ESCOLA DE ARTILHARIA DE COSTA E ANTIAÉREA
CURSO DE PÓS-GRADUAÇÃO NO NÍVEL LATO SENSU EM ARTILHARIA DE COSTA E ANTIAÉREA.

WATSON DAVID DE OLIVEIRA CARVALHO

A IMPORTÂNCIA DO DESENVOLVIMENTO E UTILIZAÇÃO DE SISTEMAS DE SIMULAÇÃO NO APRENDIZADO DE RADARES, GUERRA ELETRÔNICA E GUERRA CIBERNÉTICA

Rio de Janeiro
2019

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DETMil
ESCOLA DE ARTILHARIA DE COSTA E ANTIAÉREA

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

COMUNICAÇÃO DO RESULTADO FINAL AO POSTULANTE (TCC)

CARVALHO, Watson David de Oliveira (1º Ten (QC-FN)). A importância do desenvolvimento e utilização de sistemas de simulação no aprendizado de radares, guerra eletrônica e guerra cibernética. Trabalho de Conclusão de Curso apresentado no programa *lato sensu* como requisito parcial para obtenção do certificado de Pós-Graduação em Operações Militares de Defesa Antiaérea e Defesa do Litoral. Escola de Artilharia de Costa e Antiaérea.

Orientador: GUSTAVO DE AZEVEDO CARVALHO MOURA / CAPITÃO / ARTILHARIA

Resultado do Exame do Trabalho de Conclusão de Curso: _____

Rio de Janeiro, ___ de _____ de 2019.

COMISSÃO DE AVALIAÇÃO

_____
ELISANDRO RODRIGUES DE FREITAS CUNHA / MAJOR / ARTILHARIA
PRESIDENTE

_____
GUSTAVO DE AZEVEDO CARVALHO MOURA / CAPITÃO / ARTILHARIA
MEMBRO

_____
RICARDO CAMPELLO DE ALCÂNTARA / CAPITÃO / ARTILHARIA
MEMBRO

WATSON DAVID DE OLIVEIRA CARVALHO

A IMPORTÂNCIA DO DESENVOLVIMENTO E UTILIZAÇÃO DE SISTEMAS DE SIMULAÇÃO NO APRENDIZADO DE RADARES, GUERRA ELETRÔNICA E GUERRA CIBERNÉTICA

Trabalho de Conclusão de Curso apresentado à Escola de Artilharia de Costa e Antiaérea como requisito parcial para a obtenção do Grau de pós-graduação em Artilharia de Costa e Antiaérea.

ORIENTADOR: Cap GUSTAVO DE AZEVEDO CARVALHO MOURA

Rio de Janeiro
2019

MINISTÉRIO DA DEFESA

AGRADECIMENTOS

Agradeço aos meus familiares por estarem sempre comigo em todos os momentos da minha vida e mesmo estando longe, estão no meu coração.

Aos meus companheiros por compartilharem seus conhecimentos e aprendizados, sempre dispostos a me ajudar nas dificuldades.

Ao meu orientador, pela paciência e disponibilidade, orientando e corrigindo sempre que possível durante todo o trabalho.

A todos os demais amigos e pessoas mais próximas por contribuirem, de maneira direta ou indireta para o meu crescimento como pessoa e como profissional.

RESUMO

Um ambiente simulado quando utilizado para as técnicas de segurança é muito importante, e fundamental, para qualificar o processo de treinamento operacional, assim como, para a segurança da informação e das comunicações, especialmente quando estas serão aplicadas numa situação real. O objetivo deste trabalho foi de avaliar a importância do desenvolvimento e utilização de sistemas de simulação no aprendizado de radares e guerra eletrônica. O mesmo foi elaborado através uma pesquisa qualitativa, do tipo exploratória e por meio de um referencial teórico. Verificou-se que nas operações militares brasileiras a preocupação com a guerra eletrônica vem crescendo cada vez mais, sendo que, está hoje é vista como um instrumento que obtém informações importantes com praticamente todos os elementos de combate. Nesse sentido, acredita-se que as informações obtidas por meio da guerra eletrônica são fundamentais para a tomada de decisão do comandante do escalão, operacional ou tático. As principais vantagens constatadas para os simuladores no aprendizado de radares e guerra eletrônica são relacionados à redução do custo de formação e treino de pessoal; a redução do tempo de formação e treino do pessoal; o aumento de segurança; o aumento de janela de oportunidade para um treino em voo; reduzem os custos operacionais de poluição atmosférica e sonora; poupam combustíveis e diminuem os distúrbios ambientais, dentre outros.

Palavras-chave: Segurança, aprendizado, simulador, radares, guerra eletrônica.

ABSTRACT

A simulated environment when used for security techniques is very important and critical for qualifying the operational training process as well as for information and communications security, especially when they will be applied in a real situation. The aim of this study was to evaluate the importance of the development and use of simulation systems in radar learning and electronic warfare. It was elaborated through a qualitative, exploratory research and through a theoretical framework. It has been found that in Brazilian military operations the concern with electronic warfare has been growing more and more and is today seen as an instrument that obtains important information with virtually all combat elements. In this sense, it is believed that the information obtained through electronic warfare is fundamental to the decision making of the echelon commander, operational or tactical. The main advantages found for simulators in radar learning and electronic warfare are related to the reduced cost of training and personnel training; reducing staff training time; increased security; increased window of opportunity for in-flight training; reduce operating costs of air and noise pollution; save fuel and reduce environmental disturbances, among others.

Keywords: Safety, learning, simulator, radar, electronic warfare.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Com o grande avanço tecnológico presenciado nos últimos anos em todo o mundo, o espaço cibernético é uma das principais preocupações das defesas armadas no Brasil, assim como, nos demais países do mundo. Nesse sentido, as ferramentas relacionadas às simulações e treinamentos podem ser utilizadas em muitos espaços de forma a ajudar consideravelmente no controle e guerra eletrônica (MACHADO, 2016).

No Brasil, a Estratégia Nacional de Defesa se tornou pública e notória especialmente a partir de 2008, quando, a Presidência da República reconheceu o setor cibernético de grande interesse para o Brasil e para a Defesa Nacional (BRASIL, 2008).

O Ministério da Defesa solicitou ao Exército a responsabilidade de coordenação e integração do Setor Cibernético no âmbito da Defesa, em que, criando o Centro de Defesa Cibernético (CDCiber), que se destaca pelo projeto Capacitação, Preparo e Emprego do Setor Cibernético, reparando os militares para atuarem no ciberespaço (MACHADO, 2016). Por esta razão o Centro de Instrução de Guerra Eletrônica (CIGE) viu a necessidade de possuir uma ferramenta específica, que atuasse no ciberespaço de forma segura e controlada (MACHADO, 2016).

Os simuladores são as ferramentas mais adequadas para a escola preparar os futuros combatentes. É importante utilizar estes simuladores para treinar e formar seus guerreiros cibernéticos, de como pode ajudar nos exercícios cibernéticos. Um ambiente simulado para as técnicas de segurança é muito importante, e fundamental para os instrutores do CIGE, considerando a utilização de redes em produção, que trabalham com técnicas que comprometem a segurança da informação e das comunicações, quando estas serão aplicadas numa situação real (MACHADO, 2016)

O simulador também ajuda na economia para o CIGE, pois, assim, não será preciso realizar a instalação de redes físicas nas instalações da escola, pois, a simulação proporcionaria o emprego de todas as técnicas necessárias para o processo de ensino-aprendizagem. O simulador é uma ferramenta que

viabiliza a virtualização de redes de computadores, para ajudar no treinamento dos alunos (GOMES, 2013).

Dessa forma, no presente trabalho pretende-se realizar uma contextualização sobre o assunto, de forma a tender aos seguintes objetivos propostos.

2. METODOLOGIA

Este estudo foi elaborado através do método de pesquisa qualitativa, sendo definida como estratégia de confecção e apresentação dos resultados a “Pesquisa explicativa”. De acordo com o autor Gil (2014, p. 46) “a pesquisa explicativa deve ser elaborada tendo o cuidado de buscar a identificação dos fatores determinantes ou que pelo menos possa contribuir para a ocorrência dos fenômenos”.

A pesquisa explicativa tem o principal objetivo de aprofundar o conhecimento da realidade, trazendo a explicação para a razão e o porquê dos fenômenos. Ainda busca identificar os motivos determinantes para o acontecimento de um determinado fenômeno ou que contribuíram e de que forma o acontecimento deste fenômeno. Esse método de pesquisa pode ser entendido ainda, como, uma extensão da pesquisa exploratória ou da pesquisa descritiva (GIL, 2014).

Com relação à pesquisa propriamente dita, esta pode ser definida como a metodologia racional e sistemática com a pretensão de encontrar as respostas para os problemas que são propostos nos trabalhos investigativos (SILVA, 2016).

Geralmente as pesquisas são requeridas em momentos que as informações não existem de modo suficiente, ou inexistem, para chegar até as respostas aos problemas da pesquisa (GIL, 2014).

Portanto, para a realização de um estudo científico é necessário a realização de uma pesquisa, que na maioria das vezes é previa ao estudo e do tipo ‘pesquisa bibliográfica’ (SILVA, 2016). Dessa forma, esta é realizada no intuito de fazer uma fundamentação teórica sobre o assunto proposto, ou até para justificar as suas limitações e também para a discussão dos respectivos resultados.

Dessa forma, o referencial teórico do presente estudo constituiu-se a partir de consultas bibliográficas realizadas por meio de leituras em trabalhos acadêmicos disponíveis na internet, em sites confiáveis como Scielo, Portal da Capes, Google Acadêmico, dentre outros. Além disso, foram realizadas leituras em livros impressos, jornais e revistas que estão á disposição em bibliotecas. A

constituição do presente trabalho se deu no período de janeiro a julho do ano de 2019.

2.1 TEMA

Utilização de sistemas de simulação no aprendizado de radares e guerra eletrônica.

2.2 FORMULAÇÃO DO PROBLEMA

A situação problematizada, que norteou a pesquisa realizada foi a seguinte: “Quais os benefícios da utilização dos simuladores no aprendizado de radares e guerra eletrônica?”.

2.3 QUESTÕES DE ESTUDO

Dentre os questionamentos levantados para o guiamento do presente estudo, destacam-se os seguintes:

a. Quais os benefícios da utilização dos simuladores no aprendizado de radares e guerra eletrônica?
b. Qual seria o maior desafio no desenvolvimento dos simuladores com tecnologia nacional?
c. Qual o principal impacto causado pelo desenvolvimento e utilização dos simuladores na Guerra Eletrônica e Radares?
d. Quais são os atuais sistemas de simulação radar e de guerra eletrônica presente nas forças armadas do Brasil e suas especificações?

2.4 OBJETIVOS

Neste tópico apresentam-se os objetivos geral e específicos, de forma a nortear o desenvolvimento do presente trabalho.

2.4.1 Objetivo Geral

- Avaliar a importância do desenvolvimento e utilização de sistemas de simulação no aprendizado de radares e guerra eletrônica.

2.4.2 Objetivos específicos

- Realizar um referencial teórico sobre a utilização de sistemas de simulação no aprendizado de radares e guerra eletrônica;

- Verificar o emprego da guerra eletrônica nas operações militares brasileiras;

- Contextualizar o uso de radares nos sistemas de simulação de aprendizagem.

2.5 JUSTIFICATIVA

O trabalho se justifica pela importância do tema em relação à segurança nacional brasileira, especialmente com relação á respectiva importância do processo de simulação no aprendizado sobre a utilização dos radares na guerra eletrônica.

O trabalho se justifica ainda pela importância em apresentar e contextualizar temas de relevante interesse do meio acadêmico atual, especialmente por se tratar de um assunto que busca esclarecer e reduzir as os custos em operações de treinamentos militares. Ainda, pretende-se apresentar os resultados no meio acadêmico e para o público em geral.

2.6 CONTRIBUIÇÃO

O presente estudo pretende ampliar o conhecimento acerca dos sistemas de simulação de radares e guerra eletrônica, seus aspectos e aplicações no aprendizado e desenvolvimento dos mesmos.

Ainda, a partir das informações levantadas, o presente estudo pretende dar subsídios para pesquisas futuras sobre os sistemas de simulação, estimular seu desenvolvimento e reconhecimento de sua importância.

3. GUERRA CENTRADA EM REDES

A Guerra Centrada em Redes (GCR) se baseia no poder e nos respectivos ligamentos de combate. A GCR pode alcançar uma posição superior de informação, em comparação ao adversário. Portanto, esta posição de informação pode ser maior por causa da sua capacidade de coletar, processar e disseminar um fluxo de informação ininterrupto, impedindo que o adversário faça a o mesmo (ALBERTS, 2009).

A Guerra Centrada em Redes amplia a projeção das forças e de alcance, mantendo um fluxo de informações interações. Neste sentido, a capacidade de sincronizar as ações, aumentar a velocidade sobre uma estrutura de rede robusta pode ser denominada de Poder da Capilaridade (SANT' ANA JÚNIOR, 2012).

As topologias de redes de comunicações adotadas pela organização são tradicionais, modernas e flexíveis, ou seja, apresentam variadas estruturas organizacionais e características próprias que dificultam a complementação de uma determinada missão ou ainda, de uma tarefa qualquer (SANT' ANA JÚNIOR, 2012).

Neste sentido, verifica-se que as topologias de redes de comunicações tradicionais tendem a ser mais rápidas e mais cíclicas, ou seja, são mais adequadas em situações simples, já, as redes cíclicas são utilizadas para a resolução de respectivos problemas complexos e dinâmicos (SANT' ANA JÚNIOR, 2012).

Segundo Alberts; Hayes, (2005) na GCR o ambiente é criado para compartilhar informações, solucionando os problemas sem perder velocidade, por meio da topologia de rede robusta, que é a melhor opção para adquirir superioridade de informação.

As forças armadas se adaptarem as novas tecnologias para enfrentar as possíveis ameaças. Portanto, o principal conceito da GCR se relaciona com as trocas de informação, com o seu processamento, com a análise e interpretação, e também com a partilha de informações que está num espaço de batalha entre os níveis de comando (SANTOS, 2007).

Segundo Harz (2005) este novo paradigma de guerra vai depender da capacidade, e do potencial que as novas tecnologias apresentam. Portanto, a

GCR possui uma grande eficácia nos seus sistemas de armas. Estes sistemas contêm as informações que são obtidas por sensores que estão espalhados entre as plataformas.

A GCR tem se fundamenta na atividade comercial, ou seja, as forças navais americanas se tornaram alvo de vários ajustamentos, por causa das especificidades de cada país, implicando na complexidade e na compreensão. Muitas nações através da GCR reconhecerem as operações militares em rede como um instrumento de afirmação política e militar (SANTOS, 2007).

O cenário GCR revela três conceitos distintos: o conceito humano; de processos; o tecnológico. A GCR serve para modernizar os sistemas de armas, a fim de promover a interoperabilidade. Portanto, ainda não se sabe ao certo se a aquisição de programas de sistemas de armas cumpre com os requisitos técnicos para a interoperabilidade num cenário de GCR (HOBBINS, 2005).

Desta forma, as vantagens da GCR são o compartilhamento da consciência situacional, também de acelerar as operações, e de proteger as forças convencionais e ações sincronizadas. Para alcançar estas vantagens é preciso seguir os princípios da GCR, onde se destaca a conexão das forças militares em redes.

Nesse sentido, verifica-se como exemplo que com a guerra entre os Russos e japoneses se originou a GE – Guerra Eletrônica, onde, os Russos impediram as comunicações de telégrafo sem fio entre o comando da esquadra japonesa (SANT' ANA JÚNIOR, 2012).

Segundo Clarke; Knake, (2010) um dos principais projetos da GE é o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), cuja principal função é de dotar a Força Terrestre de meios para uma efetiva presença em áreas de interesse do território nacional.

Com o objetivo de interferir e também de interceptar os sinais eletromagnéticos dos emissores de uma força oponente. Dessa forma, um sistema inimigo para o no ataque e amigo para a proteção. Portanto, a Guerra Cibernética é outro conceito de proteção e ataque dos sistemas de controle (CLARKE; KNAKE, 2010).

A Guerra Cibernética é usada para referenciar ações de um Estado contra outro, atingindo computadores e redes, causando prejuízos e interrupções. Portanto, o Ciberespaço que se forma com meios digitais, por

onde a informação passa se torna um campo de batalha da Guerra Cibernética, em que se gera uma intersecção com a Guerra Cibernética, por possuírem necessidades de segurança da informação, como é o caso da criptografia (SANT' ANA JÚNIOR, 2012).

Desta forma, a Guerra Cibernética amplia o campo de batalha virtualmente, influenciando nas dimensões físicas. Assim, a GC e a GE juntamente com os preceitos estabelecidos pela GCR têm superioridade da informação, ampliando o poder de combate de uma força.

A principal definição da GCR são as operações impregnadas que geram o combate que é interligado em rede de sensores, atingindo assim, uma consciencialização partilhada, com toda sua superioridade informacional em poder de combate (ALBERTS, 2003).

A GCR conta com diversos elementos de combate, dentre eles, podemos destacar o planeamento, a logística, os elos C4ISR, e também as unidades de combate e os sistemas de emprego de armas (HOBBINS, 2005).

Portanto, o conceito da GCR se traduz na aplicação da partilha de conhecimento, sendo que, na prática existe a criação da informação, que só será possível através do uso das tecnologias. A partilha significa serve para equilibrar as redes que são interligadas, e proporcionam ligações tridimensionais as unidades de uma força. O conceito da GCR significa conhecimento, e, no momento em que este conhecimento for comparado a “informação”, vai refletir em uma grandeza diferente (HARZ, 2005).

O conhecimento que também pode ser chamado de “informação enriquecida” junta às comunidades que estão associadas às áreas de interesse, e que permanecem apoiadas ao fluxo de informação e na capacidade de sentir a informação elevada (HARZ, 2005).

Neste sentido, a partilha de informação ultrapassa os processos de recolha, por meio dos níveis de comando. Assim, a GCR permite a recolha de imagem por meio de uma aeronave não tripulada, que ajuda a melhorar as informações fornecidas pelos observadores aéreos (SANTOS, 2007).

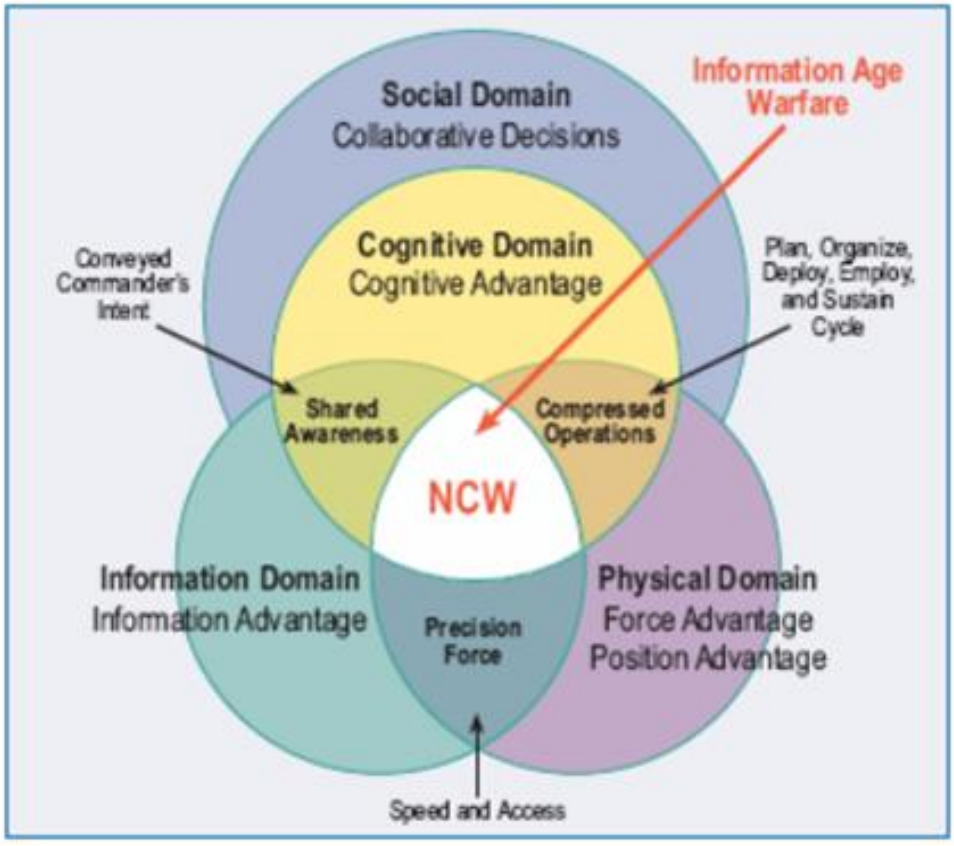
Numa batalha os combatentes usam câmeras de vídeo para poder passar a informação de alvos, com a utilização da internet. A conexão entre os quartéis-generais e as linhas da frente trouxe um novo conceito, que serviu

para aproximar os indivíduos, as organizações e os sistemas (ALBERTS, 2003).

A informação e tecnologia se diferenciam pelo fato de que a “informação” é utilizada para identificar diversos pontos que se transformam em conhecimento. A informação utilizada vai depender de um o domínio envolvente, que se diferencia entre o físico, informacional, cognitivo e social (PHISTER, 2004).

Neste sentido, os domínios definem a informação de maneira diferente, pois, há uma base importante que evidência a informação como sendo um resultado de observações individuais. Nesse sentido, na figura 1 apresenta-se uma imagem que se refere aos domínios da guerra centrada em rede.

Figura 1: Os domínios da guerra centrada em rede.



Fonte: Adaptado de Dod (2005).

A GCR transmite uma informação através de um processo de decisão em combate. Sendo assim, estas informações possuem algumas vantagens

que são evidenciadas no momento em que a mesma for potencializada por uma rede alicerçada, informada e dispersa, que vai se caracterizar pela partilha de informação, e pelo conhecimento do comandante. Ainda existem algumas vantagens em combate que poderão servir para as mudanças de comportamento, aumentando a sincronização de cada elemento, e também a velocidade de comando e o potencial de combate.

3.1 GUERRA CIBERNÉTICA

De um modo em geral, no domínio cibernético, as intenções de um ataque são de confiabilidade reduzida, porém, existem algumas dificuldades de identificar a autoria de seus delimitadores geográficos. Pesquisar o alvo do ataque, os interesses e os padrões de comportamento, não resulta em certeza sobre a identificação da fonte (BRICK, 2014).

Os ataques que aconteceram na guerra na Geórgia, por exemplo, geraram alguns benefícios vindos das ações nas redes georgianas, porém, não existe evidência clara do patrocínio dessas ações. A dimensão das ações cibernéticas é alcançada com o conhecimento de que as interfaces entre os mundos físico e digital foram direcionadas a controladores computadorizados, ou seja, ao sistema Scada (BRICK, 2014).

O controle do espaço cibernético representa o domínio dos sistemas interligados à infraestrutura, a habilidade de usar o espaço cibernético para gerar vantagens e eventos em outros ambientes operacionais. A Guerra Cibernética são ações militares, no espaço cibernético, a fim de destruir ou comprometer a integridade de ativos do adversário baseando-se nas informações, e nas redes de computadores (BRICK, 2014).

O Planejamento Estratégico Militar só é possível através da classificação das ações cibernéticas. Portanto, estas ações podem ser classificadas em: exploração, ataque e proteção cibernética. Quanto mais complexa e desenvolvida for à tecnologia da Guerra Cibernética, maior será a dependência dos serviços ofertados no espaço cibernético (BRICK, 2014).

Desta forma, conforme o autor supracitado, verifica-se que o controle dos efeitos decorrentes do emprego de arma cibernética representa um aspecto tecnológico a ser observado em um ataque.

3.2 A CONDUÇÃO DA GUERRA CIBERNÉTICA NO CENÁRIO MUNDIAL

A eficácia do ataque cibernético comprovou a validade dos esforços de estruturação da guerra. Assim, no cenário mundial, muitas preocupações em relação a isso foram sendo discutidas, como por exemplo, a concretização do domínio cibernético para a Segurança Nacional, no caso brasileiro, através do entendimento da Guerra Cibernética como sendo uma grande ameaça aos Estados (BRICK, 2014).

Ainda, segundo o autor, ainda em 2011 a Presidência dos Estados Unidos da América, baseando-se nas tecnologias em rede (internet) para a sociedade e a economia, estabeleceu princípios para sua operacionalização livre e segura. No mesmo período, o respectivo Departamento de Defesa norte americano divulgou sua Estratégia de Operação no Ciberespaço, derivada de cinco estratégicas:

- Estabelecer o ciberespaço para domínio operacional, e para a segurança nacional;
- Empregar novas formas operacionais para proteger as redes e sistemas e segurança das informações digitais;
- Ir à busca de parcerias governamentais e privadas;
- Buscar parceiros no âmbito internacional;
- Preparar continuamente os recursos humanos.

Da mesma forma, é grande a preocupação do Estado brasileiro em proteger os ativos e a capacidade de atuação em rede na Cibernética nas forças armadas, especialmente na Marinha do Brasil. A National Security Agency (NSA) é a agência de segurança dos Estados Unidos. Esta agência engloba ações de ataque em prol da defesa dos sistemas de segurança dentro do seu espaço com o estabelecimento do Setor Cibernético como estratégico, a fim de conferir a confidencialidade, disponibilidade, integridade e autenticidade dos sistemas do espaço cibernético (BRICK, 2014).

No ano de 2012 o ministério da defesa aprovou a Política Cibernética de Defesa, a fim de orientar as atividades nos níveis operacional e tático, das

Forças Armadas. O espaço cibernético pelas Forças Armadas dificulta seu uso contra os interesses da Segurança Nacional, garantindo assim, a liberdade de ação.

Desse modo, a estruturação do Setor Cibernético brasileiro contribui para a Segurança da Informação, da comunicação, e para a Segurança Cibernética que é feita por outros órgãos do governo envolvidos (BRICK, 2014).

Da mesma forma, a Marinha do Brasil estabeleceu a Guerra Cibernética como tema de interesse, inserida também no Plano de Tecnologia da Informação da Marinha. Portanto, as atividades de proteção realizadas pela Marinha do Brasil são monitoradas e avaliadas continuamente aos princípios aplicados à guerra cibernética. Foram realizadas simulações no espaço cibernético da Marinha, a fim de explorar este novo domínio e sua importância para o Comando e Controle das Operações Militares (BRICK, 2014).

4. EMPREGO DA GUERRA ELETRÔNICA NAS OPERAÇÕES MILITARES BRASILEIRAS

Em vários estados percebe-se que a estruturação do setor cibernético e o domínio tecnológico a guerra cibernética não é mais um novo conceito doutrinário. Portanto, as comunicações, e informações, corroboram a existência de ações de exploração e Inteligência da nova guerra global.

Neste sentido, a guerra no domínio cibernético é mais complicada no ponto de vista financeiro, se não for comprovado o ataque. Já do ponto de vista defensivo, a ameaça cibernética é considerada de maior complexidade, em que a adaptação dos Estados para enfrentá-la precisa ser elaborada com responsabilidade, flexibilidade, rapidez e visão estratégica.

No Brasil, a Estratégia Nacional de Defesa se tornou pública e notória especialmente a partir de 2008, quando, a Presidência da República reconheceu o setor cibernético de grande interesse para o Brasil e para a Defesa Nacional (BRASIL, 2008).

O Ministério da Defesa solicitou ao Exército a responsabilidade de coordenação e integração do Setor Cibernético no âmbito da Defesa, em que, criando o Centro de Defesa Cibernético (CDCiber), que se destaca pelo projeto Capacitação, Preparo e Emprego do Setor Cibernético, reparando os militares para atuarem no ciberespaço (MACHADO, 2016). Por esta razão o Centro de Instrução de Guerra Eletrônica (CIGE) viu a necessidade de possuir uma ferramenta específica, que atuasse no ciberespaço de forma segura e controlada (MACHADO, 2016).

A estruturação militar no Brasil, em se tratando do Ministério da Defesa, percebe-se que as ações do governo brasileiro estão em busca de uma sinergia com outros parceiros, para compras, contratações e desenvolvimento de produtos e sistemas de defesa, juntamente com a necessidade de estabelecer incentivos ao para as áreas de informação e de Inteligência, neste novo domínio operacional da guerra, o cibernético.

O cibernético, no cenário militar, ajudará as forças armadas a atuarem em rede, e, com a coordenação do Exército Brasileiro, o MD vem promovendo maneiras e métodos para implementar estruturas para assegurar o uso efetivo

do espaço cibernético pelas Forças Armadas, de forma a impedir seu emprego contra interesses da Defesa Nacional.

Desta forma, com o desenvolvimento do Setor Cibernético, e os avanços tecnológicos, desejado pelas Forças Armadas, são limitados pela disponibilidade orçamentária do Governo Federal.

De um modo em geral, nas operações militares brasileiras a constatação de guerra eletrônica vem crescendo cada vez mais, sendo que, a guerra eletrônica é um instrumento que obtém informações importantes com os elementos de combate. Nesse sentido, acredita-se que as informações obtidas por meio da guerra eletrônica são fundamentais para a tomada de decisão do comandante do escalão, operacional ou tático (SILVA, 2017).

Após a segunda guerra mundial a Educação Técnica Militar do Exército Brasileiro se originou, atuando em todo o território nacional, dispondo de um público de estudantes, oficiais do Exército (CUPERSCHMID; AMORIM; MATOS, 2015).

Nesse sentido, verifica-se que uma das missões do exercito é de preparar os soldados para entrar em situações de conflitos urbanos, como em favelas, a fim de perseguir e prender criminosos, especialmente quando há intervenção federal. O Centro de Instrução de Operações de Garantia da Lei e da Ordem (CIOpGLO) forma profissionais, e preparar oficiais para o combate urbano (GOMIDE, 2012),

O Exército Brasileiro além de operar em favelas, também recupera o controle de territórios, sendo que, necessário treinar todos os militares envolvidos nestas operações para que as mesmas sejam bem sucedidas (GOMIDE, 2012).

Os conflitos acontecem dentro das cidades, sendo que, se faz necessário o combate urbano, e para isso as Forças Armadas devem simular ambientes como favelas e bairros onde mora a população de baixa renda, para realizar o treinamento (CUPERSCHMID; AMORIM; MATOS, 2015).

Conforme Brasil (2009) a guerra eletrônica se empregada de maneira certa, pode ser multiplicadora do poder de combate, porém, suas implicações são reconhecidas e suas potencialidades indispensáveis à sobrevivência das forças e ao sucesso da missão.

Os objetivos das atividades da guerra eletrônica conforme o (Brasil, 2009) podem ser:

- Medidas de Apoio de Guerra Eletrônica: que obtém dados do oponente, a partir das emissões eletromagnéticas;
- Medidas de Ataque Eletrônico: impede o uso do espectro eletromagnético pelo oponente;
- Medidas de Proteção Eletrônica: assegura a utilização eficaz e segura das próprias emissões eletromagnéticas.

De um modo em geral, nas operações de combate, todo comandante pode orientar seus subordinados às missões que irão desenvolver. Para passar estas informações, o comandante precisa buscar informações acerca de seu oponente, por meio de sinais e de imagens (BRASIL, 2009).

Neste contexto, as informações são obtidas pela MAGE, um conjunto de sensores que extrai do espectro eletromagnético, todo tipo de informações acerca do inimigo. Portanto, estas informações auxiliam na busca de interceptação, monitoração, localização eletrônica e registro. Por outro lado, as MAE são ações que impedem o uso do espectro eletromagnético pelo oponente, destruindo seu poder de combate (SILVA, 2017).

Da mesma forma, existe ainda as MPE, que por sua vez são um conjunto de ações que asseguram o emprego eficiente do espectro eletromagnético, apesar da atuação das MAGE e MAE oponentes.

O CIOpGLO possuí várias instalações para treinamento, e, a cidade simulada tem características de uma cidade real, com diferentes blocos, semelhante a uma cidade cenográfica (GOMIDE, 2012).

Segundo Gomide, (2012) nas simulações militares, o uso de explosivos simulados e a exposição gradual ao estresse são necessários, sendo os instrutores do CIOpGLO que devem observar os alunos que apresentarem os mesmos sintomas de estresse de combate.

Os soldados militares durante o treinamento utilizam de vários tipos de simulação, como por exemplo, réplicas de armas que fazem uso de paintball em espaços físicos constituídos por paredes feitas de madeira e tijolos. Portanto, com a informática, é possível coletar dados em tempo real sobre os

treinamentos, e também idealizar um treinamento militar com o uso de gamificação.

Segundo Kap (2012) a gamificação é o uso de elementos de jogo em um contexto de não-jogo que por sua vez motiva os usuários, ou seja, ela consiste em elementos tradicionalmente ligados à diversão e ao jogo que promove o aprendizado.

No treinamento militar alguns jogos possuem características importantes que envolvem os soldados durante a sua formação. Os videogames imergem um mundo sintético já os jogos que utilizam RA (Realidade Aumentada) Móvel, a interação acontece num ambiente real.

Neste sentido, o controle do estresse é realizado para aqueles militares que não atingem o nível de controle emocional, sendo esses colocados fora da missão de combate.

4.1 IMPLICAÇÕES DAS POLÍTICAS PÚBLICAS NA GUERRA ELETRÔNICA NAS OPERAÇÕES MILITARES BRASILEIRAS

As implicações das políticas públicas na área da guerra eletrônica são muito influenciadas pela competitividade, pela capacidade produtiva, e pela tecnologia de inovação disponível, sendo que se destacam pela elevação dos investimentos, maior integração da indústria de defesa com o Sistema Nacional de Inovação, e pelo estabelecimento de parcerias estratégicas (VIANELLO, 2018).

Desta forma, é fundamental a criação de uma agência que esteja vinculada ao MD (Ministério da Defesa) ou ao MCTI (Ministério da Ciência, Tecnologia e Inovação), de forma similar a outras agências reguladoras de diversas atividades estratégicas como, por exemplo, a Anatel, Aneel e ANS. Nos Estados Unidos, por exemplo, uma das agências é a DARPA, que engloba o modelo de Departamento de Defesa, universidades e empresas públicas e privadas (VIANELLO, 2018).

As compras governamentais de defesa que ficam mantidas correm o risco de queda da demanda, porém, a estabilidade e expansão destas compras seriam importantes para a sobrevivência da BID. No Brasil a privatização de setores estratégicos, como as telecomunicações geram tecnologias, como por

exemplo, a produção de produtos duais e ao crédito; a melhoria e a expansão da infraestrutura; o desenvolvimento maior do mercado de seguro-garantia; e a simplificação tributária (VIANELLO, 2018).

A eliminação de barreiras políticas e econômicas são fundamenteis, especialmente para a América do Sul, em que há incentivo de aumento de fornecimento de insumos de alta tecnologia. Neste sentido, o governo federal poderia negociar para que serviços de manutenção sejam realizados no país, por técnicos do próprio comprador, se produtos estratégicos forem importados, ou com o próprio vendedor dentro do país.

Também é negociável a manutenção de estoque estratégico de peças com defeito, mapeadas pelo comprador ou vendedor que são realizadas pelas empresas estrangeiras para as nacionais. Portanto, para aumentar a capacidade produtiva é importante o alinhamento no setor das políticas públicas, em que, os insumos vêm de dezenas de países e os produtos acabados são vendidos localmente e exportados para os mercados mundiais.

Uma das estratégias de impedir o fornecimento de insumos seria o mapeamento do comprador ou vendedor das peças com maior probabilidade de defeito. As ações públicas implantadas, voltadas para a organização e à expansão da BID também é outra estratégica.

Desta forma, a disponibilização e a disseminação de informações dos programas e serviços disponibilizados pelo governo federal, como programas de financiamento, programas para P&D e desenvolvimento de produtos e serviços poderão viabilizar a criação de redes de pequenas e médias empresas, a fim de atender as às necessidades do segmento.

O estratégico segmento tecnológico de defesa e segurança são os sistemas eletrônicos e de comando e controle, que podem ser câmeras, sensores, radares, sonares, e também os equipamentos de comunicações e guerra cibernética, além dos sistemas que se encontram nas aeronaves, navios, mísseis, veículos blindados, e outros (BARROS et al., 2013).

O comércio de equipamentos relacionados ao sistema de defesa movimentou 247 bilhões, entre 2003 e 2012. Porém, 13 bilhões foram destinados em sensores e 4%, o que representa aproximadamente 10 bilhões em sistemas de comando e controle para defesa antiaérea. Desta forma, as aeronaves, navios, mísseis, veículos blindados, motores, artilharia, satélites,

têm vasta gama de componentes eletrônicos atualizados, tornando-se um percentual ainda maior (BARROS et al., 2013).

4.2 PRINCIPAIS NORMATIVAS

A segurança dentro da aviação é regulada pela convenção de Chicago, baseando-se nas normas desenvolvidas pela Organização da Aviação Civil Internacional (ICAO). Nas transportadoras aéreas a segurança é supervisionada pelo país de origem, por isso é fundamental o uso dos simuladores na Formação de Pilotos e CTA´S e Seu Impacte na Segurança de Voo.

De um modo em geral, a segurança na União Europeia se baseia na criação de uma Agência Europeia para a Segurança da Aviação, e nos requisitos de segurança para certificação da aeronavegabilidade de todos os produtos aeronáuticos.

No Brasil, conforme a regulamentação n.º 1592/2002 da ESA assegura todas que todas as operações aéreas ficarão sob a responsabilidade da Agência, que estabelece um controle rigoroso na segurança do projeto, protegendo os passageiros, os trabalhadores do setor de transporte aéreo e os cidadãos que vivem em zonas próximas dos aeroportos.

Desta forma, para assegurar a segurança na aviação de todas as aeronaves que voam com destino à comunidade, ou no interior do seu território, o Parlamento Europeu juntamente com o Conselho adoptaram a Diretiva 2004/36/CE, uma segurança das aeronaves de países terceiros que utilizem aeroportos comunitários.

A Diretiva 2004/36/CE prevê também o intercâmbio de informações entre os Estados-Membros, levando para toda a Comunidade medidas adotadas por um Estado-Membro.

Desta forma, as medidas associadas à aviação têm a responsabilidade de: Identificar e avaliar as ameaças à segurança; Definir as políticas e padrões que afetam a segurança; Alocar os recursos para suportar as atividades de gestão de risco; Incorporar os avanços técnicos no desenho e manutenção do equipamento; Investigar os acidentes e incidentes graves; Promover a segurança na aviação; Conduzir a monitorização e avaliação do programa de

segurança; Adoptar as práticas mais apropriadas à indústria; Atualizar os regulamentos de segurança na aviação civil (COSTA, 2008).

Nos Estados Unidos as estratégias de Sistemas eletrônicos e sistemas de comando, controle, defesa e segurança têm um papel muito importante no desenvolvimento da indústria, sendo que, os governos estão investindo cada vez mais nas indústrias, em cooperação com entidades de P&D militares e civis, e nos produtos que são usados para a defesa nacional. Portanto, com o desenvolvimento destes produtos os governos podem garantir as indústrias, encomendas públicas, equipando suas Forças Armadas e de segurança (VIANELLO, 2018).

As encomendas realizadas garantem o lucro e um controle de capital para as indústrias, buscando a inserção dos produtos que são fabricados no mercado externo, através de exportações (VIANELLO, 2018).

O Estado precisa direcionar a comercialização dos produtos eletrônicos de defesa, viabilizando financeiramente sua comercialização, com mecanismos públicos de apoio, como por exemplo, a redução de impostos, facilidades de financiamento e infraestrutura logística (BARROS et al., 2013).

Desta forma os maiores orçamentos de defesa se encontram em países como os Estados Unidos, China, Rússia, Reino Unido, Japão e França. O orçamento brasileiro está em 11º lugar no mundo, tanto em termos absolutos quanto também em percentual do produto interno bruto (PIB) (BARROS et al., 2013).

5. USO DE RADARES NOS SISTEMAS DE SIMULAÇÃO DE APRENDIZAGEM

O militar da guerra eletrônica pode analisar por meio dos parâmetros técnicos de um radar, qual é o radar que foi interceptado por seu sistema de MAGE, indicando o seu emprego operacional. Portanto, existem dois tipos de radares: os de onda contínua (CW) e os pulsados, sendo que, somente os radares pulsados serão considerados para efeito da objetividade.

Desta forma, os parâmetros técnicos de um radar são mais relevantes para configurar a emulação de radares no TS-100+: antena, pulso e faixas de frequência de operação (EZEQUIEL; OLYMPIO; EUPHRÁSIO, 2018).

É normal existirem restrições formais à comercialização de produtos e serviços incorporados as tecnologias nos países não alinhados politicamente e militarmente ao país detentor destas tecnologias. O Regime de Controle de Tecnologia de Mísseis, liderado pelos Estados Unidos, para os países que prometeram a não comercializar nem exportar mísseis capazes de portar armas de destruição (VIANELLO, 2018).

Neste sentido, o elevado conteúdo tecnológico dos produtos de defesa, faz com que o setor apresente maiores indicadores de agregação de valor, indicando que os investimentos em P&D de novos produtos deste setor se encontram viáveis economicamente (VIANELLO, 2018).

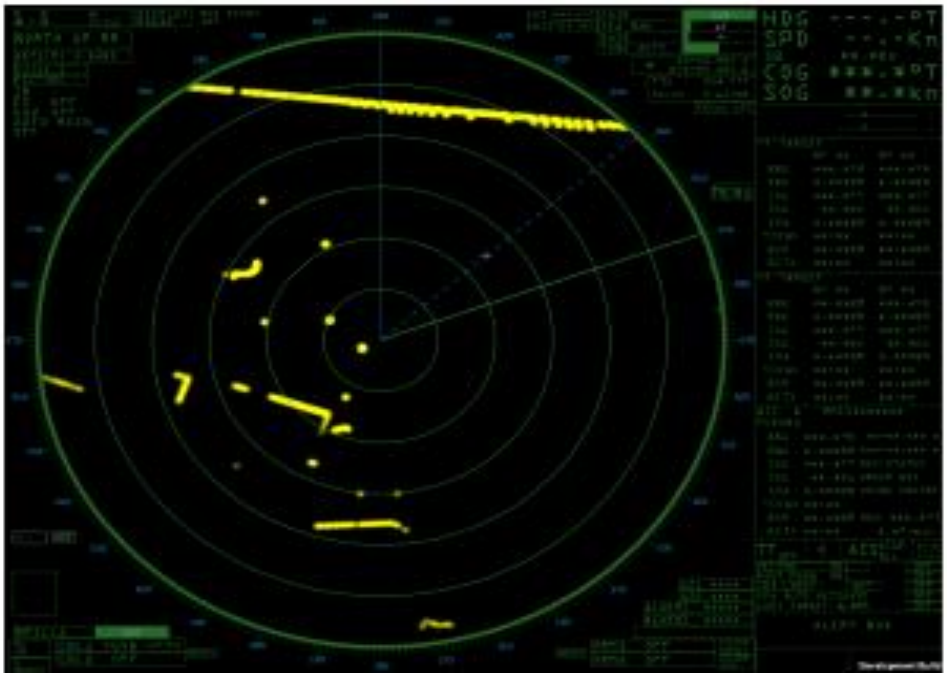
As empresas possuem vários projetos para criação de novos produtos, porém, estes projetos devem interessar o departamento de defesa, que solicitam uma versão de produto ajustada conforme suas necessidades. Este ajuste representa um projeto com duração maior que um ano.

Desta forma, a Odebrecht Defesa e Tecnologia (ODT) produz grande parte dos equipamentos de defesa, visando ampliar para outros lugares. A iniciativa pública é importante para o desenvolvimento deste e de outros parques tecnológicos do setor pelo país, contando com a ajuda de incentivos fiscais, apoio financeiro à pesquisa e fomentação de maior interação entre as universidades e as indústrias (VIANELLO, 2018).

O sistema que melhor garante segurança da navegação, por exemplo, é o simulador de radar ARPA (Automatic Radar Plotting Aids), sendo este destinado para uso em exercícios de treinamento dos operadores de radar. Na

figura 2, abaixo, apresenta-se o layout do radar simulado que é baseado em um radar real: o chamado Furuno FAR-2117(CUPERSCHMID; AMORIM; MATOS, 2015).

Figura 2: Captura de tela do simulador de radar, no Furuno FAR-2117.



Fonte: Adaptado de Cuperschmid; Amorim; Matos (2015).

O Furuno FAR-2117 é um radar que possui todas as funcionalidades necessárias para um amplo treinamento dos operadores de radar. Portanto, é fundamental que a apresentação quanto à interface de uso sejam semelhantes ao radar que o operador irá encontrar, criando certa familiaridade e automatismo (CUPERSCHMID; AMORIM; MATOS, 2015).

A interação do usuário com o sistema fundamental, sendo que, há duas maneiras de interação com usuário: mouse e teclado. O trackball do mouse permite o deslocamento do cursor pela tela, por outro lado o scrollwheel permite a mudança de valores numéricos. O teclado permite ligar/desligar diferentes elementos como, por exemplo, o transmissor, alarmes, mudar a escala de visualização e acesso ao menu (CUPERSCHMID; AMORIM; MATOS, 2015).

Desta forma, para poder simular o eco do radar, é fundamental haver uma malha 3D do cenário de navegação. O radar possui diversas

funcionalidades que estão na EBL, utilizada para obter marcações e a VRM utilizada para fazer medições de distância, ou seja, é uma circunferência, tracejada, que mede a distância do próprio navio até um alvo qualquer (CUPERSCHMID; AMORIM; MATOS, 2015).

O radar se comunica com a simulação através de troca de mensagens pela rede de conexões TCP e UDP. Esta conexão é feita no momento em que o radar se conecta como um cliente e se inscreve para receber mensagens sobre a posição do navio, seu aproamento e velocidade. Desta forma, o módulo do Radar possui a capacidade de receber e processar mensagens em formato NMEA [2], permitindo a interoperabilidade com outros simuladores que usam este padrão para se comunicar (CUPERSCHMID; AMORIM; MATOS, 2015).

O sistema de radar é usado para alertar a aproximação de aeronaves inimigas, portanto, o emprego de sinais eletromagnéticos, é desenvolvido pelas doutrinas voltadas para o ramo das NCom. Surgiram também o ESM l, e o ELINT em um contexto estratégico, e por fim o MAGE.

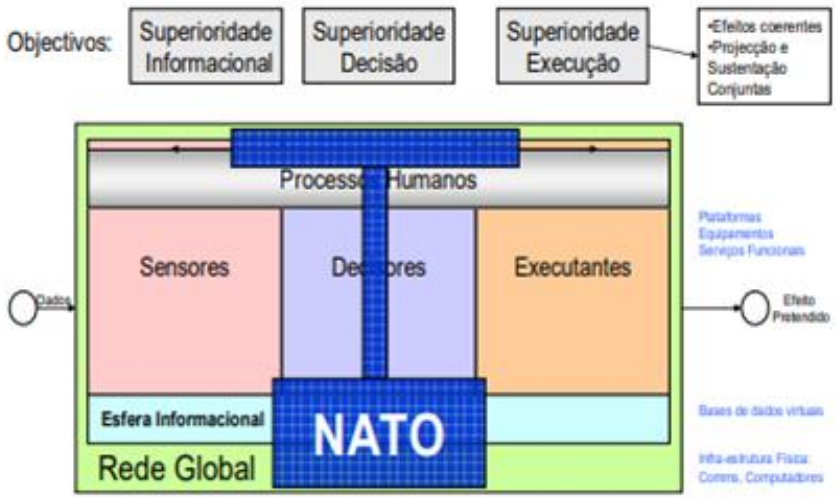
Desta forma, o desenvolvimento de equipamentos de MAGE precisa de meios para atender toda essa demanda usando de ferramentas de simulação de sinais radar, sendo que, um dos equipamentos utilizado é o Simulador de Ameaça TS-100+ (Excalibur), pertencente à Força Aérea Brasileira. Portanto, para realizar as aplicações do TS100+, é importante conhecer os parâmetros técnicos de um radar a serem usados na simulação, nos aspectos dos sistemas de MAGE NCom a serem alvo de avaliação e sobre o funcionamento do TS-100+.

5.1 O CONCEITO NATO NETWORK ENABLED CAPABILITY (NNEC)

O NNEC se adapta ao modelo britânico, originando-se da relação entre a ligação de sensores, e também pela sua capacidade operacional NATO, que se matem centrada em rede. Para transformar a informação num potencial de combate, se projeta o emprego e a sustentação de conjuntos de forças (SANTOS, 2007).

Nesse sentido, na figura 3 apresenta-se uma representação da NNEC, conforme Santos (2007)

Figura 3: Representação da NNEC.



Fonte: Adaptado de Santos (2007).

Os sensores, conforme a figura acima, se dividem entre sensores humanos ou tecnológicos, mas somente são considerados os sensores tecnológicos durante a investigação. A rede global se forma pela infraestrutura, que conta com computadores e sistemas de comunicação, para disponibilizar a capacidade física de plug-and-play1, atingindo assim, a conectividade entre as entidades participantes (SANTOS, 2007).

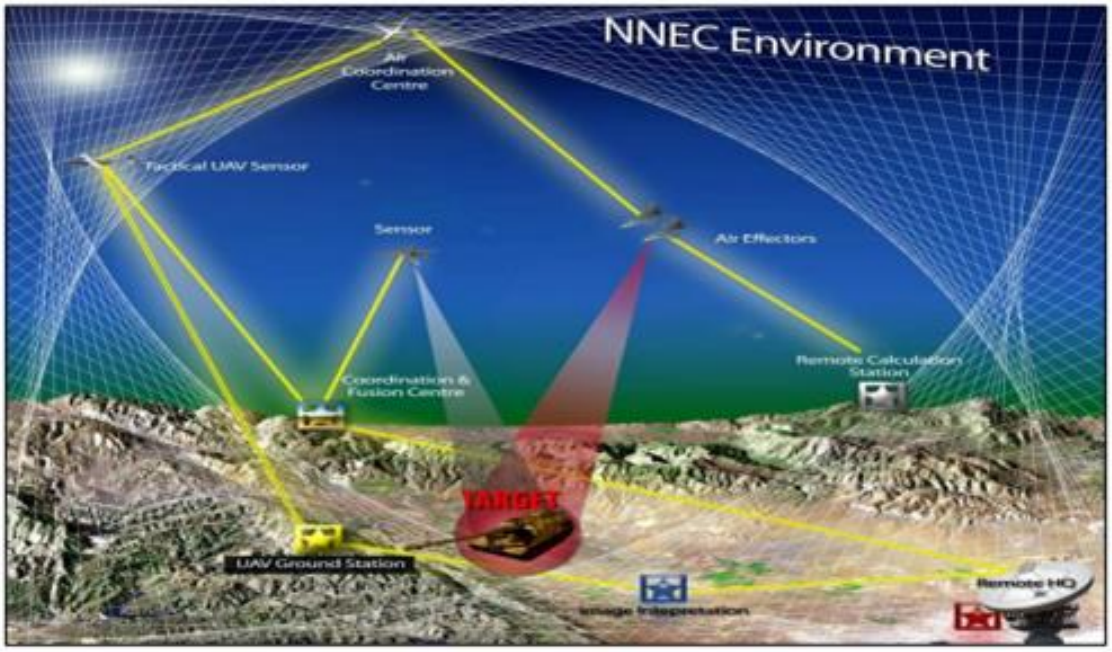
Neste sentido, toda esta estrutura de redes possui largura de banda suficiente para executar as operações em todo o espectro, especialmente para as agências nacionais, internacionais e não governamentais (VICENTE, 2005).

O NNEC é recomendado pelas nações aliadas, considerado, o mais adequado para as operações militares. Portanto, o caminho para as nações é de investir mais nas tecnologias da informação na GCR, para ajudar as forças multinacionais.

Desta forma, o ambiente da NNEC é adequado, para a aproximação das futuras operações, para implementar novas estruturas, para a flexibilidade e a agilidade, que conduzem as operações da GCR.

Nesse sentido, na figura 4 apresenta-se uma imagem do ambiente da NNEC.

Figura 4: Ambiente da NNEC.



Fonte: Adaptado de Santos (2007).

Neste sentido, Nato (2006) coloca alguns atributos potenciadores do conceito NNEC:

- Uma rede que coloca fim no “núcleo protegido” para comunicações em voz, dados e vídeo;
- Numa tecnologia de mensagens, que transferem os dados;
- Ferramentas adaptadas à realidade operacional;
- Comunidades de Interesse que devem ser identificadas;
- Ferramentas avançadas;
- Mais sensores de partilha de informação em todos os níveis de atividade;
- Informação passada para os utilizadores, aplicações e ligadas sobre domínios, ou seja, nos atributos que refletem numa imagem do que o conceito NNEC;
- Países que desejam participar das futuras forças da NATO devem estar conscientes, dos grupos de trabalho já existentes ou em formação, que tem como principal objetivo de definir requisitos

técnicos, estruturantes para as capacidades de força em ambiente NNEC.

5.2 AS VANTAGENS DOS SISTEMAS DE SIMULAÇÃO NO APRENDIZADO DE RADARES NA GUERRA ELETRÔNICA

De um modo me geral, os simuladores de hoje são indispensáveis para a formação de pilotos, especialmente devido aos elevados custos para este processo de treinamento. Um dos principais motivos está relacionado com o aumento dos combustíveis que são fundamentais para o funcionamento das aeronaves. Dessa forma, os simuladores são amplamente utilizados no treino de pilotos, tripulações, dentre outros (COSTA, 2008).

Os simuladores são importantes na formação de pilotos e ATC, sendo que, alguns simuladores já permitem o treino conjunto de alunos, mesmo em manobras de aproximação a aeroportos para estes treinamentos. Os simuladores de voo reduzem os custos operacionais de poluição atmosférica e sonora, também poupam combustíveis e diminuem os distúrbios ambientais (COSTA, 2008).

Neste sentido, ainda existem algumas vantagens que vão depender das condições atmosféricas ou congestionamento do espaço aéreo, possibilidade de interrupção do exercício conforme o desejado pelo instrutor, treino de emergência que de outra forma não seria possível de realizar sem colocar em risco pessoas e bens (OLIVEIRA, 2005).

Segundo Gomes (2013) depois de adquirir um simulador deve-se analisar os simuladores que poderiam ser adquiridos para atender às necessidades do CIGE. O desenvolvimento de um simulador próprio, para atender às necessidades nacionais, foi o mais apropriado (BRASIL, 2011).

Desta forma, o primeiro simulador adquirido foi em 2012, com o objetivo de construção de um software simulador baseado em ambiente virtual, a fim de atender as necessidades dos recursos humanos para executar ações de proteção cibernética e defesa ativa (GOMES, 2013).

Desta forma a Seção de Cibernética estabeleceu novas funções de automatização e apoio ao instrutor. Portanto, o simulador do CIGE é um software que permite através da tecnologia de virtualização, a configuração e

administração de redes de computadores, proporcionando um ambiente educacional para treinamento de operações cibernéticas de ataque e defesa às redes, sistemas operacionais instaladas nas máquinas demais dispositivos existentes na rede (GOMES, 2013).

Conforme Matsuura (1995) as vantagens do simulador são: A redução do custo de formação e treino de pessoal; A redução do tempo de formação e treino do pessoal; O aumento de segurança; O aumento de janela de oportunidade para um treino em voo.

Desta forma, os simuladores não tem tanta manutenção ou tanto combustível como uma aeronave real, representando um investimento para a grande maioria das escolas de aviação em Portugal (OLIVEIRA, 2005).

Os programas que reproduzem o comportamento de um ambiente real num ambiente computacional são denominados de simuladores virtuais. Para que esta simulação seja real, é fundamental que todos os modelos de comportamento do fenômeno a ser reproduzido sejam conhecidos (BASTOS; CARVALHO; SILVA, LIMA; DUARTE, 2018).

Desta forma, quanto mais conhecido for o modelo, ou seja, quanto mais informações sobre o fenômeno tiver, mais fiel será o comportamento no mundo virtual. Portanto, os simuladores são empregados para gerar conhecimento prévio sobre um determinado sistema, auxiliando na tomada de decisões, permitindo a viabilidade de um processo, possibilitando a redução de custos e riscos no processo produtivo.

A informação é muito importante no campo de batalha, e os Serviços de Inteligência Militar fornecem necessárias para uma vitória sem muitas perdas. Portanto, a Inteligência de Sinais, se relaciona com as atividades de Guerra Eletrônica (EZEQUIEL; OLYMPIO; EUPHRÁSIO, 2018).

5.3 USO DO PLANO ESTRATÉGICO ELETRÔNICO EM GRANDES EVENTOS

As Forças Armadas brasileiras foram orientadas para trabalhar na Copa do Mundo FIFA Brasil 2014, para isso foi criado um Plano Estratégico de Segurança, com objetivo de prever e coibir ameaças à população em geral. O Exército Brasileiro participou deste evento, sendo que, foram empregadas as

variadas células do Estado-Maior em operações nas cidades-sede. Destas células, as mais importantes eram as ações de Guerra Eletrônica, que fornecem dados importantes e estratégicos sobre os sistemas eletrônicos durante o evento.

Desta forma, as ações de Guerra Eletrônica ocorreram de forma bastante dinâmica, ou seja, coletando dados a fim de ratificar ou retificar condutas em tempo real. Portanto, neste trabalho apresentaram-se os conceitos e a composição da célula de Operações de Informação, voltados para Operações Militares, Operações de Informação e emprego de Guerra Eletrônica.

O objetivo principal deste trabalho foi de analisar as características e aspectos do emprego da Guerra Eletrônica, com o intuito de retificar ou ratificar os manuais no que diz respeito às informações. Verificou-se que a Guerra Eletrônica seria bem aplicada no planejamento e na condução das operações.

Um estudo mais aprofundado é necessário no contexto das Operações de Apoio a Órgãos Governamentais, que devem ter as seguintes responsabilidades de acordo com o (EXÉRCITO BRASILEIRO, 2014):

> Integrar, coordenar e sincronizar todas as CRI e recursos relacionados às Op Info disponíveis com as funções de combate; Selecionar, analisar e priorizar alvos e indicar meios “não letais”, “menos letais” ou “letais”; Planejar e acompanhar a condução das Op Info aprovadas pelo Cmt - Fornecer requisitos de informação para o plano de obtenção de Inteligência, e Fornecer requisitos de informação para o plano de Medidas de Ataque Eletrônico. (EXÉRCITO BRASILEIRO, 2014, p. 5-8).

Desta forma, as ações de Guerra Eletrônica ainda demandam de melhor orientação quanto à sua respectiva forma de atuação, sendo que, os manuais de Operações e Operações da Informação proporcionam subsídios para o entendimento das atividades, porém, não existe definição concreta de quem faz cada atividade. É muito importante à realização de novos estudos sobre o emprego da Guerra Eletrônica na célula de Operação de Informação.

5.4 SIMULAÇÕES DE TRÁFEGO AÉREO BRASILEIRO

As simulações de tráfego aéreo no contexto brasileiro foram recentemente normatizadas por meio da Portaria DECEA – Departamento de Controle de Espaço Aéreo, nº 201/DGCEA/2016, onde a mesma foi criada com a finalidade de estabelecer processos, critérios e requisitos para a aplicação da simulação ATM (Gerenciamento de Tráfego Aéreo) no SISCEAB (Sistema de Controle do Espaço Aéreo Brasileiro).

Nesse sentido, verifica-se que a capacitação ATC se caracteriza por um processo de aprendizagem que tem por objetivo proporcionar os conhecimentos, habilidades e atitudes a um profissional, de modo a desenvolver sua competência para o desempenho das atribuições de suas funções técnico-operacionais (MINISTÉRIO DA DEFESA, 2016).

O ensaio ATM, por sua vez se dá pela aplicação de simulação com vistas à avaliação crítica para a implementação de mudanças ou de novas tecnologias relacionadas ao ATM, procedimentos de navegação aérea, conceito de espaço aéreo ou fluxo de tráfego aéreo. Por outro lado, a simulação ATM (Simulação de Tráfego Aéreo) é caracterizada pelo processo de reproduzir em um modelo computacional o ambiente operacional de um ou mais órgãos ATC, de determinada porção do espaço aéreo e seu fluxo de tráfego aéreo ou, ainda, o meio ambiente da cabina de pilotagem de um determinado tipo de aeronave a fim de realizar capacitação ATC, treinamento ATC ou ensaio ATM (MINISTÉRIO DA DEFESA, 2016).

Nesse sentido, conforme o Ministério da Defesa, as simulações se dão especialmente de duas formas, sendo em tempo real e tempo acelerado, conforme abaixo:

.

> SIMULAÇÃO EM TEMPO REAL Processo baseado em um sistema computacional no qual um ambiente operacional é reproduzido em tempo real, cujo objetivo principal é a observação da influência do ATCO no cenário proposto. SIMULAÇÃO EM TEMPO ACELERADO Processo baseado em um sistema computacional no qual um ambiente operacional é reproduzido em tempo acelerado, sem a influência direta das intervenções táticas do ATCO e cujas decisões são baseadas em regras que controlam as ações simuladas nos cenários em estudo. (MINISTÉRIO DA DEFESA, 2016, p. 10).

De um modo em geral, a STA e STR diferem em termos de custo, realismo, complexidade, tempo e número de amostras de tráfego e de casos de

teste. Quanto mais completo o método de simulação utilizado, maior o seu custo e maior a necessidade de tempo para a preparação e execução, porém, mais próximos da realidade ficarão os resultados adquiridos. No entanto, em geral, por razões de custo/tempo, o número de amostras de tráfego ou casos de teste tende a diminuir com o aumento da complexidade do método de simulação utilizado (MINISTÉRIO DA DEFESA, 2016).

Dessa forma, apresenta-se na figura 2 um comparativo de benefícios e limitações do processo de simulação em tempo real, conforme o Ministério da Defesa (2016).

Figura 5: Benefícios e limitações da STA e da STR.

SIMULAÇÃO EM TEMPO REAL	
Benefícios	**Limitações**
• Método de simulação mais próximo às operações ATM reais, que pode ser utilizado para avaliar e validar os objetivos da simulação; • Oferece oportunidade para coletar dados quantitativos e qualitativos de alto grau de confiabilidade; • Informação dos ATCO baseada em sua experiência operacional (avaliação qualitativa adicional); • Informação dos pseudopilotos em função de sua perícia e das condições de simulação; • Pode indicar e avaliar questões relacionadas com o desempenho dos fatores humanos (avaliação quantitativa e qualitativa adicional); • Coleta automática de dados (para uma avaliação quantitativa); • Alcance ilimitado e maior flexibilidade em comparação com os ensaios reais (avaliação qualitativa adicional); • Sem risco à operação real; • Permite comprovar os procedimentos de contingência e a análise de risco (avaliação qualitativa e quantitativa); • Facilidade para avaliar várias alternativas; • Informação instantânea e adaptação ao cenário operacional (avaliação qualitativa); • Pode utilizar dados reais de tráfego aéreo e ambiente operacional (dados quantitativos); • Boa aceitação dos resultados pelos ATCO (avaliação qualitativa de grande alcance); • Permite aos ATCO se familiarizarem com as mudanças propostas; • Pode ser parte de um fundamento da segurança operacional.	• Alto custo e necessidade de tempo; • Pode exigir muitos recursos; • Capacidades limitadas da interface homem-máquina (IHM), transmissão simulada por rádio e performance limitada dos sistemas de vigilância ATS; • Performance limitada da aeronave e comportamento simplificado da mesma; • Comportamento pouco realista da aeronave devido a pseudopilotos com pouca ou nenhuma experiência em aviação; • Os pseudopilotos não podem reproduzir o desempenho real dos equipamentos; • Baixa representação das condições meteorológicas; • Questões relacionadas ao desempenho dos fatores humanos (durante a simulação): • Mentalidade/ atitude do ATCO; • Capacidade do ATCO; • Curva de aprendizagem do exercício/ cenário; • Subjetividade da avaliação (principalmente com relação à carga de trabalho); • Resultados provenientes da simulação influenciadas experiência anterior do ATCO. • Dificuldades de planejamento relacionadas com a disponibilidade dos ATCO para a simulação; e • Dificuldade de intervenção dos usuários do espaço aéreo.

Fonte: Adaptado de Ministério da Defesa (2016).

Já na figura 3, apresenta-se um comparativo de benefícios e limitações do processo de simulação em tempo acelerado, conforme o Ministério da Defesa (2016).

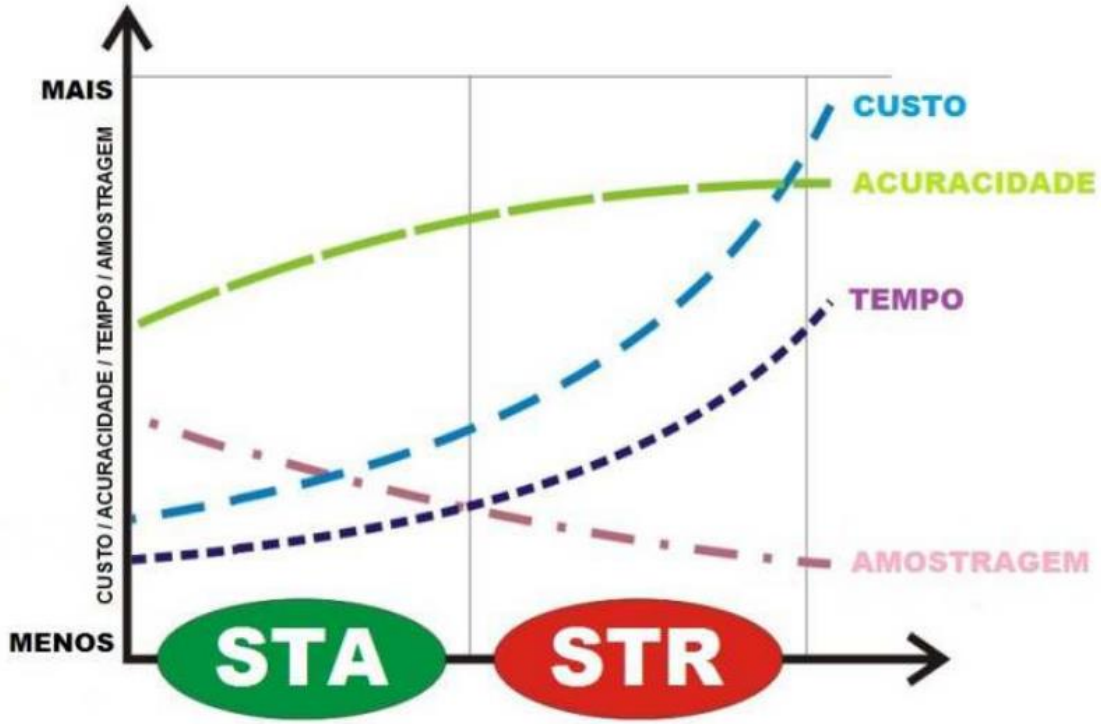
Figura 6: Benefícios e limitações da STA e da STR.

SIMULAÇÃO EM TEMPO ACELERADO	
Benefícios	**Limitações**
• Custo de operação relativamente baixo; • Um dos métodos mais utilizados nas avaliações da capacidade de espaço aéreo e aeroportos; • Oportunidade para coletar dados qualitativos; • Alcance relativamente ilimitado e com grande flexibilidade; • Facilidade relativa para avaliar várias alternativas; • Adaptação relativamente simples a casos de teste; • Relativamente fácil testar um grande número de amostras de tráfego aéreo; • Pode utilizar dados reais sobre tráfego aéreo e ambiente operacional; • Boa aceitação dos resultados; • Pode avaliar o sucesso do nível desejado de segurança operacional (TLS); e • Pode informar a evolução do fundamento da segurança operacional.	• Modelo simplificado de operação "real"; • Somente proporciona dados estatísticos; • Não pode reproduzir as intervenções táticas do controlador; • A qualidade dos resultados depende consideravelmente da precisão do modelo; • Performance limitada da aeronave e comportamento simplificado da mesma; • Baixa representação das condições meteorológicas; e • Dificuldade de intervenção dos usuários do espaço aéreo.

Fonte: Adaptado de Ministério da Defesa (2016).

Já na figura 4 é apresentado um gráfico comparativo entre a STA e STR que mostra as diferentes entre ambas relacionadas ao custo, acuracidade, tempo e amostragem.

Figura 7: Comparação entre STR e STA.



Fonte: Adaptado de Ministério da Defesa (2016).

O gráfico mostra que o STA apresenta menor custo, tempo, acuracidade e maior amostragem em relação ao STR.

6. CONSIDERAÇÕES FINAIS

O presente estudo se propôs a realização uma breve avaliação da importância do desenvolvimento e utilização de sistemas de simulação no aprendizado de radares e guerra eletrônica. Dessa forma, com o mesmo, acredita-se que seja possível ampliar o conhecimento nesta área e contextualizar seus aspectos e aplicações no aprendizado e desenvolvimento dos sistemas de simulação com a finalidade de usar radares na guerra eletrônica.

Verificou-se então que os simuladores são ferramentas especialmente adequadas para qualificar os treinamentos de futuros combatentes inclusive no aspecto cibernético.

De um modo em geral, um ambiente simulado quando utilizado para as técnicas de segurança é muito importante, e fundamental, considerando também a utilização de redes em produção, que trabalham com técnicas que relacionam a segurança da informação e das comunicações, especialmente quando estas serão aplicadas numa situação real.

A Guerra Centrada em Redes, por sua vez, possui a capacidade de ampliar a projeção das forças e de alcance, mantendo um fluxo de informações interações. Neste sentido, a capacidade de sincronizar as ações, aumentar a velocidade sobre uma estrutura de rede robusta pode ser maximizada pelo chamado “Poder da Capilaridade”.

Portanto, os simuladores são empregados para gerar conhecimento prévio sobre um determinado sistema, auxiliando na tomada de decisões, permitindo a viabilidade de um processo, possibilitando a redução de custos e riscos no processo produtivo. Ainda, de um modo me geral, os simuladores de hoje são indispensáveis para a formação de pilotos, especialmente devido aos elevados custos para este processo de treinamento.

Desse modo, constatada a sua importância, verifica-se que nas operações militares brasileiras a preocupação com a guerra eletrônica vem crescendo cada vez mais, sendo que, está hoje é vista como um instrumento que obtém informações importantes com praticamente todos os elementos de combate. Nesse sentido, acredita-se que as informações obtidas por meio da

guerra eletrônica são fundamentais para a tomada de decisão do comandante do escalão, operacional ou tático.

As principais vantagens constatadas para os simuladores no aprendizado de radares e guerra eletrônica são relacionados à redução do custo de formação e treino de pessoal; a redução do tempo de formação e treino do pessoal; o aumento de segurança; o aumento de janela de oportunidade para um treino em voo; reduzem os custos operacionais de poluição atmosférica e sonora; poupam combustíveis e diminuem os distúrbios ambientais, dentre outros.

Por fim, diante da complexidade e importância do tema, bem como, das limitações da presente pesquisa, sugere-se a continuidade nos estudos sobre o tema, com desenvolvimento de trabalhos futuros que proporcionem uma maior contextualização sobre o tema, de forma a contribuir com o meio acadêmico e profissional da área.

REFERENCIAS

ALBERTS, D. S., (2003a). **Network Centric Warfare**: Developing and Leveraging Information Superiority. Washington D.C.: CCRP.

ALBERTS, D. S.; HAYES, R. E. **Power to the edges: command andcontrol in the information age**. Washington: DoD CCRP, 2005.

ALBERTS, D. S. **NEC2 short course: Module 1**. DoD CCRP, 2009.

BARROS, D. C. et al. **Panorama sobre a indústria de defesa e segurança no Brasil.** Rio de Janeiro: BNDES, 2013.

BRASIL. **Ministério da Defesa. Estratégia Nacional de Defesa.** 2. ed. Brasília: Ministério da Defesa, 2008.

BRASIL. C 34-1: **Emprego da Guerra Eletrônica**, 2. ed. Brasília, DF: EME, 2009.

BRASIL. **Ministério da Defesa. Edital do pregão eletrônico.** *28.* Brasília: SALC, base administrativa do Centro de Comunicações e Guerra Eletrônica do Exército, 2011.

BASTOS, F. A. C; CARVALHO, B. C; SILVA, J. A. N; LIMA, D. A; DUARTE, J. C. **Simulador de Guerra Eletrônica Não-Com Utilizando Modelagem de Emissões de Radar**. Rio de janeiro, 2018. Disponível em: <http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_03.pdf>. Acesso em: 08. Jul. 2019.

BRICK, E. S. **As forças armadas e a base logística de defesa.** Marít. Bras. Rio de Janeiro v. 134 n. 01/03 p. 1-320 jan. / mar. 2014. Disponível em: < http://www.revistamaritima.com.br/sites/default/files/rmb-1-2014.pdf >. Acesso em: 09. Jul. 2019.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war: the next threat to national security and what to do about it**. 1 ed. New York: Harper Collins Publishers, 2010.

COSTA, J. A. M. **A Importância dos Simuladores na Formação de Pilotos e CTA´S e Seu Impacte na Segurança de Voo.** Covilhã Agosto, 2008. Disponívelem:<https://ubibliorum.ubi.pt/bitstream/10400.6/3636/1/Tese%20M1803%20Jorge%20da%20Costa.pdf>. Acesso em: 08. Jul. 2019.

CUPERSCHMID, A. R. M; AMORIM, J. A; MATOS, C. E. A. B. **Uso de realidade aumentada para o treinamento militar.** 2015. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2015/RMCT_187_E8A_13.pdf>. Acesso em: 09. Jul. 2019.

DE SOUZA, R. C. P. **Sistema integrado de monitoramento de fronteiras (SISFRON): concepção estratégica e estrutura**. Palestra [16 ago.2011]. Rio de Janeiro: Escola de Comando de Estado-Maior.

EXÉRCITO BRASILEIRO. **Estado-Maior. EB20-MC-10.103:** Operações. Brasília, DF: EME, 2014.

EZEQUIEL, S. B., OLYMPIO, L. C., EUPHRÁSIO, P. C. S. **aplicações do simulador de ameaça ts-100+ (excalibur) em equipamentos de medidas de apoio à guerra eletrônica de não comunicações de interesse do exército brasileiro.** 2018. Disponível em: < http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_06.pdf >. Acesso em: 09. Jul. 2019.

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** São Paulo: ATLAS, 2014.

GOMES, R. **Simulador de operações de guerra cibernética.** Palestra, 2013.

GOMIDE, R. **Exército treina para Garantia da Lei e da Ordem e ‘guerra no meio do povo’.** iG, Rio de Janeiro, 27/08/2012.

HARZ, C. (2005). **Network Centric Warfare:** Allied Progress [em linha]. [Sine loco]: 6 Sense Newsletter.

HOBBINS, W. T. (2005). **Airmen on the Battlefield:** Warfighting Integration in Support of Special Operations Forces [em linha]. [Sine loco]: Air & Space Power Journal - Spring 2005.

KAP, K. M. **The Gamification of Learning and Instruction:** Game-based Methods and Strategies for Training and Education. Wiley.com, 2012.

MACHADO, A. F. A. **Utilização de simuladores para a formação de guerreiros cibernéticos.** 2016. Disponível em: **<**https://webcache.googleusercontent.com/search?q=cache:cfsenbWzckEJ:https://www.publicacoesacademicas.uniceub.br/gti/article/download/4322/3635+&cd=2&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 08. Jul. 2019.

MATSUURA, J. **Aplicação dos Simuladores de Voo no Desenvolvimento e Avaliação de Aeronaves e Periféricos**. São José dos Campos, Centro Técnico Aeroespacial – Instituto Tecnológico de Aeronáutica, 1995.

MINISTÉRIO DA DEFESA. Comando da Aeronáutica Departamento de Controle do Espaço Aéreo. **Portaria DECEA No 201/DGCEA,** de 08 de Setembro de 2016. Aprova a edição da ICA 100-42, que trata da “Simulação ATM no Âmbito do SISCEAB”.

NATO, A. **Command for Transformation** (2006). NATO NNEC Roadmap (Working Draft - version 3.0). Norfolk: NATO.

OLIVEIRA, P. **Os simuladores e as TI para a formação do pessoal aeronáutico,** ISCTE, Lisboa, 2005.

PHISTER, P. W. (2004). **Aplicações militares das tecnologias da informação** [em linha]. [Sine loco]: ASPJ Em Português 4º trimestre de 2004.

SANT' ANA JÚNIOR, B. **Escola de comando e estado-maior do exército/escola marechal Castello branco.** Rio de janeiro, 2012. Disponível em:<http://webcache.googleusercontent.com/search?q=cache:http://www.eceme.eb.mil.br/images/IMM/producao_cientifica/dissertacoes/dissertacao-de-mestrado-eceme-maj-sant-ana-jnior.pdf>. Acesso em: 08. Jul. 2019.

SANTOS, P. A. S. **O Conceito "Guerra Centrada Em Rede" E A Modernização Dos Sistemas De Armas Da Força Aérea Portuguesa**. Lisboa 2007. Disponível em: < https://comum.rcaap.pt/bitstream/10400.26/12629/1/TII_CAP%20PAULO%20SANTOS%20%28NAV%29.pdf >. Acesso em: 11. Set. 2019.

SILVA, W. A. L. A **Guerra eletrônica nas operações de informação em grandes eventos: copa do mundo Fifa brasil 2014** - cidade – sede recife/pe. Brasília 2017. Disponível em: < http://bdex.eb.mil.br/jspui/bitstream/1/919/1/TCC%20Leal%20%2820JUL%29%20FINAL%20REVISADO.pdf >. Acesso em: 09. Jul. 2019.

WETZEL, R., et al. **Designing Mobile Aumented Reality Games.** In: B. Furht (Ed.), Handbook of Augmented Reality. New York: Springer New York, chap. 25, p. 513-539, 2011.

VIANELLO, J. M. **Sistemas eletrônicos e sistemas de comando e controle.** IPEA, 2018. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/160706_livro_mapeamento_defesa_capitulo_02.pdf>. Acesso em: 08. Jul. 2019.

VICENTE, J. P. N. (2006). A (R). **Evolução do Pensamento Estratégico** [em linha]. [Sine loco]: ASPJ Em Português 2º trimestre de 2006.