e cibernético.

2 Rede de Pesquisas desenvolvida pela atual *Defense Advanced Research Projects Agency* (DARPA) em conjunto com as principais universidades e centros de pesquisa dos EUA, com intuito de manter a segurança das comunicações militares, em caso de ataque a um dos nós. Com seu exponencial crescimento, acabou por tornar-se a precursora da internet.

incorporadas como tecnologias facilitadoras dos meios militares, influenciando diretamente as operações de guerra.

Como resultado, tem-se uma era de inovações que exigirá dos diversos países um planejamento quanto aos artifícios a serem usados neste novo ambiente de guerra. E as forças militares, em seus planejamentos estratégicos, não poderão ignorar as possíveis ameaças, investindo em tecnologias cujo uso poderão impulsionar as ações defensivas e ofensivas.

Neste contexto, evidencia-se que os países detentores de inovações tecnológicas que possam melhorar o desempenho cibernético voltado para a guerra, serão aqueles com maior probabilidade de obter vantagens em possíveis conflitos. No entanto, não basta ser detentor da tecnologia, é necessário prever aplicações direcionadas para o campo de Defesa, usufruindo dos benefícios trazidos por tais evoluções.

Em consonância com este novo cenário, a tecnologia 5G tem surgido como um modelo com potencial para influenciar de maneira significativa o novo ambiente operativo de guerra, gerando facilidades e permitindo novas aplicações que comporão os campos de batalha. A 5ª geração de internet móvel tem sido o cerne das questões que envolvem as novas projeções de uso do espaço cibernético para fins militares.

Alguns países têm apresentado soluções para a área de Defesa, projetando o uso do 5G em cenários que poderão ser potencializados com os diferenciais da tecnologia, além de novos empregos que só se tonarão factíveis muito em função de outras tecnologias que vieram de “carona” com a promissora geração de rede móvel.

Diante do exposto, o presente trabalho tem a intenção de analisar de que forma o 5G, como tecnologia disruptiva, poderá ser implementando no setor de Defesa, impactando no *modus operandi* da Guerra Cibernética, mostrando as oportunidades para o uso da nova tecnologia no campo de batalha e em aplicações militares em geral.

Para tal fim, este trabalho encontra-se dividido em cinco capítulos. Após o presente capítulo com esta introdução, tem-se o segundo capítulo que traz a conceituação da Guerra Cibernética bem como os seus princípios, a fim de contextualizar o *modus operandi* neste novo ambiente de guerra, bem como suas características principais, provendo conhecimentos que permitirão o melhor entendimento de como a tecnologia de quinta geração pode influenciar operações que utilizam o espaço cibernético.

O terceiro capítulo discorre sobre a evolução tecnológica da internet móvel até a chegada do 5G, de forma a mostrar os motivos da nova tecnologia não ser considerada apenas uma evolução das anteriores, mas sim uma inovação. Nesta seção serão descritas,

ainda, as principais características do 5G, que permitem um melhor entendimento a respeito do seu funcionamento e possibilidades de emprego em aplicações de Defesa.

O quarto capítulo apresenta algumas projeções de aplicações do 5G na área de Defesa, com as oportunidades de emprego e seus pontos fortes quando utilizadas nas diversas operações e realidades militares, indicando, quando aplicável, os projetos e testes já em andamento em alguns países. Em complemento, será mostrada a influência do uso ampliado do espaço cibernético para operações de guerra, em função da junção da Guerra Cibernética com a tecnologia de 5ª Geração. E por fim, a conclusão com a visão geral deste trabalho.

Para realizar esta abordagem, foram utilizados como recursos metodológicos a pesquisa bibliográfica e documental, tendo como fontes sites especializados da internet, bem como livros, artigos acadêmicos e doutrinas que regem os assuntos aqui abordados.

2 GUERRA CIBERNÉTICA: CONCEITOS E PRINCÍPIOS

De acordo com Clarke e Knake (2015), nos idos de 1990, a Guerra Cibernética era confundida pelas Forças Armadas como Operações de Informações ou Operações Psicológicas. Já o setor de Inteligência passou a enxergar o crescimento da internet como um meio de espionagem eletrônica. Porém, durante as coletas de informações, começou a ficar claro que uma sequência específica de teclas seria capaz de derrubar uma rede. Com isso, gerou-se o dilema de divulgar ou não que o espaço cibernético tornava possível um novo tipo de guerra, visto que se o fizessem, perderiam o controle desse espaço para os *geeks*[3]. O dilema foi solucionado com a certeza de que as oportunidades apresentadas neste tipo de guerra, para atingir de forma considerável o oponente, eram valiosas demais para passar despercebidas.

Com o passar do tempo, considerações mais precisas a respeito das novas táticas de guerra foram se formando, criando definições e princípios mais consistentes que regem este modelo de combate, conforme descritos a seguir.

2.1 Conceito de Guerra Cibernética

Segundo o Ministério da Defesa (MD), em sua Doutrina Militar de Defesa Cibernética (DMDC), a Guerra Cibernética:

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático

3 Pessoa aficionada da tecnologia.

> ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014, p.19).

Conforme verifica-se no conceito acima, o termo Guerra Cibernética, dada a sua atuação para fins militares, é restrito às Forças Armadas (FA), visto que as ações cibernéticas, neste sentido, demandariam os meios operativos e táticos destas forças. No entanto, o conceito também pode ser conhecido de forma mais abrangente, sem um cunho especificamente militar.

Neste sentido, uma outra definição também aceita seria a Guerra Cibernética como sendo o uso de ataques cibernéticos entre nações, cujo resultado geraria danos significativos, incluindo uma guerra física e interrupção de sistemas vitais, considerando também a possibilidade de perda de vidas (HANNA; FERGUSON; ROSENCRANE, 2021).

O termo “Guerra Cibernética”, no entanto, gera algumas discussões a respeito de sua caracterização. Especialistas questionam quais seriam os limites que definiriam o que seria apenas um ataque cibernético, evidenciando um crime, e o que denotaria efetivamente uma Guerra Cibernética. O fato é que este tipo de guerra se utiliza de ataques cibernéticos para atingir suas finalidades.

Desta forma, o que difere a Guerra Cibernética de um crime cibernético, dentre outros, é a intenção, a origem do ataque e alvo de destino. Para caracterizar a guerra no espaço cibernético seria preciso analisar quais seriam os alvos envolvidos, os autores do ataque, se houve investimento público nas ações empreendidas, resultando em ferramentas e metodologias mais avançadas, caracterizando um conflito entre nações adversárias.

Neste cenário, seria importante frisar, ainda, que o fato de um ataque partir de um país para outro, não caracteriza a intenção ou o começo de uma Guerra Cibernética. As conclusões a esse respeito dependerão de diversos fatores que precisarão ser analisados de acordo com a conjuntura envolvida. Sem que haja um objetivo específico de prejudicar uma nação ou responder a algo que envolva assuntos políticos internacionais, mesmo que o resultado do ataque cause sérios danos à nação atingida, poderá tratar-se, apenas, de um ataque cibernético (COMPUGRAF, 2020).

Outra característica que gera dúvidas se um determinado ataque faz parte ou não de uma Guerra Cibernética é o fato de não haver uma declaração formal de guerra, instituindo o seu início ou final, sendo executada numa informalidade preocupante e sem leis

ou acordos que controlem ou limitem as ações, visto que tem o potencial de interromper o funcionamento de infraestruturas vitais para a população de um país.

Corroborando com essa visão, Clarke e Knake (2015) consideram que as diversas nações já vêm preparando seus campos de batalha antecipadamente, invadindo redes de interesse, instalando gatilhos lógicos em tempo de paz, levando em conta uma condição permanente de Guerra Cibernética, em função de uma instabilidade incessante. Desta forma, presume-se que futuros conflitos cibernéticos afetarão diretamente o equilíbrio militar do mundo, alterando relações políticas e econômicas de maneira indiscriminada.

Neste contexto, o estrategista militar Clausewitz (1883) dizia que a guerra seria a continuação da política, porém por outros meios, corroborando com a ideia de que a componente política é uma das premissas básicas para se pensar em guerra. E, em se tratando da Guerra Cibernética como um método expoente para atingir nações inimigas, entender seus princípios torna-se importante para uma melhor compreensão de como as ações cibernéticas podem ser operacionalizadas.

2.2 Princípios da Guerra Cibernética

Parks e Duggan (2011) indicam alguns princípios para a condução da Guerra Cibernética, comparando-os, em alguns momentos, à Guerra Cinética[4]. Destaca-se que os princípios de uma guerra guiam o combate em todos os seus níveis, sejam eles estratégico, tático ou operacional, de acordo com suas possibilidades de emprego.

Cabe ressaltar que os autores ao sugerirem esses princípios, não tiveram a intenção de esgotá-los, sendo uma proposta para discussão da comunidade cibernética no que se refere ao assunto. Os princípios tiveram como base a experiência prática dos autores como parte do *Sandia National Laboratories' Information Design Assurance Red Team* (IDART)[5].

Esses princípios nada mais são que características intrínsecas da Guerra Cibernética, em função do seu *modus operandi*, quando em combates reais ativos e online, sendo aqui destacados, a fim de prospectar como o uso de novas tecnologias podem potencializar ações, gerando vantagens no ambiente cibernético, conforme listados a seguir:

a) Efeitos no mundo cinético

Neste princípio, espera-se que a Guerra Cibernética, mesmo sendo operada no espaço cibernético, tenha efeitos no mundo cinético impactando a sociedade ou a força

4 A Guerra Cinética é a guerra convencional ocorrida no "mundo real", praticada em terra, mar, ar e espaço.

5 O *Red Team* é uma equipe que trabalha realizando testes de penetração para verificar a segurança de sistemas e redes. Neste caso, os autores realizavam este trabalho utilizando o *framework* IDART, desenvolvido pelo *Sandia National Laboratories,* projetado para identificar vulnerabilidades de acordo com comportamentos prováveis de adversários.

adversa, como em ataques que afetem infraestruturas críticas de um país inimigo, ultrapassando as fronteiras virtuais.

Como exemplo prático do uso de artefato cibernético para conseguir esse efeito, tem-se o ataque empreendido na usina de enriquecimento de urânio de Natanz, no Irã, em abril de 2021, tendo como resultado algumas centrífugas danificadas. Acredita-se que a causa tenha sido um ataque cibernético bem-sucedido arquitetado pelo Estado de Israel, ao Sistema de Controle Industrial (ICS, sigla em inglês) da usina, num esforço para frear o programa nuclear iraniano (THE GUARDIAN, 2021).

A usina nuclear, parte crucial do programa atômico iraniano, já havia sido atacada em 2010 pelo *worm* Stuxnet, também atribuído a Israel em parceria com os EUA, caso que gerou grande repercussão. O *worm*, artefato bastante sofisticado, foi projetado especificamente para atacar as centrífugas nucleares, resultando na destruição de mais de mil delas, gerando um atraso de anos no projeto nuclear iraniano. O *malware* teria explorado vulnerabilidades desconhecidas do Windows, com intuito de atingir o sistema de controle de automação e monitoramento industrial, conhecido como SCADA, desenvolvido pela Siemens, tornando-se o calcanhar de aquiles das grandes instalações industriais (THE GUARDIAN, 2021).

b) Ausência de fronteiras

Em uma Guerra Cibernética não há limites de distância ou espaço. Os autores dos princípios dizem que no espaço cibernético a distância física não representa um obstáculo e nem um facilitador para a execução dos ataques, e que a efetividade dos resultados é independente da localização física da força adversa. Os autores ressaltam, ainda, que com o uso indiscriminado de redes sem fio, os ataques adquiriram uma nova dimensão física, intensificando ainda mais essa característica de amplitude geográfica.

Na Guerra Cinética, as armas utilizadas precisam muitas vezes ser transportadas por grandes distâncias, podendo, ainda, ocorrer perdas materiais desses artefatos durante a batalha. Na Guerra Cibernética, a distância a ser percorrida dependerá da tecnologia a ser utilizada no "campo de batalha", podendo ter suas "armas" replicadas e distribuídas de maneira rápida e destrutiva. Neste princípio, tem-se claramente a importância do uso de novos recursos tecnológicos para que o resultado seja alcançado de forma eficaz.

c) Furtividade

O princípio da furtividade confere à Guerra Cibernética a característica de disfarce, incutindo, porém, uma contradição, visto que apesar de as técnicas utilizadas para

esconder os passos no espaço cibernético, tudo que é feito neste ambiente é possível de ser rastreado, interferindo na anonimização.

A dificuldade de rastreio estaria em procurar no lugar certo, na hora certa. Tal princípio, porém, incute o efeito surpresa nas ações, visto que não é fácil saber quando o oponente está próximo de atacar. Representaria o equivalente a uma camuflagem na Guerra Cinética.

Na guerra convencional, o efeito surpresa acaba quando a chegada do inimigo é visualizada no horizonte, permitindo à outra parte reagir para se defender da incursão. No caso do espaço cibernético, a furtividade pode favorecer o atacante, resultando na limitação de ação do atacado. Normalmente, o resultado consolidado do ataque torna-se o ponto de partida para que uma reação ocorra, podendo inutilizar ou fragilizar, porém, os meios que seriam utilizados como resposta.

d) Mutabilidade e Inconsistência

Na guerra empreendida no mundo físico, quando um atirador dispara um projétil, é possível prever a sua trajetória por meio da ciência da balística, com possíveis variações em função do ambiente físico. No espaço cibernético, no entanto, essa precisão não é possível, visto que o ambiente pode mudar durante o ataque, não podendo prever o quão essas mudanças poderão influenciar diretamente nesse ataque.

De acordo com Singer e Friedman (2014), o espaço cibernético é sem dúvidas bem mais mutável que os outros ambientes, pois montanhas e oceanos não são mobilizáveis, mas áreas do espaço cibernético podem ser ligadas e desligadas apenas com o clique de um botão.

Desta forma, compreende-se que no espaço cibernético não se aplicam as leis imutáveis da física, a não ser aquelas que representem alguma ação no mundo cinético. Este espaço de batalha é mutável, o que o torna inconsistente e não confiável, precisando abranger várias hipóteses para a execução do ataque, tendo, ainda assim, uma imprevisibilidade nos resultados.

A falha de um software ou hardware, as alterações de configuração dos sistemas em meio a um ataque sendo empreendido e falhas de rede são exemplos de inconsistências que podem causar mudanças do ambiente cibernético. Em função disso, torna-se difícil afirmar se uma etapa empreendida em um ataque funcionará como esperado.

e) Identidade e Privilégios (Usurpação)

No espaço cibernético, aquele que tiver o controle do espaço utilizado pelo oponente poderá usurpar da identidade e privilégios deste, assumindo sua posição. Este é um

princípio que demonstra claramente o que pode acontecer, por exemplo, quando um determinado país é detentor de alguma tecnologia ou equipamento cujo uso de outras nações possa favorecer interferências intencionais do país detentor dessa tecnologia.

Em função do espaço cibernético ter sido construído de forma artificial, ele será de alguma forma controlado pelas pessoas e ferramentas por elas desenvolvidas. Sempre haverá neste espaço alguém com acesso, autoridade e habilidade para realizar as ações que o oponente pretende realizar. Neste caso, para que um ataque prospere, o atacante precisará assumir identidade e privilégios dessa pessoa no ambiente a ser explorado, levando em conta que não há no mundo cibernético nenhuma parte considerada neutra.

f) Uso Dual

Na Guerra Cinética, dificilmente um armamento poderá ser utilizado de maneira dupla. Não será possível, por exemplo, utilizar um armamento contra um inimigo e também na própria tropa, assim como também não se emprega um carro de combate contra o oponente e os próprios soldados.

Em contrapartida, as ferramentas utilizadas na Guerra Cibernética sempre são de duplo propósito, podendo ser usadas tanto para ataque quanto para defesa. Como exemplo, pode-se citar o uso de um *scanner* de vulnerabilidades[6], que se empregado de forma maliciosa, pode buscar vulnerabilidades na rede a ser atacada, e se empregado de forma defensiva, pode mostrar os pontos fracos a serem corrigidos na própria rede.

Com o uso dual das ferramentas e consequentemente dos procedimentos, tem-se o chamado “dilema do atacante”, que faz com que um atacante, diante da descoberta de uma vulnerabilidade, tenha dúvidas quanto à sua correção, uma vez que se não corrigi-la, poderá usufruir dela para uma possível exploração, e de outro modo, ao efetuar a correção, estará fortalecendo suas próprias defesas (BRASIL, 2014).

g) Compartimentação (Controle da Infraestrutura)

Tanto o atacante quanto o defensor controlam apenas uma pequena parte do espaço cibernético pretendido. Ambos podem intervir, normalmente, nos hardwares e softwares que lhes pertencem, limitando-se aos seus perímetros de segurança. Raramente esse controle se expande para além de suas próprias infraestruturas.

E, ainda que esse controle se expanda, sugere-se que apenas 10% deste perímetro (PARKS; DUGGAN, 2011), aproximadamente, seja controlado de forma concreta, visto que em uma infraestrutura de rede, sempre haverá equipamentos, enlaces e serviços pertencentes

6 Ferramenta utilizada para realizar varredura em redes, seus softwares e dispositivos, com intuito de identificar possíveis brechas de segurança.

a uma terceira parte, que detém o poder de administrá-los de forma conveniente aos seus interesses no caso de uma Guerra Cibernética.

Um exemplo contundente são as empresas que disponibilizam os *backbones*, provedores de internet, serviços de *Domain Name System* (DNS) e roteadores. Desta forma, tanto o ataque quanto a defesa estão vulneráveis a esta terceira parte envolvida no processo. Em consequência, neste princípio, quem conseguir controlar essas infraestruturas, ficará em vantagem em relação ao oponente.

h) Informação como ambiente operacional

Toda guerra precisa de estratégias e táticas. Mas para isso, é preciso conhecer o ambiente operacional e suas particularidades. Neste contexto, a informação torna-se uma preciosa arma que conduzirá a melhor tática a ser implementada.

Na guerra convencional, fatores que definem a realidade física do ambiente operacional estão diretamente ligados ao terreno, ao clima, ao conhecimento das potencialidades inimigas, dentre outros. É necessário, então, transformar esses sensores físicos em informação. No caso da Guerra Cibernética, as próprias informações já constituem esse ambiente, tornando-o fértil para a batalha.

Com isso, atribui-se à Guerra do Futuro um vasto campo de informações que se exploradas de forma criteriosa e adequada, trazem a amplitude ideal para ser analisada na tomada de decisões tanto no ataque quanto na defesa. Mas para essa exploração, é necessário utilizar ferramentas apropriadas que no caso da Guerra Cibernética é o emprego de tecnologias de ponta. Neste contexto, tem-se o 5G como tecnologia facilitadora que agregará nos futuros combates, conforme será verificado a seguir.

3 TECNOLOGIA 5G: POTENCIALIDADES E DISRUPÇÃO

A tecnologia 5G já faz parte do cotidiano de alguns países, sendo considerada uma evolução promissora no que se refere não só à comunicação móvel mundial, mas agregando potencial a diversas outras tecnologias, abrindo um leque de possibilidades para os diversos setores, dentre eles o de Defesa.

Para compreender as motivações da tecnologia 5G ser considerada disruptiva, faz-se necessário relembrar a evolução da comunicação móvel com suas possibilidades e limitações comparadas aos recursos que serão disponibilizados com a implementação da quinta geração de rede móvel.

3.1 Evolução tecnológica da telefonia e internet móvel

De acordo com o QMC Telecom (2020) e a Sociedade 5G (2019), a evolução da telefonia e internet móvel ocorreu conforme descrito a seguir.

Os primórdios desta tecnologia encontram-se na década de 80, com o antigo 1G, primeira geração de telefonia móvel, com sinal analógico, utilizando-se do sistema *Advanced Mobile Phone System* (AMPS) que suportava apenas chamadas de voz, com aparelhos que pesavam 1kg, aproximadamente, cuja ligação sofria várias interferências e com cobertura limitada a determinadas regiões onde existiam antenas próprias para disponibilidade de sinal.

O 2G, a segunda geração que chegou nos anos 90, trouxe o sinal digital, predominando o sistema *Global System for Mobile Communications* (GSM), ainda em uso para chamadas de voz e operações via *Point-of-Sales* (POS)[7] por ter menor custo. *O* 2G permitiu, além das chamadas de voz, o envio de *Short Messaging Service* (SMS). Implementou uma internet bastante lenta, com velocidade de 64 a 144 kbps, o que à época foi considerado uma grande evolução. Com esta internet, já no final do 2G foi possível baixar sons e imagens, porém de forma bastante limitada.

Com a chegada do 3G nos anos 2000, ocorreu um grande ganho em termos de conectividade, trazendo um aumento exponencial da velocidade da internet até então disponível, chegando à promessa de mais 2Mbps, obtendo taxas próximas a 144,4 Kbps, que chegavam até 21 Mbps, o que aumentou a potencialidade dos dispositivos, introduzindo os *smartphones* com diversas funcionalidades, e permitindo a transmissão de vídeos em tempo real, além de *streaming* de música e vídeo e mensagens de texto longas. As ligações de voz tornaram-se escassas, dando vez às mensagens instantâneas.

O 4G foi implementado em 2010, chegando ao Brasil em 2013, sendo conhecido também como *Long Term Evolution* (LTE), priorizando o tráfego de dados em vez do tráfego de voz (BRAGA, 2018), conseguindo alcançar velocidades de 150 Mbps nos dispositivos móveis, dez vezes mais rápido que o 3G. Trouxe consigo os *streamings* de vídeo de alta resolução em tempo real, com qualidade *Hight Definition* (HD), jogos on-line e algumas poucas aplicações de missão crítica em função da baixa taxa de latência[8] até então considerada. Foi a geração que mudou o comportamento digital em função das novas perspectivas criadas por essa conexão móvel, incrementando, ainda, o uso das diversas redes sociais.

Já o 4G+ ou 4G LTE *Advanced* aumentou a velocidade da rede em torno de quatro a cinco vezes mais que o 4G, alcançando taxas de 600 Mbps, podendo, porém,

7 Transações financeiras realizadas em máquinas de cartão de crédito.
8 A latência é o tempo que um pacote leva para chegar da origem ao destino.

apresentar variações de velocidade e disponibilidade conforme a localização que atende. Com o término do sinal de TV analógico e consequente liberação da faixa de 700 Mhz, a tecnologia ganhou espaço, se expandindo no mercado. Não representando, no entanto, uma intermediária entre o 4G e o 5G, visto a exponencial e díspar velocidade desta última rede em relação às anteriores (GARRETT, 2017). O 4,5G ou LTE *Advanced Pro* é o nome comercial dado ao 4G+ em sua melhor performance, visto algumas melhorias na qualidade do sinal, velocidade e tráfego de dados.

A demanda por uma maior conectividade, velocidade, cobertura e disponibilidade, em função do aumento de dispositivos, fez com que se chegasse à quinta geração de redes móveis, consolidando o 5G. Esta última tecnologia vem sendo implementada pelo mundo desde seu lançamento comercial em 2019, não sendo ainda tão difundida, por questões de infraestrutura, além de política e segurança.

> Assim, pode-se entender que o 5G não é apenas uma evolução do 4G: sua proposta vai além do simples aumento da capacidade de vazão do transporte de dados, como ocorreu nas mudanças de geração anteriores. As redes móveis 5G proporcionarão serviços avançados de banda larga móvel, com taxas de dados mais altas, menor latência e mais capacidade, que possibilitarão enorme potencial para novos serviços sem fio de valor agregado. (MCTIC, 2019, p.3).

Deste modo, diante das novas possibilidades provenientes das redes 5G, faz-se necessário um melhor entendimento a respeito de sua arquitetura e cenários de uso, no intuito de compreender suas reais potencialidades e tecnologias promissoras que estão sendo impulsionadas com a sua implementação.

3.2 Arquitetura do 5G e projeções de uso

A rede móvel de quinta geração foi idealizada para responder às demandas de conectividade, velocidade, latência e confiabilidade que suas antecessoras não conseguiram suprir, tais como *streaming* de vídeo de alta resolução, utilização de aplicativos de realidade virtual e aumentada, além de diversas outras aplicações que exigem tráfego rápido e confiável (FIG01 – ANEXO). Deste modo, conforme já citado, a quinta geração de redes móveis não representa apenas a evolução das redes anteriores, mas sim um modelo disruptivo para atender às necessidades emergentes de conexão móvel dos diversos setores.

A padronização do 5G ficou sob a responsabilidade de duas grandes instituições mundiais, a *International Telecommunication Union* (ITU), que definiu os requisitos e diretrizes para a implementação da tecnologia, e o *3rd Generation Partnership Project* (3GPP), que tem por atribuição definir e manter o padrão técnico das tecnologias que

servirão de base para satisfazer os requisitos de implantação da rede de quinta geração (MCTIC, 2019).

As redes 5G preveem uma velocidade de transmissão de até 10 Gbps, contra 1Gbps do seu antecessor 4G/LTE, o que corresponde a baixar um vídeo inteiro em pouquíssimos segundos, aumentando a velocidade de 100 a 1000 vezes em relação a atual rede. As conexões possíveis são de até 1 milhão de dispositivos por quilômetro quadrado, volume de tráfego de 1 Terabit por segundo (Tbit/s), permitindo, ainda, uma mobilidade de até 500 km/h em trens de alta velocidade e até 1000 km/h em aviões (MECHAILEH, 2020).

Outra característica que faz dessa tecnologia um expoente é a baixíssima taxa de latência que enquanto no 4G é de 35 a 52 milissegundos (ms), no 5G ela é de 1ms, tornando o tempo de resposta mais rápido e satisfatório, entregando conexões mais estáveis e com menos atrasos, favorecendo e promovendo o uso de outras tecnologias como a Internet das Coisas (IoT – *Internet of Things*), serviços em nuvem, *Big Data*, Inteligência Artificial (IA), além de outros serviços inovadores (NOOHANI; MAGSI, 2020).

Dentre as vantagens esperadas em relação ao 4G, além do aumento das taxas de transmissão e latência, estão a maior densidade de conexões por área, maior eficiência no uso do espectro e maior eficiência energética, o que reduzirá o consumo de energia e o incremento da sustentabilidade (ANATEL, 2021).

O foco desta nova tecnologia não se encontra somente no aumento da velocidade de transmissão, mas no atendimento a uma diversidade de aplicações com suas diferentes necessidades, respondendo a todas elas de maneira versátil, unindo soluções e outras tecnologias que as tornarão mais eficazes e com resultados que correspondam às demandas dos variados setores.

Desta forma, a aplicação de tecnologias disruptivas na Guerra Cibernética como é o caso do 5G, demanda o conhecimento de suas potencialidades e limitações. E, em se tratando de inovações ainda incipientes em todo o mundo, é fundamental o conhecimento a respeito de suas características de projeto, a fim de compreender o seu alcance e projeção de uso. A intenção deste trabalho não é esgotar todos os detalhes técnicos da tecnologia 5G, abordando apenas os considerados essenciais para o entendimento de suas várias possibilidades, principalmente no que se refere a área de defesa.

Neste contexto, alguns requisitos técnicos importantes de serem mencionados serão mostrados a seguir.

3.2.1 Cenários de uso do 5G

O 5G, em sua arquitetura, previu a disponibilidade de vários serviços heterogêneos, para os quais servirá de suporte. E para cumprir as exigências desses serviços, será necessário um equilíbrio entre velocidade, latência, confiabilidade, disponibilidade e largura de banda, conforme as particularidades de cada um. Desta forma, dividiu-se em três grandes grupos de cenários de uso (FIG02 – ANEXO) serviços e aplicações que compartilharão os mesmos requisitos (ANATEL, 2021).

a) Banda Larga Móvel Aprimorada (eMBB - *Enhanced Mobile Broadband*)

Este cenário prevê a disponibilidade de altas velocidades de download e upload, visando atender aos serviços utilizados por usuários comuns de banda larga, que exigem uma ampla área de cobertura, tais como navegação rápida de internet, jogos em nuvem, transmissão de conteúdos multimídia 4K/8K, realidade virtual, hologramas, robôs colaborativos, dentre outros. Os principais requisitos de desempenho neste cenário são largura de banda e velocidade de transmissão.

b) Comunicação do Tipo Maquina Massiva (mMTC - *Massive Machine Type Communications*)

Este cenário de uso prevê a possibilidade de conexão massiva de dispositivos, focando nas comunicações Máquina a Máquina (M2M – *Machine to Machine*), aplicações não críticas de comunicações Veículo para Veículo (V2V- *Vehicle to Vehicle*), uso de sensores inteligentes sem fio, provendo cobertura em áreas restritas ou mais extensas, em dispositivos com pouca mobilidade, permitindo um baixo consumo de bateria. Este cenário impulsionará o uso da IoT, tornando-se a solução tecnológica viável para sua expansão. Dentre os serviços previstos estão as *Smart Cities*, *Smart Homes*, monitoramento ambiental, controles de estoque inteligentes, dentre outros. A característica principal neste caso é a hiperconectividade e eficiência energética.

c) Comunicação de Baixa Latência Ultra Confiável (URLLC - *Ultra Reliable Low Latency Communications*)

Este cenário foi desenvolvido para atender a serviços de “missão crítica” que exijam altíssima confiabilidade e baixíssima latência, que são o caso, por exemplo, de aplicações em tempo real onde qualquer atraso ou erro pode ser crucial, como em cirurgias remotas, direção autônoma, automação industrial, serviços de reabilitação por meio de exoesqueleto remotamente controlado por terapeutas com realimentação tátil (ITU, 2014). Neste cenário, em função da criticidade das aplicações, a taxa de disponibilidade precisa ser de 99,99999%, com uma latência menor que 1 milissegundo (MECHAILEH, 2020).

3.2.2 Componentes tecnológicos do 5G

Para que o 5G possa atender aos requisitos tecnológicos de velocidade, latência e disponibilidade a que se propõe, é necessária a implementação e suporte de diversas tecnologias que servirão de base, algumas já existentes nas redes 4G LTE e outras que foram propostas com o advento da quinta geração de redes. Dentre as tecnologias fundamentais para a efetivação do 5G estão:

a) Fatiamento de Rede (*Network Slicing*)

A implementação do fatiamento de Rede permite a uma infraestrutura de rede comum fazer a personalização, isolamento e suporte a multilocação de serviços, possibilitando a divisão física e lógica dos recursos dessa rede (LOPES; LOPES, 2019). Com esta tecnologia é possível compartilhar em uma mesma infraestrutura física, diferentes redes lógicas capazes de atender aos distintos cenários de uso e suas respectivas demandas, sem influenciar no tráfego uma da outra (FIG03 – ANEXO).

Desta forma, cada aplicativo poderá ser configurado para atender especificamente as suas peculiaridades, sem prejudicar os requisitos demandados por outras aplicações que dividem a mesma rede. Cada fatia é isolada virtualmente uma da outra, permitindo o ajuste ideal para cada grupo de serviços que possui as mesmas exigências técnicas. A virtualização de rede é a tecnologia que dá o suporte a essa variedade de arquiteturas independentes implementadas em cada fatia.

b) Pequenas Células (*Small Cells*)

Diferentemente do 4G e das outras gerações de tecnologias móveis, que dependem de grandes torres atendendo a dezenas de quilômetros quadrados, cada uma delas, o 5G trouxe o conceito de pequenas células que são distribuídas aos milhares, para atender a extensões menores, porém utilizando de maneira mais eficiente o espectro, propiciando uma melhor cobertura, sem os “pontos cegos” existentes em determinadas áreas por falta de alcance das antenas ou devido a obstáculos. As redes 4G+ já utilizam, em parte, este tipo de estações base, necessitando, porém, de um número muito maior destas para atender às exigências do 5G (SILLIMAN, 2018).

Em função do pequeno tamanho e custo, as antenas poderão ser instaladas em maior número, atendendo à demanda por maior conectividade em áreas com maior concentração de equipamentos. As *small cells* representarão um novo paradigma para o mercado de internet móvel, visto que reduzirão a dependência de hardware e pessoal altamente especializado, em consequência da maior facilidade e rapidez de instalação, acelerando a entrega do serviço (INTRAWAY, 2019). Como alcançam uma menor área

geográfica, utilizam transmissores de baixa potência, sendo bastante adequadas para áreas urbanas, onde normalmente existem muitas barreiras tais como prédios e árvores, podendo ser instaladas em locais mais fáceis como em postes de luz (FIG04 – ANEXO) (MECHAILEH, 2020).

c) MIMO Massivo (*Massive* MIMO)

A tecnologia *Multiple-Input and Multiple-Output* (MIMO) já é utilizada nas atuais redes 4G. Ela consiste em um método que utiliza múltiplas antenas transmissoras e receptoras para expandir a capacidade de um link via rádio. E, o MIMO Massivo é a utilização desta tecnologia com um número bastante vasto de antenas[9] aumentando, desta forma, a sua eficiência espectral e a cobertura da rede que usufrui do sinal (JUNIPER, 2021).

Além do ganho de fluxo de dados, as antenas MIMO podem, também, melhorar a relação sinal-ruído dos canais com a utilização de antenas direcionais. Tecnologia ainda mais avançada é a *Full Dimension* MIMO (FD-MIMO), que é capaz de formar feixes nas direções horizontal e vertical, alcançando todos os espaços 3D (FIG05 – ANEXO). Tal inovação permite ganhos exponenciais em relação à tecnologia padrão, obtendo melhoria de resultado de 3 a 5 vezes na capacidade e na taxa de transferência (MECHAILEH, 2020).

d) *Beamforming*

O *Beamforming* é uma tecnologia de distribuição de sinal que emite feixes com ondas milimétricas de rádio de maneira mais direcional aos diversos dispositivos móveis que demandam por sinal de rede sem fio, melhorando, desta forma, a largura de banda e tornando a conexão mais rápida. Uma estação base localiza o dispositivo solicitante e transmite o sinal especificamente na direção deste.

Uma maneira bastante simples de se explicar esta tecnologia é fazendo uma analogia com uma lâmpada de luz que ao ser ligada emite luz de maneira indiscriminada no ambiente, representando um sinal sem o uso do *Beamforming*. Com a implementação da tecnologia, seria o equivalente a colocar um cone na lâmpada, evitando que o feixe de luz se espalhe por todas as direções, concentrando-o unicamente na direção onde é necessário (COSSETTI, 2019).

A tecnologia *Beamforming* é usada em conjunto com os múltiplos transmissores e receptores MIMO (FIG06 – ANEXO) que utilizam um farto número de antenas para propagar este tipo de sinal, com intuito de aumentar o alcance do link, a taxa de transferência de dados e reduzindo possíveis interferências, visto que o sinal não é propagado em direções

9 O número de antenas MIMO Massivo varia de acordo com o cenário onde são implementadas, não podendo estimar um número específico, sendo, no entanto, bem maior que as utilizadas na tecnologia MIMO, anteriormente usada.

dispensáveis. Estas duas tecnologias unidas, são consideradas primordiais para a habilitação do 5G com seus rigorosos requisitos de qualidade de serviço.

e) 5G *New Radio* (5G NR)

A tecnologia 5G NR significa uma nova interface de acesso a rádio padronizada mundialmente e utilizada nas redes móveis, baseadas no princípio de design "*ultra-lean*". Para entender esse design, é necessário compreender como funcionam as redes móveis sem ele. Normalmente as redes transmitem sinais mesmo quando não há dados a serem transmitidos, como sinais de sincronização, informações de transmissão do sistema, sinais de referência, etc. A proposta do sinal *ultra-lean* é diminuir tanto quanto possível essas transmissões, fazendo-as somente quando preciso. Tal implementação permitirá a redução da interferência de sinal em caso de tráfego alto, além de melhorar a eficiência energética da rede, diminuindo despesas operacionais (ZAIDI, 2017).

O NR foi desenvolvido para ter flexibilidade, no intuito de atender a uma vasta faixa de frequências (< 1 GHz a 100 GHz) utilizadas em distintas implementações como nos variados casos de uso já apresentados (eMBB, mMTC e URLLC), cujos requisitos são diferenciados e rigorosos. A tecnologia vislumbrou, também, a possibilidade de compatibilidade futura com novos serviços 5G ainda não previstos, permitindo o escalonamento da rede por aproximadamente quinze anos, não afetando a atual rede e permitindo melhorias de desempenho futuras (MECHAILEH, 2020).

f) Uso expandido de espectro

Dentre os serviços utilizados nos diversos cenários de uso apresentados, alguns necessitam prioritariamente de baixa latência, outros de velocidades ultrarrápidas e outros de maior conectividade. Para que todos esses requisitos sejam cumpridos, é necessário o uso de diferentes espectros de rede para atendê-los. Para isto, o 5G necessita utilizar uma larga faixa de frequências, que contemplam faixas mais baixas chamadas de Sub-6 e faixas mais altas, denominadas *millimeter Wave* (*mmWave*). E tal feito só é possível em virtude da implementação do 5G NR que gera essa flexibilidade (FIG07 – ANEXO).

O Sub-6 compreende as faixas de frequência abaixo de 6GHz. Elas são divididas em bandas de baixa frequência, que utilizam o espectro abaixo de 1GHz, e as bandas de média frequência que operam no espectro de 3,4GHz a 6GHz (CLOVER, 2021). A vantagem das frequências Sub-6 é que algumas já estão em uso demandando pouca infraestrutura para se adequar ao 5G, representando a solução mais rápida a curto prazo, para sua implantação, tendo em vista a possibilidade de compartilhamento de parte destas bandas com os atuais 2G, 3G e 4G.

Cabe salientar que a tecnologia 5G que compartilha o espectro com tecnologias anteriores é conhecida como 5G *Dynamic Spectrum Sharing* (DSS), que apesar de tratar-se do 5G, não entrega toda sua potencialidade, ficando bem longe das propostas inovadoras do 5G "tradicional". A vantagem está exatamente no reaproveitamento da infraestrutura já existente, trazendo economia e possibilitando a expansão do 5G onde sua instalação do zero torna-se economicamente inexequível, como em locais distantes e com poucos recursos. No entanto, apesar de muitas vezes ser confundido com o 4G LTE *Advanced* sugerindo um marketing comercial, trata-se sim, do 5G, em função de utilizar a tecnologia 5G NR (BRAGA, 2020). Esse compartilhamento é previsto ocorrer até a plena substituição das antigas tecnologias.

Neste caso, como o Sub-6 utiliza frequências mais baixas, o alcance do sinal é maior, permitindo uma melhor cobertura de rede, em função do sinal alcançar grandes áreas, aumentando a conectividade. E, devido o comprimento de onda utilizado ser mais longo, há uma maior capacidade de penetração em obstáculos. Apesar desta última funcionalidade, o seu uso está previsto para grandes áreas menos populosas e mais remotas, visto seu alcance.

A *mmWave* operam nas faixas de frequência mais altas, a partir de 24 GHz a 40GHz, podendo utilizar faixas maiores no futuro, atendendo de maneira mais eficaz a serviços que demandem alta velocidade, baixa latência e maior tráfego de dados, diminuindo o congestionamento das redes. Porém, o uso de ondas de comprimentos mais curtos, apesar de melhorar exponencialmente a velocidade de transmissão, têm menor penetração e alcance do sinal, necessitando de um número maior de células, com tipos específicos de antenas, aumentando o custo de implementação. Além disso, são facilmente bloqueadas por obstáculos tais como paredes, janelas, árvores, morros e também pelo próprio corpo humano.

O *mmWave* se tornou possível, dentre outros, em função do grande avanço tecnológico do *Massive* MIMO, devido à formação adaptável dos feixes e a miniaturização de difíceis funções de processamento das antenas (CLOVER, 2021). O uso do *beamforming* também será de extrema importância para minimizar a perda de sinal, já que sua tecnologia permite a melhor escolha do caminho para evitar obstáculos que degradam este tipo de onda (HIGA, 2019).

As ondas milimétricas, devido ao custo elevado de instalação, estão previstas para serem usadas em locais densamente povoados, como centros urbanos, onde as quantidades de células para conexão podem ser espalhadas em um ambiente mais restrito, fazendo com que o alcance de sinal seja adequado e a conectividade e velocidade atendam plenamente ao público-alvo.

Deste modo, cada espectro possui vantagens únicas que permite um equilíbrio para superar as limitações apresentadas em cada um deles, gerando oportunidades para melhorar o desempenho dos diversos serviços possibilitados ou aprimorados com a implementação do 5G. As disponibilidades das faixas de espectro, no entanto, são variáveis de país para país.

3.2.3 Eficiência energética

Um dos requisitos que o 5G precisa atender é o de eficiência energética, considerando que permitirá um gigantesco número de aparelhos conectados ao mesmo tempo, principalmente com o impulsionamento da IoT. A previsão é que a nova rede aumente mil vezes o tráfego em um período de aproximadamente dez anos exigindo soluções que atendam a demanda e equilibrem o consumo sem degradar a eficiência. De acordo com Noohani e Magsi (2020), o 5G possui algumas características que preveem eficiência energética, conforme alguns parâmetros já expostos e outros comentados a seguir.

Uma das técnicas utilizadas para minimizar o *boom* energético é a implementação de um "*sleep mode*" aprimorado nas estações base de rádio, desativando alguns dispositivos quando o volume de tráfego estiver baixo, fazendo com que entrem no modo de hibernação, permanecendo desta forma o máximo possível. A técnica permite um rápido retorno à atividade quando detectada a necessidade de envio de rajadas de dados.

Outra característica já comentada neste trabalho que contribui com a eficiência energética, é o fato do 5G possuir altas taxas de transferência de dados e baixa latência. Com isso, os dados são transmitidos em menor tempo, permitindo que o link entre a estação base e o consumidor fique ocioso por um intervalo superior, possibilitando um maior período de hibernação.

A tecnologia MIMO Massivo é outra coadjuvante que colabora com essa economia. Em função da tecnologia utilizar um grande número de antenas concentradas para atender a um número de usuários no mesmo recurso de tempo/frequência, há uma concentração da potência, fazendo com que a transmissão da mesma seja significativamente pequena, reduzindo interferências e consequentemente melhorando o desempenho da eficiência energética (BHARDWAJ, 2020). Da mesma forma, as *Small Cells* pelo fato de serem de pequeno porte e possuírem estações base portáteis, demandam pouca energia.

Outra estratégia utilizada que permite o uso eficiente de energia é a conectividade Dispositivo a Dispositivo (D2D). Atualmente os dispositivos não podem se comunicar entre si, necessitando de equipamentos intermediários que são as estações base. Com a

implementação do D2D, tem-se o conceito de comunicação cooperativa onde os nós formam uma grande rede para fazer retransmissões entre dispositivos próximos sem ou com pouca intervenção das estações base.

Tal modelo de comunicação reduz os congestionamentos de rede, em função da possibilidade de comunicação direta entre dispositivos, fazendo um uso mais eficiente dos diversos equipamentos envolvidos no processo de transmissão de dados. Ademais, a potência de transmissão para comunicação entre dispositivos adjacentes é consideravelmente menor, equiparada à consumida por uma estação base (GOMES, 2018).

Estas são apenas algumas características e soluções que influenciarão na necessária proficiência energética para a implementação do 5G, dentre tantas outras previstas. Uma proposta bastante incentivada para diminuição do consumo de energia é o uso de fontes alternativas autossuficientes pelas operadoras de telecomunicações para gerar a energia demandada pelos equipamentos do 5G (JULIÃO, 2020), já que o vultoso aumento no consumo de energia traria impactos negativos ao meio ambiente.

Esta eficiência, entretanto, ocorrerá de forma gradual, visto que atualmente o consumo dos aparelhos que já utilizam o 5G é bem maior que os que usufruem do 4G. À medida que a infraestrutura adequada ao 5G for sendo implementada, a eficiência energética atingirá o patamar previsto em sua arquitetura. A proposta é que o 5G diminua em até 90% o consumo de energia da rede e aumente em até 10 anos a vida útil das baterias (MUÑOZ, 2017).

Com essa e as demais características aqui apresentadas, é possível verificar que o 5G é uma tecnologia que impulsionará aplicações já existentes, trazendo novas oportunidades de implementação que mudarão o cotidiano e a maneira com que dispositivos e pessoas se conectam. Por conseguinte, o setor de Defesa tem feito previsões de uso que trarão vantagens em suas aplicações militares, promovendo avanços que não poderiam se concretizar sem os recursos advindos da nova tecnologia, conforme demostrado a seguir.

4 A GUERRA DA TECNOLOGIA E A TECNOLOGIA DE GUERRA

De acordo com as explanações apresentadas, o 5G tem sido projetado para atender, dentre outras, aplicações onde a disponibilidade e a confiabilidade se tornam fatores imprescindíveis. Em uma Guerra Cinética, por exemplo, o tempo de resposta a um ataque faz toda a diferença para incapacitar o oponente no momento oportuno. A falha de um

armamento, um disparo não realizado, uma armadilha que não funciona e um soldado inabilidoso podem comprometer uma missão, gerando resultados destrutivos para uma nação.

Desta forma, em uma Guerra Cibernética, as armas utilizadas também devem favorecer o tempo de resposta, permitindo ações acertadas, minimizando possibilidades de falhas e no tempo esperado. Para isto, o emprego de novas tecnologias que possam fazer a diferença é de fundamental importância, devendo ser aplicadas em favor dos resultados pretendidos. É neste contexto que podemos verificar a inserção do 5G para expandir as potencialidades militares, seja na área de comunicação ou em outros empregos onde possam gerar facilidades, obtendo melhores resultados.

Uma vez que o domínio cibernético, como espaço de guerra, permeia todos os outros domínios operacionais (BRASIL, 2014), tem-se a constante relação entre esses domínios, projetando um futuro onde a maior parte das Guerras Cinéticas serão, de alguma forma, providas com recursos que utilizem o meio cibernético, afetando diretamente este ambiente, como poderá ser constatado com as aplicações militares apresentadas nos próximos tópicos.

4.1 O 5G em aplicações militares

O 5G tem sido projetado de diversas formas para prover melhores resultados, aumentar capacidades e gerar facilidades ainda não implementadas no setor militar, permitindo uma melhor análise do campo de batalha, com informações que favorecem a tomada de decisões. A informação tornou-se, então, uma arma de guerra e a velocidade com que uma informação é compartilhada, faz toda diferença.

Desta forma, a junção do 5G com outras tecnologias como a IA, *Big Data*, Computação em nuvem e a Internet das Coisas Militares (IoMT – *Internet of Military Things*) alavancará as ações dos comandos operacionais, com o compartilhamento em tempo real de informações de inteligência e análise situacional dos campos de batalha, permitindo operações em um nível mais avançado. Dentre estas, destaca-se a IoMT, visto que a maioria dos cenários aplicáveis na área da defesa engloba, necessariamente, uma hiperconectividade entre dispositivos e equipamentos, funcionando como um facilitador dos processos, como mostrado a seguir.

4.1.1 Internet das Coisas Militares

A IoT é uma tecnologia que prevê a interconexão, via internet, de dispositivos e equipamentos utilizados no cotidiano, no intuito de transmitir dados entre si, possibilitando

uma cooperação e troca de informações úteis entre estes. Como exemplo, pode-se citar câmeras de segurança controladas por *smartphone*, eletrodomésticos e rede elétrica sendo controlados a distância por meio de sensores e carros autônomos que poderão enviar e receber informações relevantes ao seu funcionamento por meio de um tablet.

Neste contexto, a IoMT ou Internet das Coisas no Campo de Batalha (IoBT – *Internet of Battlefield Things*) [10] engloba a conexão de equipamentos afetos ao domínio militar. Esta utilização é possível muito em prol da implementação do cenário de uso mMTC, aqui descrito, que permite a hiperconectividade entre vários dispositivos ao mesmo tempo, facilitando e agilizando a coordenação das informações. Com isso, os diversos órgãos de Defesa têm feito algumas previsões de uso do IoMT baseado no 5G, para aplicações militares, como a interconexão de drones, câmeras, equipamentos médicos e demais dispositivos, conforme mencionadas a seguir.

a) Comunicações

Uma das áreas mais evidentes em que as melhorias do 5G seriam aplicadas é a das comunicações militares, tornando mais eficaz o compartilhamento de informações nos campos de batalha. Atualmente, a incursão em matas e ambientes ermos não permitem um acompanhamento efetivo das tropas, necessitando, muitas vezes, de equipamentos pesados que influenciam na locomoção.

Com o uso do amplo espectro de frequências e a disponibilidade de faixas baixas e altas, é possível fazer uma adequação entre elas, a fim de atender a cobertura de sinal em locais extensos e despovoados, bem como em ambientes menores e densamente habitados, garantindo a comunicação em locais antes não alcançados.

Ademais, a facilidade de comunicação D2D permitida no 5G, onde há a comunicação direta entre dispositivos sem a obrigatoriedade de usar frequentemente satélites de comunicações militares ou aeronaves retransmissoras de comunicações, faz com que o custo das operações reduza drasticamente (QINGLIANG; GUONING, 2019).

Esse tipo de conexão dispositivo a dispositivo permite, ainda, a continuidade da transmissão no caso de desastres ou destruição proposital de antenas e estações base, quando o estabelecimento urgente de uma comunicação é possível (GOMES, 2018).

A comunicação com a IoMT não se restringe a rádios transmissores ou celulares, podendo ser expandida com o uso de quaisquer outros dispositivos como *smartwatches*, drones e demais equipamentos passíveis de serem conectados na rede móvel a fim de transmitir e receber informações.

10 Os termos IoMT e IoBT possuem o mesmo significado, utilizando-se ambos para representar a Internet das Coisas no meio militar.

Além disso, a transmissão de dados se torna mais rápida e a economia de bateria mais eficiente, sobretudo em locais isolados onde é mais difícil recarregar as baterias de equipamentos, como é o caso dos campos de batalha, favorecendo a mobilidade, visto ser um dos aspectos mais importantes para ganhar vantagem tática.

b) Monitoramento médico e cirurgias remotas

A necessidade de socorro médico nos campos de batalha é algo premente que muitas vezes em função do ambiente hostil e, em alguns casos, de difícil acesso, dificulta remoções imediatas, fazendo com que os combatentes se vejam isolados e dependentes de recursos limitados, tendo como principal consequência a perda de vidas, em função da demora no atendimento.

Em decorrência da implementação do cenário de uso URLLC no 5G, onde conexões ultraconfiáveis são permitidas, será possível realizar o tratamento médico sem grandes deslocamentos do combatente. Haverá a viabilidade de conexão entre médicos e plataformas de cirurgia robótica, interligando diversos equipamentos, dando o suporte necessário para a realização de atendimentos e cirurgias remotas, aumentando as chances de sobrevivência (QINGLIANG e GUONING, 2019).

O monitoramento de pessoal operativo pode ser realizado, por exemplo, por sensores acoplados a roupa dos soldados (PROLIM, 2021) ou por um *smartwacth* que compartilharia em tempo real informações dos combatentes tais como localização geográfica, sinais vitais como frequência cardíaca, pressão arterial, sinais de fadiga (GAMBUZZI, 2019), tempo em atividade de combate, etc, contribuindo para um controle mais efetivo da tropa.

Com o rastreamento e envio de alertas sobre as condições de saúde dos soldados, uma equipe médica poderá ter acesso antecipado à gravidade da lesão, e, se for o caso, providenciar de forma rápida os recursos médicos necessários para o atendimento, aumentando as chances de sobrevivência (PROLIM, 2021).

c) Operações Logísticas

Os setores de logística terão um grande ganho no controle e distribuição de suprimentos e demais materiais necessários para dar suporte a uma tropa em conflito e também para as devidas supervisões em tempo de paz. Como exemplo, tem-se o 5G, acompanhado da IA e da ajuda de diversos sensores, permitindo uma maior flexibilidade no monitoramento, por exemplo, de frotas de veículos não tripulados (QINGLIANG; GUONING, 2019).

A gestão eficiente de estoques pode ser realizada com o auxílio de rastreadores *Radio Frequency Identification* (RFID) que permitirão o controle do estoque e da cadeia de

suprimentos em tempo real, facilitando a provisão das necessidades de recompletamento e o controle de produtos em excesso (SAHU, 2021), minimizando perdas e contribuindo para uma rápida auditoria.

Na Califórnia, a base naval de San Diego vem realizando testes de aplicações em 5G para operações de logística naval envolvendo o transbordo de armazéns inteligentes, concentrando as movimentações de materiais entre instalações costeiras/navios e vice-versa, melhorando a eficiência das operações logísticas, tais como identificação, registro, organização, armazenamento, recuperação, além de transporte de material e suprimentos (KELLER, 2020).

Como exemplo de outro modelo aplicável, tem-se, em bases navais, a possibilidade de utilização do 5G para auxiliar operadores remotos de guindaste e pórticos, fornecendo um retorno tátil e de vídeo para o acompanhamento da carga e descarga de navios. Neste modelo, será possível verificar a localização precisa de veículos e ativos, favorecendo o rastreamento das operações logísticas. Deste modo, os navios poderão baixar os dados antes mesmo de sua atracação, por meio da conectividade 5G navio-terra (VERRANT, 2021).

d) Gerenciamento de frotas de veículos

A diversidade de veículos utilizados no meio militar bem como sua grande quantidade tornam a gerência difícil e a manutenção dispendiosa. A adoção do 5G aliado a IoMT facilitará o monitoramento em tempo real com auxílios de sensores e GPS, que disponibilizarão o status do veículo como sua localização, velocidade, condições do motor, situação do combustível dentre outros, minimizando custos operacionais (SAHU, 2021).

A integração dessas informações permitirão a identificação de falhas e/ou necessidades de manutenções, além de permitir a avaliação do desempenho do motorista, gerando uma economia em torno de 25% de combustível, em relação aos valores normalmente despendidos (PROLIM, 2021). A redução de gastos em função da manutenção preventiva também é um fator positivo neste emprego.

Em Albany, na Geórgia, a Base Logística do Corpo de Fuzileiros Navais coordena um projeto de controle inteligente de armazenamento de frotas de veículos. Similarmente ao exemplo citado acima, o projeto prevê a criação de armazéns inteligentes voltados para a gerência e manutenção de veículos (KELLER, 2020).

e) Armamento

Cenários considerados de ficção científica, em pouco tempo se tornarão realidade. Países como China, Rússia, Estados Unidos e França têm trabalhado no

desenvolvimento de armas hipersônicas capazes de viajar a uma velocidade Mach 5, igual ou superior a cinco vezes a velocidade do som, o que corresponde a aproximadamente 1,6 km/s (GAMBUZZI, 2019). A Rússia realizou um teste com sucesso em julho de 2021, com o míssil hipersônico Zircon, que atingiu um alvo a 350 km de distância, viajando à velocidade Mach 7, que corresponde a sete vezes ou mais a velocidade do som (RAJAGOPALAN, 2021).

Este tipo de armamento possui velocidade extrema, capacidade de manobrar obstáculos fixos de defesa, além de operar em altitudes variadas, inclusive voando próximo à superfície e, portanto, fora da cobertura do radar (RIGUES, 2019). Tais capacidades fazem com que se torne cada vez mais difícil a detecção por parte dos atuais sistemas antimíssil.

Desta forma, estes sistemas necessitarão, além da inteligência convencional, de recursos com alto poder de processamento em tempo real, que transmitam dados de interesse para tornar possível a rápida defesa, que terá o tempo de aproximadamente um minuto para reagir (GAMBUZZI, 2019). É neste panorama que o 5G se aplica, proporcionando as altíssimas velocidades de resposta, integrando vários sistemas e redes que darão a oportunidade de acionar as medidas de contra-ataque ou defesa em tempo hábil.

Vários tipos de sistemas automatizados de armas conseguirão alcançar ciclos de controle no nível de milissegundos, com a utilização de diversas soluções inteligentes como medições por sensor, transmissão rápida de dados dentre outros (QINGLIANG; GUONING, 2019).

f) Comando e Controle (C^2)

Os centros de C^2 terão um ganho imensurável na coleta, processamento e transmissão de informações, permitindo a análise da situação no campo de batalha em tempo real. A velocidade com que as informações chegarão ao C^2 levarão a uma percepção acurada dos decisores, influenciando nos resultados das operações militares.

O uso de plataformas inteligentes de C^2 possibilitarão o reconhecimento, a identificação, o rastreamento e a emissão de alertas antecipados em tempo real, para uso contra alvos do adversário. Com essas facilidades, o comando poderá tomar decisões unindo informações de outras fontes com as obtidas em tempo real, alcançando uma perspectiva mais ampla do ambiente operacional (QINGLIANG; GUONING, 2019).

A velocidade alta, com baixíssima latência, além do grande número de dispositivos conectados simultaneamente, viabilizará o compartilhamento de mapas, vídeos e fotos de cenários do campo de batalha (GAMBUZZI, 2019). A transmissão ao vivo com câmeras acopladas ao corpo dos soldados também são recursos possíveis.

A Base Aérea de Nellis, localizada no estado americano de Nevada, possui um projeto em curso, para implantação de um Comando e Controle aéreo com uso do 5G, cujo objetivo é atualizar a arquitetura deste comando para situações de combate (SCORSIM, 2020), onde serão testadas as facilidades de recursos possíveis de serem implementadas em um C^2.

g) Treinamento militar com realidade aumentada e virtual

A Realidade Aumentada (RA) e Realidade Virtual (RV) permitirão o desenvolvimento de novas capacidades militares quando usadas em jogos de guerra, simulações e exercícios militares, tanto em ambientes internos quanto externos. Especialistas militares têm trabalhado em redes 5G resilientes e seguras para usufruir das melhores capacidades que estas aplicações podem oferecer.

A RA, quando usada no campo de batalha, permitirá informações em tempo real dos principais edifícios da área de operação, das condições do terreno e da situação geral dos combatentes (FIG08 – ANEXO), tanto de forças amigas, quanto inimigas, trazendo uma percepção ampliada e fidedigna que apoiará os decisores (EUN-JIN, 2019). Um combatente dentro de uma aeronave usando um óculos de realidade aumentada poderá controlar drones lançados a partir desta, tendo uma visão vantajosa do ambiente operacional, como se estivesse num jogo, porém vivenciando a realidade com um drone de verdade (KELLER, 2020).

Já a RV permitirá, por exemplo, o treinamento de situações em condições adversas, como em mau tempo e à noite, utilizando vários tipos de armas e projéteis, conforme a necessidade. Um simulador de vôo permitirá o treino de manobras arriscadas preparando pilotos de forma segura para situações reais (SAHU, 2021). Neste seguimento, a Academia Militar da Coreia do Sul está desenvolvendo um simulador de treinamento de C^2 com RA e outro de precisão de tiro baseado em RV, cujo objetivo é aumentar as capacidades de combate individuais e em tropa (EUN-JIN, 2019).

Já o Departamento de Defesa (DoD) dos EUA anunciou investimentos em redes 5G em bases militares, onde prevê o uso desses recursos. A base Lewis-McChord em Washington foi contemplada com este tipo de aplicação, podendo prover treinamentos de forma mais realística, além do suporte a novas técnicas essenciais para a preparação de soldados em futuros conflitos de alto nível (SCORSIM, 2020).

h) Varredura de Minas Terrestres

Outra previsão possível de ser implementada com o 5G é a varredura de minas terrestres. Tal tarefa constitui missão arriscada quando efetuada pela tropa, estabelecendo

desafios, mesmo para pessoal com treinamento específico, tendo em vista essas minas serem sensíveis a estímulos externos.

O 5G permitirá o manuseio remoto de uma escavadeira não tripulada para operações de remoção deste tipo de mina. O procedimento é possível devido a utilização de vídeos de alta resolução em tempo real apoiando o operador que estará isento de riscos. O Ministério de Defesa Nacional da Coreia do Sul planejou um projeto com este tipo de implementação, utilizando a tecnologia para remoção de minas terrestres ainda não identificadas próximas a áreas com demarcações militares (EUN-JIN, 2019).

i) Monitoramento em tempo real

Uma das áreas com crescimento mais promissor e cujos benefícios do 5G serão amplamente aproveitados é o de sistemas de Inteligência, Vigilância e Reconhecimento (ISR – *Intelligence, Surveillance and Reconnaissance*). Com a diminuição do tempo de retardo, as respostas virão em tempo real e com informações mais aprimoradas, visto a alta qualidade de vídeos e rapidez no poder de reconhecimento, por exemplo.

No que diz respeito ao monitoramento de áreas e instalações, o uso da tecnologia de ondas milimétricas, cuja velocidade supera 1Gbps, traz um cenário perfeito para a criação de um monitoramento altamente integrado e em tempo real dos perímetros militares. Câmeras utilizando as velozes ondas milimétricas, assim como dispositivos com sensores de movimento poderão ter suas imagens/informações compartilhadas, permitindo uma rápida comunicação entre centros de comando, veículos e demais envolvidos, melhorando a proteção dos perímetros, favorecendo uma ação rápida em caso de alterações detectadas (GAMBUZZI, 2019).

Um aspecto que inicialmente poderia se tornar um problema, é o fato das ondas milimétricas terem maior atenuação do sinal em caso de obstáculos como, por exemplo, muros e arbustos. Mas neste emprego, acaba por tornar-se um motivo de força, tendo em vista que evita a difusão indevida do sinal, impedindo que agentes não autorizados façam uma interceptação para obtenções de imagens/informações ou para ataque cibernético.

j) Veículos Aéreos Não Tripulados (VANTS)

Os VANTS já são amplamente utilizados pelas Forças Armadas dos diversos países e demais áreas de Defesa. No entanto, suas capacidades serão potencializadas com o uso do 5G, visto que a precisão desses veículos dependem de tempos de resposta mais curtos. Ademais, essa precisão permitirá que esses veículos sejam manobrados com maior segurança, tendo em vista muitas vezes operarem em um espaço aéreo congestionado, com aeronaves e helicópteros comerciais, possibilitando colisões (KELLER, 2020).

Atualmente, os VANTS não têm a capacidade de compartilhar com suas bases imagens 4K em tempo real, o que poderá ocorrer quando da implementação das redes móveis de quinta geração. Com a possibilidade de um processamento mais veloz aliado ao uso da IA, as missões de reconhecimento se tornarão mais eficazes, pois será viável transmitir informações do ambiente operacional, acelerando os processos de tomada de decisão (GAMBUZZI, 2019).

Deste modo, será possível obter uma consciência mais apurada do campo de batalha, com a utilização de câmeras acopladas a drones com capacidade de mapear a estrutura do terreno e as posições dos adversários em um modelo 3D, transmitindo essas informações para o C^2 (FIG09 – ANEXO). Os drones poderão, também, realizar patrulhas autônomas de fronteiras, alertando para o caso de possíveis ameaças, eliminando riscos desnecessários ao pessoal empregado na atividade (SAHU, 2021), que em caso de necessidade de deslocamento, já terão conhecimento dos riscos a serem enfrentados.

Com a ajuda de algorítimos de IA, será possível, por meio das imagens captadas por drones, realizar com precisão a detecção de possíveis alvos, por meio de sistemas de reconhecimento (FIG10 – ANEXO). Com os recursos de aprendizado de máquina que essa tecnologia dispõe, será possível, também, realizar projeções do comportamento adversário, antecipando vulnerabilidades. Este tipo de reconhecimento contribui, ainda, para os casos de busca e salvamento ou quando houver reféns envolvidos (SAHU,2021).

Como exemplo, tem-se um projeto idealizado pelo Pentágono nos EUA, conhecido como “Projeto Maven”, que faz uso de IA para classificar massas de dados de inteligência, vigilância e reconhecimento geradas por filmagens de VANTS, propiciando a detecção de objetos e demais detalhes que demoram a saltar aos olhos dos analistas, fazendo com que se tornem mais fáceis e rápidos de serem distinguidos (ATHERTON, 2018).

Desta forma, e diante de uma gama de cenários de aplicações militares possíveis de serem implementadas com o 5G, utilizando o espaço cibernético para tal, haverá, inevitavelmente, uma influência direta nas ações de Guerra Cibernética, conforme discorrido a seguir.

4.2 Influência do 5G na Guerra Cibernética

É indubitável os benefícios e facilidades que o 5G trará para o campo de Defesa, introduzindo novos recursos e aumentando o desempenho das capacidades militares. Desta forma, o ambiente cibernético que é o campo de batalha da Guerra Cibernética, se

tornará um dos principais protagonistas para a implementação de recursos de guerra em suas diversas facetas.

O primeiro e mais rápido processo de mudança que poderá ser verificado na Guerra Cibernética será a ampliação das possibilidades de ataque, visto os inúmeros equipamentos e dispositivos que terão interface no ambiente cibernético. Com o aumento desses dispositivos, aumenta-se também a superfície de ataque, fornecendo ao oponente mais oportunidades para realizar investidas.

Outro fator a ser considerado, é a dependência tecnológica que as novas aplicações trarão, favorecendo as ações de Guerra Cibernética. Uma vez implementadas as facilidades aqui descritas, as novas gerações de soldados serão treinadas e aplicarão os conhecimentos no campo de batalha que se tornará altamente tecnológico podendo causar uma forte dependência destes recursos, não sabendo como proceder, caso um ataque cibernético paralise os meios disponíveis.

A falta de vigilância do oponente no meio cibernético é mais um aspecto proeminente que poderá se tornar um trunfo para a obtenção de informações estratégicas e táticas a serem utilizadas pelo inimigo. Uma vez de posse de credenciais de sistemas do adversário, o país atacante pode se inserir nestes a fim de acompanhar as decisões, verificar imagens de câmeras em tempo real, além dos dispositivos e equipamentos que serão utilizados em campo pelo seu opositor, tendo em vista a interconexão massiva dos recursos, obtendo vantagens. Neste caso, o ataque estaria exatamente no desconhecimento do inimigo sendo espionado.

Em outro contexto, tem-se, ainda, o fato da Guerra Cibernética não possuir uma lei internacional explícita que a limite, estando sujeita às leis existentes, como sugerido no Manual de Tallin[11]. No entanto, sua aplicação ocorre em situações onde as ações cibernéticas resultem no "uso da força" com resultados no mundo cinético. Caso as ações cibernéticas se limitem a danos no espaço cibernético inimigo, não há garantias de como os executores serão punidos, tanto pela dificuldade de descoberta da autoria dos atos, quanto por lacunas nas leis internacionais atuais criadas para os domínios de guerra até então existentes, necessitando de interpretações legais caso a caso.

Fator não menos importante é a situação geopolítica do 5G nos diversos países. Muitas discussões têm sido criadas em torno da implementação desta tecnologia e sua relação com a soberania das nações, visto que a escolha dos fabricantes dos equipamentos que

11O "Manual de Tallin" é um documento acadêmico que aborda a interpretação do Direito Internacional aplicado à Guerra Cibernética. Apesar de não se tratar de um documento oficial, é considerado um norteador para a solução de conflitos cibernéticos.

comporão a infraestrutura de rede, poderá interferir na segurança das redes e de tecnologias associadas, podendo favorecer atos de espionagem e/ou sabotagem, afetando diretamente a autonomia e potencialidade de ataque e defesa dos países no caso de um Guerra Cibernética.

Inevitavelmente os países operarão redes 5G de inteligência militar e/ou de governo, onde informações sensíveis e sigilosas tramitam, gerando preocupações. Um único país detentor da tecnologia se tornando um fornecedor mundial, poderá ter acesso privilegiado aos equipamentos de rede, usurpando dos poderes de algumas nações de interesse, obtendo vantagens no espaço cibernético. Desta forma, a imposição de regras rígidas e limitações que restrinjam a ação da inteligência do oponente nas contratações torna-se um ato imprescindível para os decisores.

Neste contexto desafiador, é sabido que as operações de guerra normalmente são executadas em ambiente hostil, não sendo diferente quando se trata do ambiente cibernético. No entanto, com a ampliação inevitável do emprego de equipamentos militares neste ambiente em virtude da implementação do 5G, sejam eles de caráter logístico ou no campo de batalha, haverá a necessidade da previsão de meios adicionais de defesa no intuito de garantir as capacidades de Guerra Cibernética das inúmeras nações.

5 CONCLUSÃO

Diante do exposto neste trabalho, é possível evidenciar que a Guerra Cibernética tem se tornado um meio proeminente de atingir sistemas, infraestruturas críticas e demais setores considerados vitais para uma nação inimiga. Um dos fatores para o seu crescimento tem sido ocasionado pela maior possibilidade de preservação de vidas humanas, além das novas tecnologias que vêm favorecendo o seu desempenho.

Deste modo, conforme discorrido, o 5G tem a capacidade de aumentar as potencialidades deste tipo de guerra tanto no que concerne à rápida fluidez com que informações de inteligência, reconhecimento, condições médicas, dentre outras são passadas, quanto pelo grande número de aplicações que permitirão avaliações mais precisas e decisões estratégicas com embasamentos mais fidedignos do campo de batalha.

As novas aplicações militares advindas com a tecnologia 5G representam, sem dúvida, uma oportunidade para potencializar recursos e dispositivos utilizados em guerra, sejam eles empregados na Guerra Cinética (mediante o apoio do meio cibernético), ou na própria Guerra Cibernética em si, aumentando o poder de ataque.

Desta forma, muitos países já fazem previsões do 5G na Guerra do Futuro, evidenciando suas intenções em bases e campos de batalha inteligentes, trazendo uma nova realidade que permitirá mudanças significativas na maneira com que a logística, os treinamentos e os novos dispositivos serão usados.

Com os conhecimentos aqui abordados a respeito da Guerra Cibernética, das funcionalidades do 5G e suas projeções de uso na área de Defesa, torna-se possível concluir que as novas aplicações influenciarão diretamente o *modus operandi* da Guerra Cibernética, tendo em vista que quanto maior a dependência de um país em relação à tecnologia, maior será a possibilidade de atingi-lo de forma eficiente com artefatos cibernéticos.

Ademais, o aumento da superfície de ataque, com as diversas aplicações previstas e em teste, trarão novas oportunidades e empregos da Guerra Cibernética, visto a possibilidade de acesso privilegiado a dispositivos e recursos militares antes não alcançados no mundo cibernético.

Com isso, em virtude do aumento de dispositivos e aplicações interfaceando o espaço cibernético, questões relativas aos investimentos e medidas necessárias na área de defesa cibernética de cada país tornam-se relevantes, não tendo sido, no entanto, o foco do presente trabalho, tornando-se uma oportunidade de complemento deste.

Desta forma, depreende-se que a Guerra cibernética ao mesmo tempo em que aumentará o potencial de combate de uma nação sem o uso de armamentos letais, poderá paralisar toda tropa, caso seus principais recursos de guerra se tornem inoperantes e/ou sejam programados para uso contra a própria tropa que os opera, em caso de ataque coordenado.

Não há, todavia, uma solução para tal impasse. O não investimento para o uso de novas tecnologias inviabilizará o progresso e a otimizações dos recursos de guerra e o seu emprego em excesso poderá tornar o teatro de operações vulnerável aos crescentes ataques e investidas do oponente. Nesta conjuntura, os decisores precisam ter em mente que o uso equilibrado da tecnologia na guerra, é o que trará os resultados mais promissores. Entretanto, as decisões caberão a cada nação, de forma a fazer o uso coerente dos diversos recursos disponíveis.

REFERÊNCIAS

5G AMERICAS. **5G Services & Use Cases**. 5G Americas, 2017. Disponível em: <https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Service_and_Use_Cases__FINAL.pdf>. Acesso em: 20 ago. 2021.

ANATEL. **Tecnologia 5G**. Agência Nacional de Telecomunicações (ANATEL), 2021. Disponível em:< https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g >. Acesso em: 08 jun. 2021.

BRASIL. Ministério da Defesa. **MD31-M-07**: Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf>. Acesso em: 17 abr. 2021.

BASTOS, Luis; CAPELA, Germano; KOPRULU, Alper. **Potential of 5G technologies for military application**. NCI AGENCY, 2020. Disponível em: <http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf>. Acesso em: 18 abr. 2021.

BHARDWAJ, Anshu. **5G for Military Communications**. Science Direct, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050920312825>. Acesso em: 26 jul. 2021.

BRAGA, Lucas. **4G/LTE:** saiba como o 4G funciona. Tecnoblog, 2018. Disponível em: <https://tecnoblog.net/88088/lte-4g-como-funciona/>. Acesso em: 04 jul. 2021.

BRAGA, Lucas. **Afinal, o 5G DSS que temos no Brasil é "5G de verdade"?**. Tecnoblog, 2020. Disponível em: < https://tecnoblog.net/378028/afinal-o-5g-dss-que-temos-no-brasil-e-5g-de-verdade/ >. Acesso em: 17 jul. 2021.

CLARKE, Richard A.; KNAKE Robert K. **Guerra Cibernética:** A Próxima Ameaça à Segurança e o que Fazer a Respeito. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, C. von. Vom Krieg. **Hinterlassenes Werk des Generals**. Berlim: Richard Wilhelmi, 1883.

CLOVER, Juli. **mmWave vs. iPhones 5G sub-6GHz:** Qual é a diferença?. MacRumors, 2021. Disponível em: < https://www.macrumors.com/guide/mmwave-vs-sub-6ghz-5g/>. Acesso em: 16 jul. 2021.

COMPUGRAF. **Guerra Cibernética, Cibercrime e Ciberterrorismo:** Qual a diferença?. Compugraf, 2020. Disponível em: < https://www.compugraf.com.br/guerra-cibernetica-cibercrime-e-ciberterrorismo-qual-a-diferenca/ >. Acesso em: 05 jun. 2021.

COSSETTI, Melissa Cruz. **O que é Beamforming e como isso beneficia o seu Wi-Fi**. Tecnoblog, 2019. Disponível em:< https://tecnoblog.net/277152/o-que-e-beamforming/ >. Acesso em: 11 jul. 2021.

EUN-JIN, Kim. **Ultra-Fast 5G Services Upgrade Military Combat Capability**. Business Korea, 2019. Disponível em: <http://www.businesskorea.co.kr/news/articleView.html?idxno=31213>. Acesso em: 28 jul. 2021.

GAMBUZZI, Agnese. **5G:** Implications on the Battlefield. European Army Interoperability Centre, 2019. Disponível em: <https://finabel.org/5g-implications-on-the-battlefield/>. Acesso em: 27 jul. 2021.

GARRETT, Filipe; VELOSO,Thássius. **O que é e como funciona o 4G Plus (também chamado de 4,5G)**. Techtudo, 2017. Disponível em: <https://www.techtudo.com.br/noticias/2017/10/alem-da-quarta-geracao-entenda-como-funciona-a-internet-45g-em-celulares.ghtml>. Acesso em: 04 jul. 2021.

GOMES, Ana C. S. **Estudo sobre a Eficiência Energética em Redes 5G**. Universidade Federal de Campina Grande (UFCG), 2018. Disponível em: <http://dspace.sti.ufcg.edu.br:8080/xmlui/handle/riufcg/18830>. Acesso em: 26 jul. 2021.

HANNA, Katie T.; FERGUSON, Kevin; ROSENCRANCE, Linda. **Cyberwarefare**. Tech Target, 2021. Disponível em: <https://searchsecurity.techtarget.com/definition/cyberwarfare>. Acesso em: 29 jul. 2021.

HIGA, Paulo. **mmWave:** o que são as ondas milimétricas que fazem o 5G funcionar em frequências altas. Tecnoblog, 2019. Disponível em: < https://tecnoblog.net/270324/5g-nr-mmwave-altas-frequencias-ondas-milimetricas >. Acesso em: 16 jul. 2021.

INTRAWAY. **Small Cells Deployment:** The impact of no-code provisioning automation in small cells deployment. Intraway, 2019. Disponível em: < https://www.intraway.com/small-cells-deployment/?creative=524387932945&keyword=5g%20small%20cell%20architecture&matchtype=b&network=g&device=c&gclid=EAIaIQobChMIl5nXzojZ8QIVx4CRCh2oawDnEAAYASAAEgL2b_D_BwE >. Acesso em: 10 jul. 2021.

ITU. **Report ITU-R M.2320-0**, Future technology trends of terrestrial IMT systems. International Telecomunication Union (ITU), 2014. Disponível em:< https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2320-2014-PDF-E.pdf>. Acesso em: 08 jun. 2021.

ITU. **Setting the Scene for 5G:** Opportunities & Challenges. International Telecomunication Union (ITU), 2018. Disponível em: <https://www.itu.int/pub/D-PREF-BB.5G_01-2018>. Acesso em: 20 ago. 2021.

JODL, Markus. **Beamforming mit 5G:** Mobilfunk punktgenau. Blog Telekom, 2019. Disponível em: <https://www.telekom.com/de/blog/netz/artikel/beamforming-5g-mobilfunk-570522>. Acesso em: 20 ago. 2021.

JULIÃO, Henrique. **Consumo eficiente de energia será desafio ainda maior para operadoras no 5G**. Teletime, 2020. Disponível em: < https://teletime.com.br/23/07/2020/consumo-eficiente-de-energia-sera-desafio-ainda-maior-para-operadoras-no-5g >. Acesso em: 18 jul. 2021.

JUNIPER. **O que é 5G?**. Juniper, 2021. Disponível em: <https://www.juniper.net/br/pt/research-topics/what-is-5g.html >. Acesso em: 10 jul. 2021.

KANIA. Elsa B. **Securing Our 5G Future:** The Competitive Challenge and Considerations for U.S. Policy. Center for a New American Security (CNAS), 2019. Disponível em:<http://files.cnas.org.s3.amazonaws.com/documents/Kania-Securing-Our-5G-Future-2.pdf>. Acesso em: 26 jul. 2021.

KASHYAP, Hemant. **Why is There Such a Fuss over mmWave in India**. Voice & Data, 2021. Disponível em:<https://www.voicendata.com/fuss-mmwave-india-overrated/>. Acesso em: 20 ago. 2021.

KELLER, John. **What 5G means to the military**. Military e Aerospace Eletronics, 2020. Disponível em: <https://www.militaryaerospace.com/rf-analog/article/14188341/military-5g-communications>. Acesso em: 29 jul. 2021.

LOPES, Guilherme Cano; LOPES, Guilherme W. S. **Network Slicing**. Unicamp, 2019. Disponível em: < https://www.ic.unicamp.br/~edmundo/MC822/mc822/MO655/Semin%C3%A1rio%20-%20Network%20Slicing%20Guilhermes%20Lopes.pdf>. Acesso em: 09 jul. 2021.

MCTIC. **Estratégia Brasileira de Redes de Quinta Geração (5G):** Versão para Consulta Pública. Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), 2019. Disponível em: < https://www.abranet.org.br/media/MCTIC-5G-Abranet.pdf?UserActiveTemplate=site >. Acesso em: 06 jun. 2021.

MECHAILEH, Jose Antonio. **Redes 5G:** Tecnologia e Implantação. Eldorado, 2020. Disponível em: < https://www.eldorado.org.br/blog/redes-moveis-5g-tecnologia-implantacao/ >. Acesso em: 10 jul. 2021.

MUÑOZ, Ramón. **5G, a tecnologia que mudará nossa rotina e nosso bolso**. El País, 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/09/05/tecnologia/1504627799_633392.html>. Acesso em: 10 jul. 2021.

NOOHANI, Meer Zafarullah; MAGSI, Kaleem Ullah. **A Review of 5G Technology:** Architecture, Security and Wide Applications. International Research Journal of Engineering and Technology (IRJET), 2020. Disponível em:<https://www.researchgate.net/publication/341541673_A_Review_Of_5G_Technology_Architecture_Security_and_wide_Applications >. Acesso em: 09 jun. 2021.

PARKS, Raymond C.; DUGGAN, David P. **Principle of Cyber-warfare**. IEEE SECURITY & PRIVACY. 2011. Disponível em: <http://pages.erau.edu/~andrewsa/bumgarner3_1.pdf>. Acesso em: 20 jun. 2021.

PROLIM. **IoT Applications in Defense**. Prolim, 2021. Disponível em: < https://www.prolim.com/iot-applications-in-defense/>. Acesso em: 14 ago. 2021.

QINGLIANG, zhang; GUONING, zhang. **5G Promotes the Acceleration of Intelligentized Operations**. Battlefield Singularity, 2019. Disponível em: <https://www.battlefieldsingularity.com/post/5g-and-the-future-of-ai-on-the-battlefield>. Acesso em. 27 Jul. 2021.

QMC TELECOM. **O Guia Completo do 5G**. QMC Telecom, 2020. Disponível em: <https://www.qmctelecom.com.br/download-do-ebook-do-5g?hsCtaTracking=7d197ba0-

e859-4f4f-b4b4-f09c4e7d68be%7C66d3004c-b5d3-445b-aadf-5117e6b23df3>. Acesso em: 18 abr. 2021.

RIGUES, Rafael. **Pentágono desenvolve sistema contra armas hipersônicas**. Olhar Digital, 2019. Disponível em: <https://olhardigital.com.br/2019/12/18/noticias/pentagono-desenvolve-sistema-contra-armas-hipersonicas/ >. Acesso em: 28 jul. 2021.

SAHU, Manisha. **7 Applications of IoT in Defence and Military**. Analitics Step, 2021. Disponível em:<https://analyticssteps.com/blogs/7-applications-iot-defence-and-military>. Acesso em: 14 ago. 2021.

SAMSUNG. **Massive MIMO for New Radio**, Technical White Paper. Samsung, 2020. Disponível em: <https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-papers/1208_massive-mimo-for-new-radio/MassiveMIMOforNRTechnicalWhitePaper-v1.2.0.pdf>. Acesso em: 20 ago. 2021.

SILLIMAN, Craig. **The forthcoming competition between cities over wireless technology**. Verizon, 2018. Disponível em:< https://www.verizon.com/about/our-company/fourth-industrial-revolution/forthcoming-competition-between-cities-over-wireless-technology >. Acesso em: 10 jul. 2021.

SOCIEDADE 5G. **Diferenças entre as redes 1G, 2G, 3G, 4G e 5G**. Sociedade 5G, 2019. Disponível em: <https://sociedade5g.com.br/quais-sao-as-diferencas-entre-redes-1g-2g-3g-4g-e-5g-2/ >. Acesso em: 04 jul. 2021.

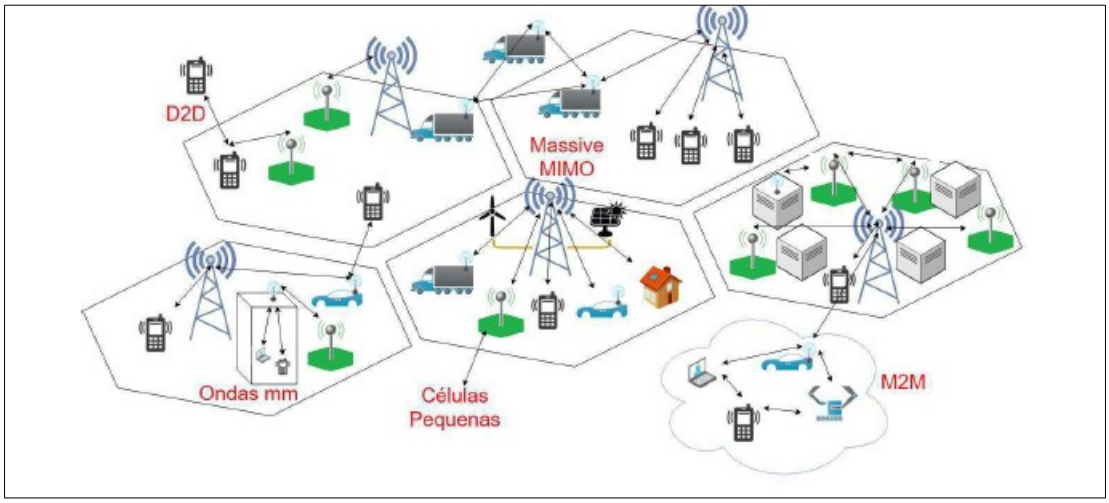
THE GUARDIAN. **Natanz 'sabotage' highlights Iran's vulnerability to cyber-attacks**. The Guardian, 2021. Disponível em: https://www.theguardian.com/world/2021/apr/12/natanz-nuclear-facility-sabotage-iran-vulnerability-to-cyber-attacks>. Acesso em: 06 abr. 2021.

VERRANT, Jeff. **Industry Perspective:** 5G Can Drive the Automation of Military Networks. National Defense, 2021. <https://www.nationaldefensemagazine.org/articles/2021/3/22/5g-can-drive-the-automation-of-military-networks>. Acesso em: 28 jul. 2021.

ZAIDI, Ali. **Three design principles of 5G New Radio**. Ericsson, 2017. Disponível em: <https://www.ericsson.com/en/blog/2017/8/three-design-principles-of-5g-new-radio>. Acesso em: 11 jul. 2021.

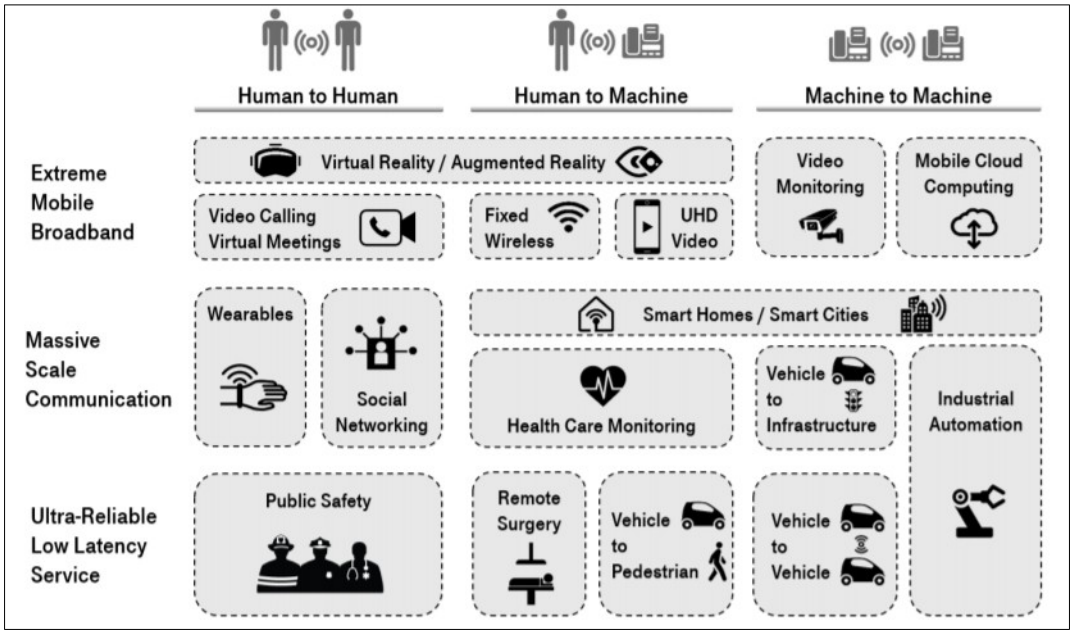
ANEXO - LISTA DE FIGURAS

Figura 01 - Arquitetura proposta para o 5G.



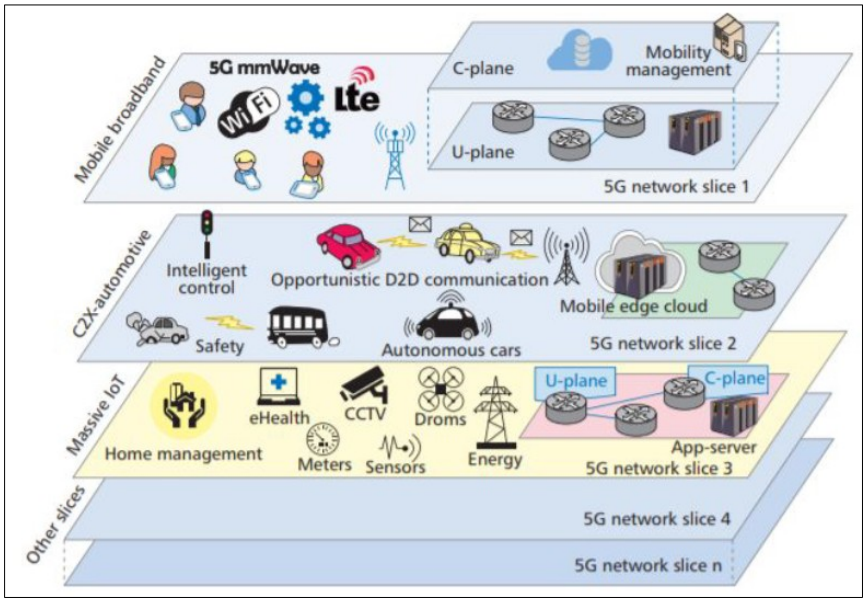
Fonte: GOMES, 2021.

Figura 02 – Cenários de Uso do 5G.



Fonte: 5G AMERICAS, 2017.

Figura 03 – Fatiamento de Rede (*Network Slicing*).

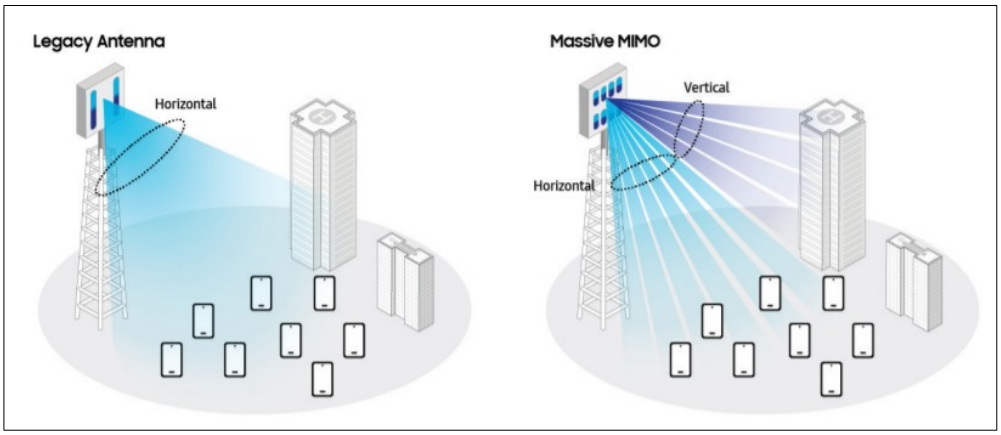


Fonte: LOPES; LOPES, 2019.

Figura 04 – *Small Cell* instalada em poste de luz.

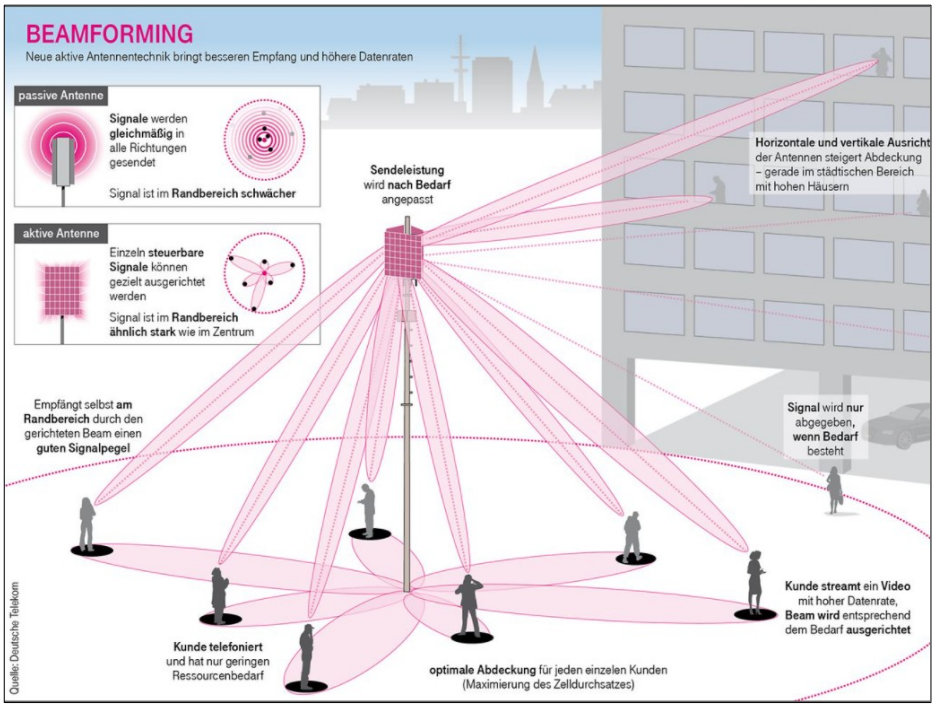
Fonte: ITU, 2018.

Figura 05 – Antena Massive MIMO com feixes verticais e horizontais.



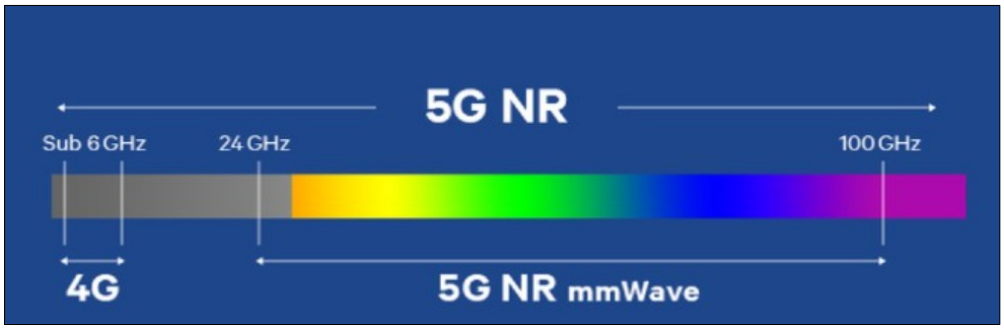
Fonte: SAMSUNG, 2020.

Figura 06 – Antena MIMO com uso da tecnologia *Beamforming* (feixes direcionais).



Fonte: JODL, 2019.

Figura 07 – Faixa de frequência utilizada pelo 5G NR.

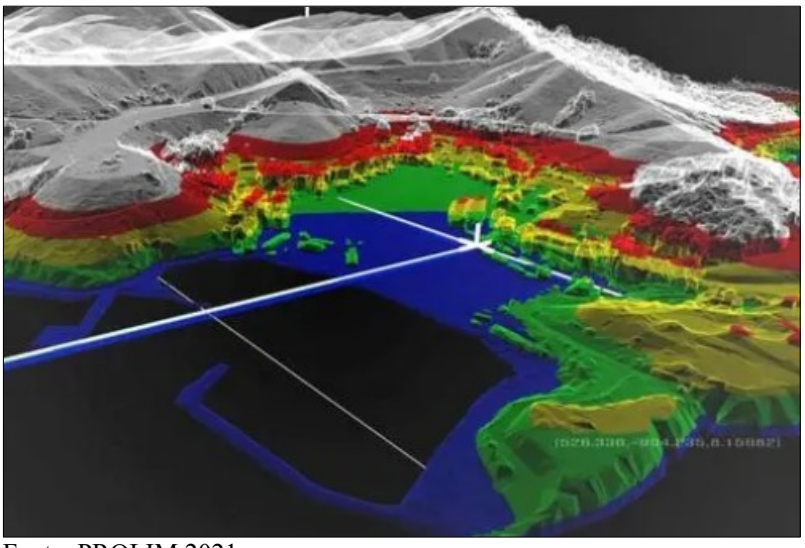


Fonte: KASHYAP, 2021.

Figura 08 – Exercício militar com Realidade Aumentada.

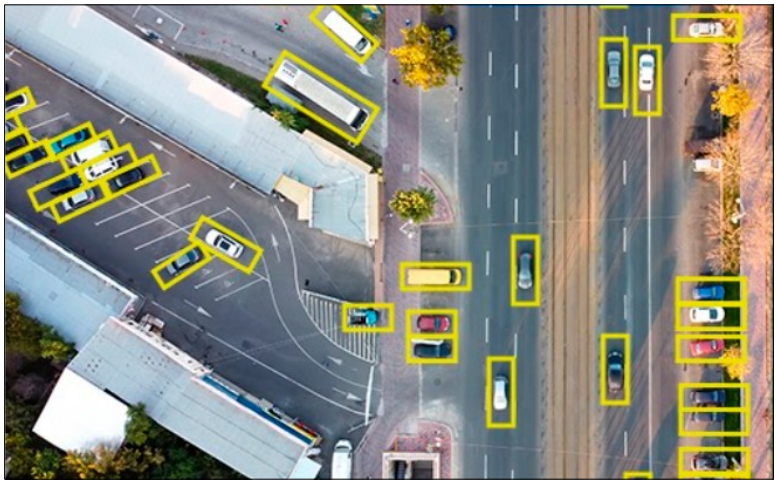
Fonte: PROLIM,2021.

Figura 09 – Mapeamento 3D de terreno, por câmera acoplada em drone.



Fonte: PROLIM,2021.

Figura 10 – Utilização de algorítimos de IA para detecção de possíveis alvos.



Fonte: SAHU, 2021.