UNIVERSIDADE DA FORÇA AÉREA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS

GLAUCIO DA ROCHA **SILVEIRA,** 1° Ten QOENG CMP

A segurança e a defesa cibernética no Brasil: uma contribuição para o Poder Aeroespacial

Rio de Janeiro
2019

UNIVERSIDADE DA FORÇA AÉREA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS

GLAUCIO DA ROCHA **SILVEIRA,** 1° Ten QOENG CMP

A segurança e a defesa cibernética no Brasil: uma contribuição para o Poder Aeroespacial

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea, como requisito parcial para obtenção do título de Mestre em Ciências Aeroespaciais.

Orientador: Prof. Dr. Carlos Cesar de Castro Deonisio

Rio de Janeiro
2019

Ficha catalográfica elaborada pela Biblioteca da UNIFA

Silveira, Glaucio da Rocha.

S587 A segurança e defesa cibernética no Brasil: uma contribuição para o poder aeroespacial / Glaucio da Rocha Silveira. – Rio de Janeiro: Universidade da Força Aérea, 2019.

77 f.: il., enc.

Orientador: Carlos Cesar de Castro Deonísio

Dissertação (mestrado) – Universidade da Força Aérea, Rio de Janeiro, 2019.

Referências: f. 72 - 77.

1. Segurança e defesa. 2. Guerra cibernética. 3. Poder aeroespacial. I. Título. II. Deonísio, Carlos Cesar de Castro. III. Universidade da Força Aérea.

CDU 623.4(08):351.814

UNIVERSIDADE DA FORÇA AÉREA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS

GLAUCIO DA ROCHA SILVEIRA

A SEGURANÇA E A DEFESA CIBERNÉTICA NO BRASIL: UMA CONTRIBUIÇÃO PARA O PODER AEROESPACIAL

Dissertação aprovada pelos membros da Banca Examinadora, no dia 11 de dezembro de 2019, como requisito parcial à obtenção do título de Mestre em Ciências Aeroespaciais pela Universidade da Força Aérea.

Rio de Janeiro, RJ, 11 de dezembro de 2019.

BANCA EXAMINADORA

Prof. Dr. CARLOS CESAR DE CASTRO DEONISIO - UNIFA
Presidente da Banca Examinadora

Prof. Dr. PEDRO ARTHUR LINHARES LIMA – UNIFA

Prof. Dr. NIVAL NUNES DE ALMEIDA – EGN

Profª. Me. CONSTANÇA MARIA MAIA ARRUDA – CCA-RJ

Dedicatória

Dedico este trabalho aos meus pais Guilherme (in memorian) e Sônia, pela educação, dedicação e incentivo aos estudos. A minha mada esposa Maira, por toda paciência, carinho, amor e por todos os momentos que lhe foram suprimidos. Aos meus filhos Grazieli e Guilherme por todo apoio e incentivo.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, pela proteção. Ao Brig Int. Linhares pelo apoio e confiança para o ingresso nesta jornada. Ao meu Orientador, Prof. Doutor Deonísio por todo convívio, confiança e dedicação ao longo do presente trabalho. Aos amigos da turma 2014, que muito me ajudaram nas pesquisas e aconselhamentos. Em especial ao amigo e irmão José Barbosa da Silva Filho que, em todos os momentos, sempre esteve ao meu lado.

A sabedoria suprema é ter sonhos bastante grandes para não se perderem de vista enquanto os perseguimos.

(FAULKNER, William, 1929)

Progresso impõe não apenas novas possibilidades para o futuro, mas novas restrições.

(Norbert Wiener)

RESUMO

A evolução trazida pela Tecnologia da Informação e Comunicações, especialmente por meio de pesquisas militares nos anos 50 e 60, deu origem à Internet. Em meados dos anos 90 ocorreu a revolução da internet, quando a rede foi aberta ao público em geral. Tal condição trouxe à tona a Era da Informação, que atualmente, já começa a dar lugar à Era do Conhecimento. Entretanto esta situação, ao mesmo tempo em que agilizou muitos processos decisórios e permitiu a circulação de informações quase que instantaneamente, tornou as pessoas, instituições e Estados altamente vulneráveis a um novo tipo de ameaça, a cibernética, que independe de fronteiras e tem alto potencial destrutivo, podendo atingir setores financeiros, infraestruturas críticas, chegando até o limite de matar pessoas. O setor cibernético constitui-se em um novo e promissor teatro de operações, onde além da guerra entre nações, encontramos a prática de diversos ilícitos, incluindo o ciberterrorismo. O presente estudo tem como objetivo auxiliar na compreensão de alguns princípios da guerra cibernética, especialmente o que cita que ela não faz sentido se não causar impactos no mundo real, fato que necessariamente engloba o Poder Aeroespacial. Visando atingir este fim, o trabalho valeu-se de uma pesquisa exploratória e descritiva. Por fim, destaca-se que o espaço cibernético ainda necessita ser explorado, pois visualiza-se sua enorme capacidade de transformar as relações de poder entre países e, consequentemente, as relações internacionais. Diferentemente do ocorrido durante a Guerra Fria, a corrida no espaço cibernético não se restringe às grandes potências, mas se vale de diversos atores de menor ou nenhuma expressão no cenário internacional. Conclui-se que há a necessidade de desenvolvimento de políticas capazes de auxiliar na promoção da segurança dos sistemas cibernéticos e híbridos do Poder Aeroespacial.

Palavras-chave: Guerra Moderna. Guerra Cibernética. Ciberespaço. Segurança Internacional.

ABSTRACT

The evolution brought by Information and Communications Technology, especially through military research in the 50s and 60s, gave rise to the Internet. In the mid-90s the internet revolution took place, when the network was opened to the general public. This condition brought to light the Information Age, which is now beginning to give way to the Knowledge Age. However, this situation, while streamlining many decision-making processes and allowing the circulation of information almost instantly, has made people, institutions and states highly vulnerable to a new type of threat, cybernetics, which is borderless and has high potential. destructive, reaching financial sectors, critical infrastructure, reaching the limit of killing people. The cyber sector is a new and promising theater of operations, where in addition to the war between nations, we find the practice of several illegal acts, including cyberterrorism. The present study aims to assist the understanding of some principles of cyber warfare, especially that it says that it does not make sense if it does not impact the real world, a fact that necessarily encompasses Aerospace Power. In order to achieve this end, the work used exploratory and descriptive research. Finally, it is highlighted that the cyber space still needs to be explored, as its enormous capacity to transform power relations between countries and, consequently, international relations, can be seen. Unlike what happened during the Cold War, the race in cyberspace is not restricted to the great powers, but it uses several actors of lesser or no expression on the international scene. It is concluded that there is a need to develop policies capable of assisting in promoting cyber security of Aerospace Power's cybernetic and hybrid systems.
Keywords: Modern War. Cyberwar. Cyberspace. International security.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

ABIN – Agência Brasileira de Inteligência

APF – Administração pública federal

ARPANET – Advanced Research Projects Agency Network

C^2 – Comando e Controle

CCMD – Comando Unificado de Combatentes

CDCiber – Centro de Defesa Cibernética do Exército

CDN – Conselho de Defesa Nacional

ComDCiber – Comando de Defesa Cibernética

CREDEN – Câmara de Relações Exteriores e Defesa Nacional

CSIRT – Computer Security Incident Response Team

DCA – Diretriz do Comando da Aeronáutica

DGE – Departamento de Gestão e Ensino

DoD – Departamento de Defesa dos Estados Unidos da América

ECMj – Estado-Maior Conjunto

EMCFA – Estado-Maior Conjunto das Forças Armadas

ENaDCiber – Escola Nacional de Defesa Cibernética

END – Estratégia Nacional de Defesa

ENEE – Encontro Nacional de Estudos Estratégicos

FA – Forças Armadas

GSI/PR – Gabinete de Segurança Institucional da Presidência da República

KdoCIR - Comando do Espaço Cibernético e de Informação

LBDN – Livro Branco de Defesa Nacional

MD – Ministério da Defesa

NSA – *National Security Agency*

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PEECFA – Planos Estratégicos de Emprego Conjunto das Forças Armadas

PNAD – Pesquisa Nacional por Amostra de Domicílios

SCTIC2 – Sistema de Comunicações e Tecnologia da Informação para Comando e Controle

SIC – Segurança da Informação e Comunicações

SisBin – Sistema Brasileiro de Inteligência

TIC – Tecnologia da Informação e Comunicações

USCyberCom – Comando de Defesa Cibernética Norte-Americano

USStratCom - United States Strategic Command

1 INTRODUÇÃO

O matemático Norbert Wiener, em sua obra ”*Cybernetics: or the Control and Communication in the Animal and the Machine”* escrita em 1948 apresenta as hipóteses e os fundamentos da cibernética, como resultado de vários anos de pesquisa e interação com pesquisadores de diversas áreas científicas, incluindo as ciências sociais. Para Wiener (1984), a cibernética se constitui em:

> [...] um campo mais vasto que inclui não apenas o estudo da linguagem mas também o estudo das mensagens como meios de dirigir a maquinaria e a sociedade, o desenvolvimento de máquinas computadoras e outros autômatos [...], certas reflexões acerca da psicologia e do sistema nervoso, e uma nova teoria conjetural do método científico. (WIENER, 1984, p. 15).

Norbert Wiener não foi pioneiro na criação da palavra cibernética, no entanto, foi o primeiro a unir diversas disciplinas científicas na compreensão da cibernética como teoria da comunicação e do controle. Na obra “The human use of human beings: Cybernernetics and Society”, publicada originalmente em 1950, Wiener passou a compreender a cibernética de forma abrangente como a teoria do controle e da comunicação nas máquinas, nos seres vivos e na sociedade: “comunicação e controle fazem parte da essência da vida interior do homem, mesmo que pertençam à sua vida em sociedade” (WIENER, 1984, p. 42).

Assim, observa-se que a interdisciplinaridade é a principal característica da cibernética, ressaltando-se os aspectos “comunicação e controle”, abrindo, desta forma, as possibilidades de estudo em diversas áreas da pesquisa científica.

Rosa (2014, p. 103), lembra que o aspecto histórico que liga a cibernética às redes de computadores e, em consequência, à Internet, nem sempre é suficientemente sublinhado. Para tal, o autor destaca a grande influência que algumas figuras do chamado movimento cibernético, entre estas, Norbert Wiener e Warren McCulloch, tiveram em alguns dos principais mentores do projeto que viria a implementar a primeira rede de computadores, entre os quais os pioneiros da Internet, como Joseph Licklider e Paul Baran. Licklider foi talvez o principal impulsionador do projeto ARPANET, que levaria à implementação da primeira rede física de computadores ligados entre si, precisamente a rede ARPANET, que foi a primeira rede da rede de redes que viria a ser a Internet. Ademais, destacxa, ainda, o autor, que foi o grupo de pesquisadores da agência de investigação norte-americana ARPA, inicialmente agrupados em torno de Licklider, e

depois dirigidos por Charles Taylor que, em 1969, implementou a primeira rede de computadores, a ARPANET.

Pinho (2003) destaca que a história da internet se inicia durante a Guerra Fria, quando os dois blocos antagônicos liderados, respectivamente, pela União Soviética (URSS) e pelos Estados Unidos, percebiam a necessidade de desenvolver novas tecnologias de comunicação. Nessa busca, a União Soviética lança, em 1957, seu primeiro satélite espacial artificial em órbita, o Sputnik. O mesmo autor relata que, devido a este fato, o presidente americano, Eisenhower, anunciou, após quatro meses, a ARPA – Advanced Research Projects Agency, como integrante do Departamento de Defesa dos Estados Unidos, com o objetivo de desenvolver pesquisas para o serviço militar, temendo um ataque por parte da URSS ao Pentágono. Surgiu aí a necessidade de criar uma rede de computadores para ser um sistema de comunicação e defesa, para informar sobre possíveis ataques terroristas. Tal sistema foi denominado Arpanet.

Manuel Castells (2003, p. 13) aponta também que as origens da internet podem ser encontradas na Arpanet, qualificando-a como “um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processinf Techniques Office (IPTO), fundado em 1962”, com objetivo de estimular a pesquisa em computação interativa.

Castells nos relata, ainda, que o IPTO valeu-se de uma tecnologia de comutação, desenvolvida de forma independente por Paul Baran na Rand Corporation e por Donald Davies no British National Physical Laboratory. Após várias evoluções, em 1973, dois cientistas da computação, Robert Kahn, da ARPA e Vint Cerf, então na Universidade Stanford, escreveram um artigo que apresentava a arquitetura básica da Internet. (CASTELLS, 2003, p.13-14).

Em 1975, a Arpanet foi transferida para a Defense Communication (DCA). Em 1983, o Departamento de Defesa, visando evitar possíveis falhas de segurança, resolveu criar a MILNET, uma rede para fins militares específicos. A Arpanet tornou-se então a ARPA-INTERNET e foi dedicada à pesquisa. Em fevereiro de 1990, a Arpanet, já tecnologicamente obsoleta, foi retirada de operação. Daí em diante, tendo libertado a Internet de seu ambiente militar, a administração da rede foi confiada à National Science Foundation (NSF) pelo governo americano. Posteriormente, a NSF decidiu encaminhar a privatização da Internet, ao se concretizar o fato de que a tecnologia de redes de computadores alcançou o domínio público.

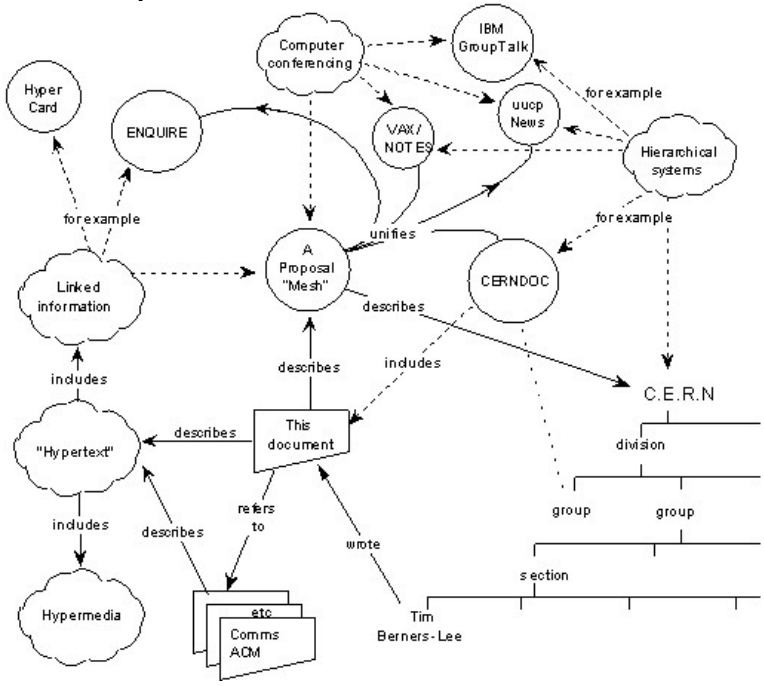
No início da década de 1990 muitos provedores de serviços da Internet montaram suas próprias redes e estabeleceram suas portas de comunicação em bases comerciais.

Ainda nesta década, a maioria dos computadores dos EUA tinha a capacidade de entrar em rede, lançando, assim, os alicerces para a difusão da interconexão de redes.

A Arpanet não foi a única fonte da Internet, tal como conhecemos hoje. O que permitiu à Internet alcançar o mundo todo foi o desenvolvimento da “world wide web (www)”. Foi Berners-Lee, que desenvolveu o programa Enquire, que ele havia escrito em 1980, e tornou realidade a Internet como conhecemos hoje. A figura 1 apresenta a proposta de gerenciamento de informações elaborada por Berners-Lee.

Em colaboração com Robert Cailliau, Berners-Lee construiu um programa navegador/editor em dezembro de 1990 e chamou esse sistema de hipertexto de www, a rede mundial. O software do navegador da web foi lançado em agosto de 1991. (CASTELLS, 2003, p.18) e (BERNERS-LEE, 1989)

Figura 1 - Proposta de gerenciamento de informações elaborada por Berners-Lee



Fonte: Berners-Lee (1989)

A criação da internet permitiu inúmeros benefícios em função da circulação da informação em tempo real e em nível mundial. Tudo graças à evolução experimentada pela Tecnologia da Informação e Comunicações (TIC). Entretanto, surgem novos tipos de ameaça, que desconhecem fronteiras e possuem um vasto potencial destrutivo, capaz de causar grandes prejuízos a pessoas e países.

De acordo com dados do MCT (2000), no Brasil, em 2000, o número de usuários da Internet girava em torno de 8,6 milhões e o governo brasileiro alertava que tal número era bastante limitado e precisaria crescer significativamente. Naquele ano, estimava-se que apenas 1% dos usuários da Internet no Brasil compraria em lojas virtuais, com média de gasto de apenas 18 dólares mensais.

No final de 2008, passou-se a contar com cerca de 55,9 milhões de usuários no Brasil segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD) e, aproximadamente, 83 milhões de pessoas de 10 anos ou mais acessaram a Internet nos três meses anteriores à realização da PNAD em 2012, apontando para um crescimento rápido de uso da Internet no país. Com relação à evolução da economia digital no país, os usuários brasileiros da Internet contribuíram com o comércio eletrônico, com faturamento da ordem de 8,2 bilhões de reais em 2008 com crescimento para cerca de 22,5 bilhões de reais em 2012, confirmando as prospecções de avanços preponderantes desta economia.

Ao se falar de conflitos, deve-se notar que eles ocorrerão quase em sua totalidade nos locais onde as pessoas vivem e trabalham. Segundo Commons (2018), existem duas tendências globais que vem caracterizando a dimensão humana do conflito: a mudança de pessoas para as megacidades, definidas aqui como as que possuem mais de 10 milhões de habitantes, e a interconexão cada vez maior entre as populações e infraestrutura. Este autor afirma ainda que no ano de 2014, já existiam aproximadamente 28 megacidades ao redor do mundo e acredita-se que este número chegará a 41 antes do ano de 2030. Como fator preponderante nota-se que a explosão de acesso à internet e celulares se dá em cidades que são densamente interconectadas.

> As megacidades modernas são os ambientes mais complexos no mundo atual, com a cidade funcionando como um ecossistema complexo e intricado. A megacidade é um ambiente operacional singular porque estratifica três elementos: amplos espaços; terreno físico complexo e restritivo; e densas aglomerações humanas. Esse ambiente cria atrito através de todos os domínios (terrestre, marítimo, aéreo, espacial e ciberespaço). (COMMONS, 2018, p. 67).

Nesse sentido, o domínio cibernético ou do ciberespaço, começa a ser amplamente estudado na arte da guerra, especialmente nas áreas de Ciência e Tecnologia, Defesa, Estratégia e Relações Internacionais. Há então um novo foco para as áreas de segurança e defesa cibernéticas, que serão melhor discutidas mais a frente neste estudo.

Com vistas a contextualizar a relevância da segurança e defesa cibernética para o Brasil, citamos o Relatório do XIII Encontro Nacional de Estudos Estratégicos – XIII ENEE, realizado em Brasília, em 2013, que tratou do tema “O setor cibernético brasileiro”:

> A segurança e a defesa cibernética são vetores estratégicos para o Estado, na medida em que afetam positiva ou negativamente aspectos políticos, econômicos e sociais do cotidiano da sociedade da informação. O próprio conceito de realidade foi expandido pelo ambiente virtual. (BRASIL, 2013a, p 17).
> Segurança diz respeito à sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza. Ao Estado compete garantir a segurança de todos, pois a todos deve e pode exigir o cumprimento dos deveres e funções necessários à manutenção dessa condição. (BRASIL, 2013a, p 17).
> "A segurança cibernética, engloba a defesa cibernética, diz respeito a uma atividade abrangente que congrega uma série de aspectos, que vão da proteção física e lógica da informação, em qualquer meio onde ela esteja abrigada, à proteção dos sistemas e redes de informação. Abrange, ainda, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações computacionais destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento – ou seja, um conjunto de ativos de informação denominado de Infraestrutura Crítica da Informação. (BRASIL, 2013a, p 17-18).

Assim, o espaço cibernético constitui-se em um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações.

> Em 2014, o cenário de uso da Internet e, consequentemente, de uso das Tecnologias de Informação e Comunicação (TIC) permanece crescente e, sem dúvida, além de qualquer expectativa e prospecção, operando-se em cifras bastante expressivas no mundo e no País, especialmente frente aos avanços do uso de dispositivos móveis, da computação em nuvem e da evolução da chamada "internet das coisas". O Brasil é considerado o quarto maior mercado mundial no setor de TIC, movimentando cerca de US$ 170 bilhões, e somente o comércio eletrônico faturou cerca de 35,8 bilhões de reais, e no mundo o movimento foi de cerca de 1,5 trilhões de dólares, demonstrando quão aquecida e intensiva vem sendo a economia digital e com tendência ascendente forte. Para 2020, estima-se um mercado global de TI na ordem de US$ 3 trilhões, e um mercado nacional da ordem de US$ 200 bilhões.(BRASIL, 2015a, p. 13).

Percebe-se que a Segurança da Informação e Comunicações (SIC) e a Segurança Cibernética, vêm se caracterizando cada vez mais como função estratégica de Estado, sendo essenciais à manutenção e preservação tanto das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, a própria Informação, entre outras, quanto dos direitos individuais, em especial da privacidade, e da soberania.

No Brasil, os assuntos relacionados à Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas são tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, por meio do GSI/PR, que exerce as funções de Secretaria-Executiva do citado Conselho e de Presidência daquela Câmara.

1.1 Justificativa

É mister o estudo da Guerra Cibernética, considerando-se que os conflitos e seus cenários de atuação têm cada vez mais deixado o teatro de operações convencional e partido para o espaço cibernético. Como exemplo clássico dessa migração pode-se citar o conflito entre Geórgia e Rússia em 2008, o ataque às instalações nucleares do irã em 2010 e os ataques aos serviços públicos da Estônia em 2007. Além destes exemplos cita-se ainda a possível influência dos Russos nas eleições presidenciais americanas durante a campanha de 2016.

Ademais, o desenvolvimento constante de novas tecnologias passíveis de serem utilizadas para este fim, bem como a existência de atores diversos, como grupos ideológicos, organizações independentes ou até mesmo simples indivíduos, fazem com que os ataques não sejam realizados somente pelos Estados ou somente contra outros Estados.

A situação atual já mostra uma preocupação das autoridades mundiais com o campo cibernético. Com vistas a manter-se em consonância com esta nova situação, o Congresso Brasileiro, publicou em setembro de 2013, a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Cabe ainda ressaltar que em 14 Dezembro de 2018 o Senado Federal promulgou uma atualização destes 3 documentos.

Da Política Nacional de Defesa, alguns marcos relevantes ao presente estudo podem ser indicados:

> Para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear. (BRASIL, 2013, p. 19).

E ainda:

> Os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e outros aperfeiçoamentos tecnológicos trouxeram maior eficiência aos sistemas administrativos e militares, sobretudo nos países que dedicam maiores recursos financeiros à Defesa. Em consequência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância. Para superar essas vulnerabilidades, é essencial o investimento do Estado em setores de tecnologia avançada. (BRASIL, 2013, p. 19).

Nota-se a inclusão do setor cibernético como estratégico para a autonomia do Estado, assim como a importância de investimentos neste campo de atuação.

A Estratégia Nacional de Defesa (END) destaca a importância do fortalecimento da pesquisa científica voltada ao setor cibernético. Assim, o escopo do presente estudo encontra-se alinhado as prioridades definidas pelo Governo Federal, dentre elas, em especial, “Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional.”(BRASIL, 2013, p. 94)

Nesta mesma direção, e, ademais, ressaltando a importância do Setor Cibernético, o Livro Branco de Defesa Nacional (LBDN) versa:

> A proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. (BRASIL, 2013, p 71).

Antecipando-se a publicação da END, a qual dá as diretrizes para a adequada preparação e capacitação das Forças Armadas, de modo a garantir a segurança do país tanto em tempo de paz, quanto em situações de crise, o Comando da Aeronáutica reeditou no ano de 2012 a Diretriz do Comando da Aeronáutica (DCA 1-1) - Doutrina Básica da Força Aérea Brasileira. Em relação ao domínio da informação no campo de batalha, esta DCA, apresenta o ambiente cibernético como uma importante peça capaz de auxiliar a manutenção da soberania do poder aeroespacial nacional.

> A informação é um fator diferencial na guerra moderna, pois afeta diretamente o processo decisório das forças em combate. Além disso, as diversas fontes de notícias que circulam no campo de batalha podem influenciar o senso comum a um posicionamento favorável ou contrário aos objetivos da campanha ou da operação militar.(BRASIL, 2012, p. 43).
> Nesse contexto, também deve ser considerado o controle do ambiente cibernético, conformado por Sistema de Comunicações e Tecnologia da Informação para Comando e Controle (SCTIC2), que são vitais para troca de informações entre todos os escalões da cadeia de comando. O domínio do ambiente cibernético pode, direta ou indiretamente, afetar as lideranças, as forças militares e as infraestruturas críticas do inimigo, até o ponto de evitar a confrontação militar direta.(BRASIL, 2012, p. 43).

Então, o presente estudo justifica-se pelo fato da Guerra Cibernética, tornar-se uma realidade presente no cotidiano da vida moderna, graças a recente explosão e desenvolvimento de novas tecnologias em, especial, da Tecnologia da Informação (TI). Outrossim o uso do espaço cibernético como arma, pois esse se mostra um meio extremamente eficiente e eficaz de ataque, dada a dificuldade de identificação da origem e o alto poder de impacto, qual seja financeiro, físico e até mesmo moral. Conflitos recentes demonstraram ao mundo o poder de destruição causado por atividades executadas no ambiente cibernético, mesmo que sem uma definição concreta do

atacante, portanto é de vital importância que o Brasil tenha o domínio de tal recurso de forma a incorporá-lo em seu arsenal.

Porém, para que atinja este grau de maturidade, é necessário a sua utilização estruturada, o que, devido aos recentes avanços tecnológicos e a relativa novidade do assunto, denota uma grande necessidade de estudos científicos acerca do tema.

Assim, o presente estudo poderá auxiliar na composição de um conhecimento necessário ao aumento do nível de maturidade cibernética nacional. Será capaz ainda de auxiliar na identificação e criação de um modelo de trabalho de melhor aderência à realidade Brasileira. Outro ponto, que dá relevância a este trabalho, é o estímulo ao debate sobre como deve ser planejada uma política de Estado que direcione os recursos necessários ao desenvolvimento sustentável das questões cibernéticas.

Nota-se que a área cibernética assumiu grande relevância para as questões de segurança, para as relações-públicas no cenário contemporâneo brasileiro e nas relações internacionais. Assim torna-se imperioso o estudo dessa nova modalidade de guerra, o que nos leva a questão problema que norteou toda a pesquisa científica:

Como as novas ameaças, geradas pela guerra cibernética em encontro com as guerras cinética e eletrônica, podem afetar o Poder Aeroespacial?

A hipótese levantada inicialmente é que há um incremento na preocupação por parte dos Estados, em relação ao que acontece no espaço cibernético, em função de seus possíveis impactos e suas consequências no mundo físico. Nota-se ainda a utilização do meio cibernético em caráter ofensivo entre os países, diversas organizações, e até mesmo indivíduos são capazes de colocar em risco a soberania e a independência das nações.

O presente estudo tem como objetivo analisar, por meio da caracterização de possíveis alvos e utilização de exemplos, como as novas ameaças cibernéticas podem afetar o Poder Aeroespacial.

São objetivos específicos desse trabalho:

a) Analisar os fundamentos da guerra cibernética, a luz dos conceitos de guerra e segurança convencionais;

b) Estudar como o Espaço Cibernético e a Guerra Cibernética podem afetar a relação entre os Estados; e

c) Apresentar um estudo comparativo da atual estrutura do Brasil, dos Estados Unidos e da Alemanha no tocante à defesa cibernética;

O presente estudo é uma pesquisa não experimental, onde se analisa o cenário cibernético no Brasil, Estados Unidos e Alemanha. O campo cibernético, inserido em um contexto tecnológico em constante e rápida evolução, aborda vários ramos do conhecimento e ainda apresenta conceituações pouco sedimentadas dentre seus teóricos. Nesse sentido o presente estudo direcionou-se para uma pesquisa qualitativa, exploratória e descritiva, visto que busca proporcionar uma maior familiaridade com o espaço cibernético como teatro de operações de guerra, além da necessidade da análise de exemplos do funcionamento da estrutura cibernética de países de que estão à frente da tecnologia, como Estados Unidos e Alemanha visando facilitar o entendimento do tema proposto. Trata-se de uma pesquisa bibliográfica e documental, fazendo uso de documentos institucionais ostensivos.

Considera-se ainda que o relacionamento entre a segurança internacional e a cibernética é muito novo no cenário acadêmico. Desta maneira o presente estudo não pretende resolver ou esgotar o tema. Ressalta-se que o objetivo final do trabalho é revisar e apresentar, de modo crítico, o conteúdo que vem sendo produzido no cenário atual.

Eventualmente, questões técnicas foram abordadas, com vistas a clarificar o estudo. No entanto, cabe reforçar que não é este o foco da pesquisa. Assim, nos atemos ao estudo da Guerra Cibernética, pois os conflitos e seus cenários de atuação cada vez mais se afastam do teatro de operações convencional e se voltam para o espaço cibernético.

1.2 Estrutura da dissertação

O trabalho está organizado em 6 capítulos, conforme descrito a seguir.

No capítulo 1 é uma apresentada uma breve introdução, e contextualização do tema de pesquisa, por meio de um breve histórico do uso da Tecnologia no cenário atual. Apresenta ainda o processo de pesquisa realizado na elucidação do problema, indica o tipo de pesquisa realizado e as limitações encontradas na metodologia escolhida.

No capítulo 2 é apresentado o referencial teórico. Foram abordados conceitos referentes ao modelo tradicional de guerra e os conflitos de quarta geração. Entendendo-se a relevância desta discussão, busca-se uma revisão teórica que permita um melhor entendimento do papel da TI na Guerra Moderna.

O capítulo 3 refere-se ao Espaço Cibernético, as principais características da Guerra Cibernética, e o aumento da importância da Cibernética no cenário mundial.

O capítulo 4 trata da Defesa Cibernética no Brasil, nos Estados Unidos e na Alemanha, seu histórico e seu modo de funcionamento atual.

O capítulo 5 apresenta uma breve discussão sobre os ataques ciber-cinéticos e políticas para mitigação de ataques.

Por fim tem-se as considerações finais, capítulo que apresenta as conclusões da pesquisa realizada e sugestões de estudos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta a revisão teórica em relação ao conceito histórico de Guerra, o conceito referente a conflitos de 4ª geração e, os conceitos voltados ao uso da tecnologia como arma.

2.1 Revolução nos assuntos militares e poder aéreo: a incorporação do espaço cibernético à conduta da guerra.

Carl von Clausewitz (1780-1831) general prussiano, autor de importante obra no que se refere à literatura militar – o livro “Da Guerra”, que traz em sua concepção as observações e a vasta experiência do general acerca da era das guerras napoleônicas. Quando a Prússia foi derrotada, esta se aliou à França de Napoleão. Neste momento, Clausewitz renunciou à sua patente no exército prussiano e se alistou no exército Russo. Teve papel relevante na retirada da Prússia da Aliança Pró França quando o exército napoleônico bateu em retirada após uma malsucedida ação contra a Rússia, sendo então, reintegrado ao exército prussiano. Clausewitz ainda participou de diversas operações no teatro de Guerra até a derrota definitiva de Napoleão.

Mesmo sua publicação tendo sido feita há quase 200 anos, a teoria política da Guerra elaborada por Clausewitz ainda é muito útil para o pensar estratégico. Ele acreditava que a Guerra é simplesmente um ato de força voltado a submeter o inimigo à nossa vontade. Clausewitz dizia ainda que a guerra é ao mesmo tempo um fenômeno político e uma atividade social. Não obstante o combate ser o principal meio da guerra, essa era composta pela intenção de distintas instâncias políticas, militares e sociais combinadas a diferentes motivações no tocante ao evento bélico. Tais instâncias formam uma “trindade” que é composta por governo, militares e povo, os quais se movem, respectivamente, pela razão, probabilidade e paixão.

Alguns pontos da teoria clausewitziana tornaram-se inadequados à realidade dos conflitos bélicos, graças a rápida evolução tecnológica ocorrida nos dois séculos seguintes e, consequente letalidade das novas armas. Um bom exemplo deste fato foi a utilização dos meios aéreos, que foram utilizados nas manobras indiretas contra o inimigo visando a obtenção de vantagem em relação à velocidade de atuação, à surpresa e aos efeitos, gerando assim mudanças especialmente no que tange às áreas política e estratégica.

> Segundo assegura Murillo Santos, antes de novembro de 1911 “pouquíssimas pessoas enxergavam o aeroplano como um instrumento bélico propriamente dito”. O autor da obra “Evolução do Poder Aéreo” percebe o advento do avião, no início do século XX, como um inédito engenho bélico, que foi agregado aos demais poderes militares quando “durante o conflito ítalo-turco, na Líbia, nove aviões italianos, em operações bélicas, haviam despejado granadas de dois quilos sobre tropas turcas”. (SIQUEIRA, 2010, p. 9).

Tal fato foi confirmado em meados do século XX, quando da construção das primeiras aeronaves com capacidade ofensiva. Este novo equipamento bélico tinha capacidade única de superar, pelo ar, obstáculos naturais e as defesas impostas pelo adversário. Com isso existia uma maior probabilidade de ataque às infraestruturas críticas, centros de comando e controle sem a necessidade prévia de superação das forças armadas dispostas na primeira linha do campo de combate. O resultado da introdução deste novo vetor no teatro de operações foi a necessidade do estudo e desenvolvimento de novas teorias da guerra, visto que com o uso deste novo vetor era possível se atingir todo o território adversário, além de uma aproximação entre os níveis tático e estratégico.

> Pode-se afirmar que o general italiano Giulio Douhet foi o primeiro profeta, apologista, teórico e estrategista do poder aéreo. Todavia, ele não estava sozinho na apologia ao emprego do poder aéreo.
> Àquela época, mais um teórico italiano do Poder Aéreo, Nino Salvaneshi, preconizou o bombardeio estratégico como um meio de pôr fim à mortandade extrema na guerra.
> Outros homens, como o norte-americano Mitchell e o britânico Trenchard, contemporâneos do italiano, partilharam de suas ideias no essencial, desenvolvendo, porém, linhas de pensamento um pouco diferenciadas. Surgiram outros proeminentes pensadores do poder aéreo como John Slessor, Arthur Tedder, e Seversky, que foi um seguidor do pensamento de Mitchell e, em parte, de Douhet.
> As ideias de Douhet influenciaram na formação e desenvolvimento do Poder Aéreo de vários países, especialmente da Grã-Bretanha e dos EUA. (SIQUEIRA, 2010, p.12).

Nesse sentido, Douhet foi o primeiro a tratar a conquista do domínio aéreo de modo a explorar as potencialidades do poder aéreo e, com isso, foi capaz de elaborar estudos e probabilidades sobre seu emprego com base nos princípios fundamentais da guerra, evidenciando a importância dos vetores aéreos no sucesso dos confrontos militares através de reconhecimento e suporte às forças de superfície, prevendo ainda grandes frotas aéreas, conduzindo as operações de guerra. Ressalta-se que no início ainda não se falava em bombardeio estratégico.

> […], Douhet, então major, comandante provisório de um batalhão, foi o responsável pelo relatório da guerra contra os turcos, na Líbia em 1911. Nessa mesma Guerra, de acordo com Longyard, Douhet foi também o comandante do esquadrão que realizou o primeiro bombardeio aéreo da história. Daí é que o interesse desse oficial se consolidou para a importância do poder aéreo. Da

> experiência desse conflito, fez um chamado à indústria italiana para que ela desenvolvesse as potencialidades das aeronaves, tanto comercialmente, quanto como instrumento de segurança nacional. (ROSA, 2014, p. 50).

Segundo ROSA (2014) a principal tese de Douhet era que o poder aéreo, através de um bombardeio estratégico, era capaz de devastar toda uma Nação e, consequentemente, por fim a guerra terrestre tornando-a insignificante.

A segunda guerra mundial vem corroborar a teoria de Douhet, com o uso do avião como diferencial e arma decisiva em relação às manifestações de força militar, tornando determinantes as ofensivas aéreas na conquista da supremacia e superioridade no teatro de operações.

A acelerada globalização e o impacto das novas tecnologias em todas as áreas desencadeou uma intensa competitividade entre os Estados-Nação, os blocos político-econômicos e as regiões. Assim, o poder aeroespacial se torna elemento líder da força político-militar. Sua capacidade de cobrir uma longa área em tempo relativamente pequeno, dá a esse vetor uma projeção global e representa a possibilidade de uma atuação imediata ao dispor do Estado em caso de guerra.

Orientado para atuar e projetar a força assimetricamente no espaço e no tempo, um poder aéreo forte proporciona ao seu detentor uma vantagem no campo de batalha, visto que dificultará o inimigo a dele ser capaz de se defender ou ao confronto direto.

Após o término da era industrial, tem início a era da informação, apesar de seu início datar do princípio do século XX, popularizou-se após os anos 80. Com o desenvolvimento da ARPANET e consequentemente, da internet, novos paradigmas passam a existir. Há então a necessidade de evolução das doutrinas militares até então existentes para este novo vetor.

A doutrina militar de comando e controle explicita a necessidade de superioridade no campo da informação:

> A Superioridade de Informação é a capacidade de fornecer informações pertinentes aos usuários interessados, no momento oportuno e no formato adequado, negando ao oponente as oportunidades de atingi-la. Envolve a habilidade de criar uma vantagem por meio da utilização dessas informações quando em confronto com o oponente. A informação tem as dimensões de relevância, precisão e oportunidade. Por isso um padrão superior no domínio da informação é atingido quando a relevância, a precisão e a oportunidade visam ao cem por cento. (BRASIL, 2015b, p. 40).
>
> Deve-se buscar a Superioridade de Informação não apenas mantendo sistemas de maior capacidade de produção de dados. É fundamental, também, considerar a qualidade da informação produzida, para que se construa e mantenha a necessária consciência situacional, conforme abordado no Capítulo II desta Doutrina. (BRASIL, 2015b, p. 40).

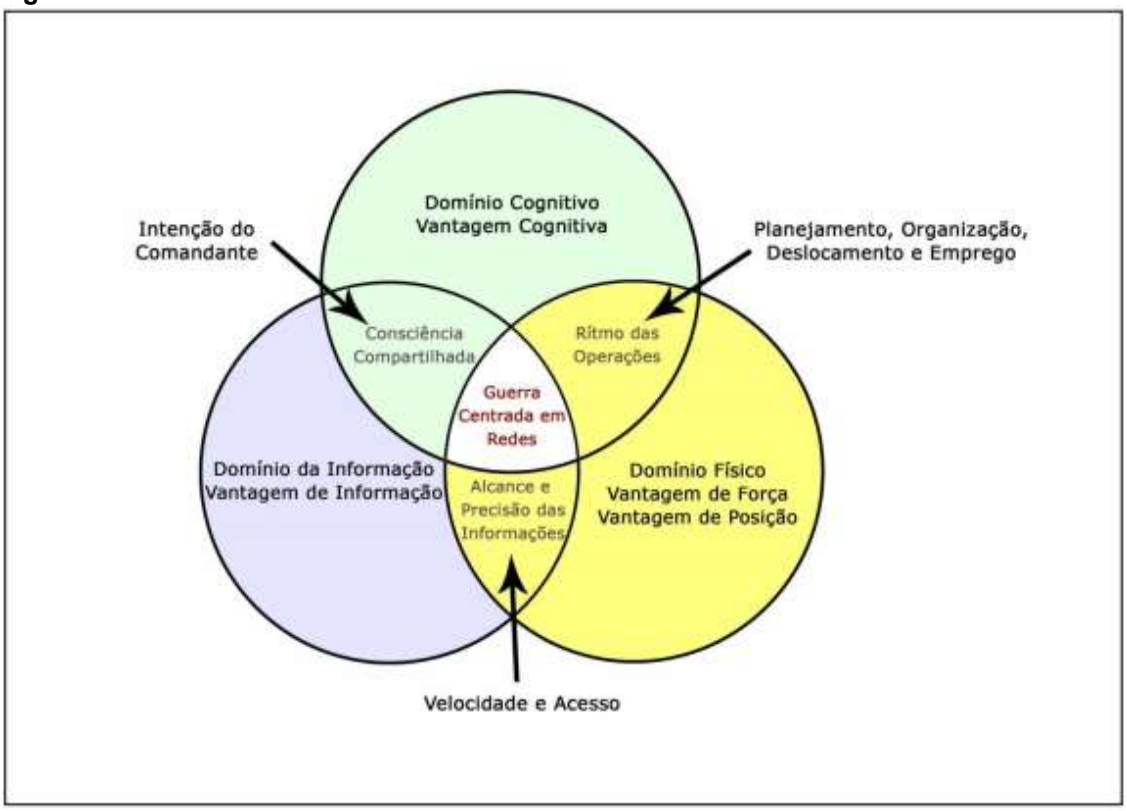
Deste novo fator emerge um novo conceito chamado Guerra Centrada em Redes (GCR) ou do inglês Network Centric Warfare (NCW). Sua concepção pretende materializar uma resposta adequada a este novo ciclo característico da sociedade que vive num mundo globalizado e interconectado por meio de redes de computadores.

Tal conceito consiste na inserção do campo cibernético ao teatro de operações da guerra convencional. Segundo BRASIL (2015b), a GCR é uma forma de atuação na guerra com a vertente oriunda da era da informação, cuja característica é o compartilhamento da consciência situacional visando obtenção da superioridade de informação mesmo que os agentes estejam geograficamente dispersos. Com vistas a facilitar o entendimento acerca do assunto, a GCR é dividida em três domínios, quais sejam, físico, da informação e cognitivo, conforme definição abaixo:

> Domínio Físico Este domínio é representado pelo ambiente onde ocorrerá o conflito, no qual as forças buscarão exercer influência e onde ocorrerão as ações de ataque e defesa nos ambientes naval, terrestre, aeroespacial e cibernético. Nesse domínio, residem as plataformas de combate e as redes que as interconectam. Existe apenas uma realidade, um domínio físico, o qual será convertido em dados, informações e conhecimento pelos sistemas de C² que compõem o domínio da informação. (BRASIL, 2015b, p. 41).
> Domínio da Informação – É onde a informação propriamente dita será criada, manipulada e compartilhada. Permite o fluxo de informações entre combatentes e entre as forças empregadas nas operações, transmitindo as intenções do comandante. Devido à importância deste domínio, torna-se necessário protegê-lo e defendê-lo, a fim de manter a capacidade da própria força em aumentar o poder de combate em relação ao oponente. Nesse sentido, a busca pela Superioridade de Informação deve ser constante. (BRASIL, 2015b, p. 41).
> Domínio Cognitivo Este domínio se encontra nas mentes das pessoas, abrangendo a percepção, a consciência, os entendimentos, as crenças e valores e, também, como resultado do raciocínio, as decisões. Todo o conteúdo do domínio cognitivo baseia-se na percepção humana, consistindo na visão pessoal de cada indivíduo, sua bagagem cultural, experiência, treinamento, valores e capacidade individual. O entendimento das intenções do comandante, da doutrina, das táticas, das técnicas e dos procedimentos pode ser citado como componente desse domínio. (BRASIL, 2015b, p. 41).

A figura 2 apresenta, em síntese, os domínios da CGR e suas características básicas.

Figura 2 - Domínios da GCR



Fonte: Brasil (2015b, p. 42)

Observa-se então que a GCR amplia as capacidades de comando e controle, quando integra esses três domínios. O espaço cibernético passa a integrar o domínio da guerra.

2.2 Gerações da Guerra

Antes de se falar das gerações da guerra, cabe aqui definir o significado do termo em sua essência:

> Não deverei começar expondo uma definição pedante, literária da guerra, mas ir direto ao cerne da questão, o duelo. A guerra nada mais é que um duelo em escala maior. Inúmeros duelos vêm formar a guerra, mas um quadro dela como um todo pode ser formado por um par de duelistas. Cada um tenta através da força física compelir o outro a fazer sua vontade; seu objetivo imediato é derrubar seu oponente de modo a torná-lo incapaz de uma resistência posterior.
> A guerra é assim um ato de violência destinado a compelir nosso inimigo a fazer nossa vontade. A violência, para se opor à violência, se vale das invenções da arte e da ciência. Junto à violência estão certas limitações autoimpostas, imperceptíveis, de pouca validade de menção, conhecidas como Lei e costumes internacionais, mas que dificilmente diminuem sua força. A violência – que é a violência física, já que a violência moral não existe, salvo como expressa pelo Estado e pela Lei – é assim o meio da guerra, impor nossa vontade ao inimigo é o fim. Assegurar que o fim que temos é o de desarmar o inimigo; e que, teoricamente é o verdadeiro objetivo da guerra. Isto toma o lugar do fim,

> descartando-se o entendimento que não é parte da própria guerra. Passos (2005 apud CLAUSEWITZ, 1984, p. 12).

Este autor deixa claro que não há limitações para a violência física em guerras pautadas nas leis, muito menos há que se falar em violência moral, assim, nessa esteira, continua Clausewitz:

> As pessoas de bom coração poderiam certamente pensar que haveria alguma ingênua maneira de desarmar ou derrotar um inimigo se muito derramamento de sangue, e poderia imaginar que este é o verdadeiro objetivo da guerra. Por mais interessante que isso pareça, é uma falácia que tem que ser exposta: a guerra é um assunto tão perigoso que os erros decorrentes da bondade são os piores. Passos (2005 apud CLAUSEWITZ, 1984, p. 13).

O Quadro 1 apresenta um breve resumo das quatro gerações de guerra moderna.

Quadro 1: Quatro Gerações da Guerra Moderna

PRIMEIRA GERAÇÃO	A Primeira Geração da Guerra Moderna, era a guerra de linha e coluna onde as batalhas eram formais, ocorreu entre 1648 a 1860, isto é, foi durante o tratado de Vestfália (1648) e as Guerras Napoleônicas. Nessa geração havia uma cultura militar de ordem, porém em meados do século XIX, o ordenado campo de batalha começou a se desordenar por conta das táticas antigas de linha e coluna suicidas.
SEGUNDA GERAÇÃO	A Guerra de Segunda Geração foi uma resposta à contradição entre a cultura da ordem e o ambiente militar. Desenvolvido pelo Exército Francês durante e depois da Primeira Guerra Mundial, pois procurava uma solução no fogo concentrado. O objetivo era o atrito, e a doutrina foi resumida pelos franceses como sendo “a artilharia conquista a infantaria ocupa”. Ela representou um grande alívio para os soldados porque preservava a cultura de ordem, presando mais a obediência do que a iniciativa do soldado.
TERCEIRA GERAÇÃO	A Guerra de Terceira Geração foi produto da Primeira Guerra Mundial, desenvolvida pelo Exercito Alemão e ficou conhecida como Guerra de manobra. Ela é baseada não no poder de fogo e atrito, mas na velocidade, surpresa e no deslocamento mental e físico. Essa guerra representa o retorno a tática e a mobilidade. É uma guerra em que não apenas as táticas são distintas, mas a própria cultura militar muda, pois se trata de uma guerra que não é linear. Diferentemente da Guerra de Segunda Geração, a Terceira dava mais importância a iniciativa dos militares do que a obediência, pois era uma questão de autodisciplina.
QUARTA GERAÇÃO	A Guerra de Quarta Geração é aquela em que o Estado perde o monopólio sobre a guerra e tem como características, a descentralização e a iniciativa, pois marca a mudança mais radical desde a Paz de Vestfália. No seu fundamento se encontra uma crise universal da legitimidade do Estado, e essa crise significa que muitos países terão evoluída a guerra de Quarta Geração em seu território.

Fonte: Ramos (2015, p. 22)

A chamada guerra de 1ª Geração, possui como característica principal um campo de batalha bem definido e o combate regido pelo “Princípio da Massa”, cujo foco é a concentração de um maior potencial de combate em determinado ponto e momento

considerados decisivos. Acrescente-se a isso que se tratava de uma guerra onde os exércitos formais eram dispostos em formações de linhas e colunas táticas. A guerra de 1ª Geração teve seu início no Tratado de Paz de Westphalia, em 1648, seu ápice durante as campanhas napoleônicas e perdurou até 1860.

A partir de meados do século XIX, percebe-se uma ruptura no campo de batalha. Os exércitos passaram a realizar missões cujas táticas de linhas e colunas estavam obsoletas, portanto, suicidas. A cultura de ordem previamente consoante com o ambiente passou a ficar cada vez mais em desalinho com ele.

Graças a este fato, surge então a guerra de 2ª Geração, que perdurou entre 1860 e à I Guerra Mundial. Esse tipo de conflito foi marcado pela utilização de armas de destruição em massa.

De acordo com Hecht e Servent (2015), as guerras da Criméia e da Secessão e de 1870-1871 já anunciavam a nova era industrial de guerra baseada na técnica aliada à rapidez crescente dos deslocamentos. Os estrategistas franceses, confiantes demais, vão logo descobrir a potência do fogo, a da artilharia em geral e da artilharia pesada em particular, capaz de imobilizar um exército muitos quilômetros antes de chegar ao campo de batalha. Nesse sentido a guerra de Segunda Geração teve sua doutrina resumida pelos franceses como: “a artilharia conquista, a infantaria ocupa”. Foi também nesse período, que graças ao surgimento dos blindados e da aviação, que surgiu um novo conceito de guerra, ou seja, as guerras de 3ª Geração.

Com a chegada da II Guerra Mundial, tem início as guerras de 3ª Geração. Essa geração foi marcada pelo Blitzkrieg ou guerra de manobra, desenvolvida pelo exército alemão, consciente que não possuía uma indústria bélica forte. Essa doutrina militar tem por base a velocidade, a surpresa e o mental, além do deslocamento físico, e não apenas do poder de fogo e do atrito, como nas gerações anteriores.

O Combate assume então um novo modo de operação, onde as tropas não mais avançam de forma linear, mas manobram em torno do exército adversário, atacando pela retaguarda, com o fito de gerar um elemento surpresa. Cabe então reforçar, que nos cenários ora apresentados (guerras de 1ª, 2ª, e 3ª Gerações), os principais atores eram os estados nacionais.

Apesar da falta de uma definição consensual acerca da melhor definição sobre guerras de 4ª Geração, o presente estudo adota a definição escrita pelo Coronel R/1 Thomas X. Hammes, do Corpo de Fuzileiros Navais Americano, publicado em 2003 afirma: Guerras de 4ª Geração utilizam de todas as redes disponíveis – políticas,

econômicas, sociais e militares – para convencer os líderes inimigos responsáveis pelas decisões políticas de que seus objetivos estratégicos são demasiadamente custosos quando comparados aos benefícios percebidos. Trata-se de um modo avançado de insurgência.

Com o advento da guerra de Quarta Geração, os Estados Nacionais deixam de ser os únicos protagonistas, surgindo novos atores como as companhias militares privadas, diversas forças irregulares com motivações diferentes, crime organizado e terrorista, entre outros.

Observa-se ainda que nas guerras de quarta geração, os insurgentes evoluem para uma crescente variedade de grupos armados, que são interligados por meio de alianças de ideias. Em face disso vivemos em uma constante mudança de atores e motivações ao longo do tempo.

Isso faz com que tal tipo de guerra represente um enorme desafio em relação aos seus predecessores, a difusão de motivações, a junção de grupos ideológicos, gera uma enorme dificuldade em se identificar contra quem ou o porquê se está lutando.

Em suma, a guerra de quarta geração se utiliza de todas as mudanças, de uma sociedade da informação com vistas a multiplicar e aumentar cada vez mais o poder das insurgências. Desta forma apresenta uma evolução dinâmica, com a sociedade, tornando-se cada vez mais perigosa e difícil de ser controlada e combatida.

3 ESPAÇO CIBERNÉTICO

Desde os primórdios, uma das preocupações inerentes ao ser humano, é referente à relação Espaço/Tempo. Conforme Santos (1989), ao estudar o campo filosófico sobre esta relação, imediatamente encontramos a célebre frase aristotélica: “aquilo que não está em nenhuma parte não existe?”

Em 1982 o autor norte-americano Willian Gibson, cunhou o termo espaço cibernético, em seu romance chamado “Burning Chrome”, por meio da junção dos termos cibernética e espaço. Gibson descreveu o espaço cibernético como sendo:

> A matriz é uma representação abstrata dos relacionamentos entre sistemas de dados. Programadores legítimos entram no setor da matriz de seus empregadores e se veem cercados por geometrias brilhantes representando os dados corporativos. (GIBSON, 2003, p.25, tradução nossa).

Deste romance há ainda de se ressaltar a preocupação com a segurança dos dados envolvido neste novo meio.

> Torres e campos variavam no não-espaço incolor da matriz de simulação, a alucinação de consenso eletrônico que facilita o manuseio e intercâmbio de grandes quantidades de dados. Programadores legítimos nunca veem as paredes de gelo nas quais trabalham, as paredes de sombra que protegem suas operações de outros, de artistas e traficantes de espionagem industrial como Bobby Quine. (GIBSON, 2003, p.25, tradução nossa).

De acordo Brasil (2010), o espaço cibernético é entendido numa visão de inteligência coletiva e mutante, baseado em redes e trocas de saber, conforme citado abaixo:

> O que seria o espaço cibernético? O espaço cibernético é um terreno onde está funcionando a humanidade, hoje.(…) é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Atualmente, temos cada vez mais conservados, sob forma numérica e registrados na memória do computador, textos, imagens e músicas produzidos por computador. Então, a esfera da comunicação e da informação está se transformando numa esfera informatizada. (…) Com o espaço cibernético temos uma ferramenta de comunicação muito diferente da mídia clássica, porque é nesse espaço que todas as mensagens se tornam interativas, ganham uma plasticidade e têm uma possibilidade de metamorfose imediata. E aí, a partir do momento que se tem o acesso a isso, cada pessoa pode se tornar uma emissora, o que obviamente não é o caso de uma mídia como a imprensa ou a televisão. (...) Do interior do espaço cibernético encontramos uma variedade de ferramentas, de dispositivos, de tecnologias intelectuais. Por exemplo, um aspecto que se desenvolve cada vez mais, nesse momento, é a inteligência artificial. Há também os hipertextos, as multimídias interativas, simulações, mundos virtuais, dispositivos de telepresença. (...) O importante é que a informação esteja sob a forma de rede e não tanto a mensagem, porque esta já existia numa enciclopédia ou dicionário”. (BRASIL, 2010, p. 18).

Já para Richard Clarke (2010), o espaço cibernético é considerado como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles. Ainda, em sua opinião, o espaço cibernético não pode ser confundido com a conceituação de Internet, pois essa é o conjunto de redes menores e equipamentos conectados a ela. Assim, para esse autor, o conceito de espaço cibernético é mais abrangente, pois, além da Internet, ele também engloba os demais computadores não conectados e também seus equipamentos.

Por ainda não possuir uma definição amplamente aceita, observa–se grande quantidade de autores buscando definição para o espaço cibernético, sendo alguns mais voltados para o caráter da informação e dos aspectos virtuais e outros que o aproximam dos aspectos físicos e estruturais.

Mandarino Júnior (2009) entende que a Infraestrutura Crítica da Informação, à qual está vinculada a Segurança da Informação e Comunicações, compreende, como já vimos, todos os hardwares, softwares e equipamentos que se interconectam, seja por fibras óticas, seja pelo espectro eletromagnético. Compreende também os locais de armazenagem, processamento, transmissão de toda a informação, além da própria informação. As pessoas que interagem com a infraestrutura também são objeto das medidas de Segurança da Informação e Comunicações. Esse todo forma um conjunto de partes virtuais ou partes físicas. O complexo virtual, aí formado, compõe o chamado espaço cibernético.

É interessante ressaltar então a visão de Mandarino Jr que considera a própria informação e os usuários como parte integrante do espaço cibernético.

Tal visão facilita entender que o espaço cibernético é não-natural, foi criado pelo homem, com uma abordagem bem diferente dos espaços aéreo, terrestre e marítimo por exemplo. Pode–se ainda definir que o espaço cibernético já nasceu com uma definição territorial, através da interligação em rede dos computadores de todo o mundo e os demais itens conectados a esses aparelhos ou sob seu controle.

Muitas características do espaço cibernético alteram a compreensão tradicional das relações internacionais, dentre eles, conforme CHOUCRI (2012):

a) Temporalidade (substitui a temporalidade convencional pela quase instantaneidade);
b) fisicalidade (transcende restrições de localização geográfica e física);
c) permeação (penetra limites e jurisdições);
d) fluidez (sustenta mudanças e reconfigurações);

e) participação (reduz barreiras ao ativismo e expressão política);
f) atribuição (obscurece identidades de atores e links para ação); e
g) responsabilização (ignora mecanismos de responsabilidade).

Cada um desses fatores em separado, foge ao conceito comum de realidade, quando agrupados, criam fortes rupturas que interferem no conceito de soberania e nas estruturas verticais de poder e influência. Nesse sentido, as relações internacionais que, geralmente são enquadradas em relações hierárquicas de poder, tornam-se incongruentes com os novos recursos. Este sistema age com um número cada vez maior de atores (indivíduos, grupos e atores não estatais), influenciando num contexto de descentralização, localização e assimetria nos modos de vantagens e poder.

Entende-se que o espaço cibernético é um contexto construído através de iterações. Para o presente estudo vamos considerar o espaço cibernético é:

a) Criado através da interconexão de milhares de dispositivos (computadores, servidores, tablets, celulares,…), através da rede global, conhecida como internet.
b) Construído em camadas, onde os elementos físicos permitem um quadro lógico de interconexão, capaz de processar, manipular, explorar, aumentar as informações e a iteração entre as pessoas.
c) Habilitado por intermediação e organização institucional, e;
d) Caracterizado pela descentralização e interação entre esses atores, eleitorados e interesses.

Para muitos o espaço cibernético tornou-se sinônimo de Internet. Segundo PACE (2006) o Presidente dos Chefes da Equipe Conjunta do Exército, Aeronáutica e Marinha dos EUA adotou a seguinte definição para o espaço cibernético: “Um domínio caracterizado pelo uso do espectro eletrônico e eletromagnético para armazenar, modificar e trocar dados através de sistemas em rede e suas infraestruturas físicas associadas”.

Fazendo uma análise da definição PACE (2006) podemos identificar que o uso da palavra “domínio” em vez de “ambiente” traz implicações legais sob as leis do conflito armado. A eletrônica e o espectro eletromagnético se referem à dualidade onda partícula da radiação que, quando modulada com a informação, cria um sinal. Os sistemas de dados e de rede referem-se a informações digitais e programas aplicativos e ao computador e redes em que eles existem, ou seja, dados e aplicativos em repouso e em

movimento. Para fins de guerra, derivamos uma definição funcional do espaço cibernético como “um domínio no qual os sinais mantêm em risco sistemas inteligentes”.

Essa definição nos remete a três componentes para o espaço cibernético: os “efetores” que abrangem uma ampla gama de ameaças de sinal carregado, analógicas e digitais; o “meio” permite que os efetores acessem as conexões cabeadas e sem fio, hardware e software; Os “alvos” incluem armas e sistemas que usam computadores ou redes.

3.1 A guerra cibernética

Dadas as enormes diferenças críticas entre a guerra cibernética e a guerra no espaço físico, pode-se afirmar que os princípios que orientam o uso da força física não possuem a mesma validade no espaço cibernético.

Parafraseando a estratégia de defesa cibernética dos Estados Unidos da América, podemos dizer que garantir a segurança do espaço cibernético é fundamental para proteger a segurança nacional americana e promover a prosperidade dos cidadãos americanos. O espaço cibernético é um componente integral de todas as facetas da vida americana, incluindo sua economia e defesa. No entanto, suas entidades públicas e privadas ainda lutam para proteger seus sistemas, e os adversários aumentaram a frequência e a sofisticação de suas atividades cibernéticas maliciosas. De acordo com Estados Unidos da América (2011), a América criou a Internet e compartilhou com o mundo. Agora, deve se certificar de proteger e preservar o espaço cibernético para as gerações futuras.

No Brasil, a preocupação com a guerra cibernética se torna clara quando se analisa sua doutrina militar de defesa cibernética. Este documento afirma que:

> A Defesa Cibernética vem se estabelecendo como atividade fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle (C^2), por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse exercício seja negado ao oponente. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares. (BRASIL, 2014, p.13).

Já a doutrina básica da Força Aérea Brasileira prevê que:

> Nesse contexto, também deve ser considerado o controle do ambiente cibernético, conformado por Sistema de Comunicações e Tecnologia da Informação para Comando e Controle (SCTIC2), que são vitais para troca de informações entre todos os escalões da cadeia de comando. O domínio do ambiente cibernético pode, direta ou indiretamente, afetar as lideranças, as forças militares e as

> infraestruturas críticas do inimigo, até o ponto de evitar a confrontação militar direta. (BRASIL, 2012, p. 43).

Nota-se então a preocupação dos Estados Unidos da América, das Forças Armadas Brasileiras e, em especial, da Força Aérea Brasileira com a defesa da informação no ambiente cibernético. Os ataques cibernéticos são iniciados pela exposição de sistemas alvo a qualquer entidade no mundo, conjuntamente com a divulgação de falhas de segurança nestes sistemas que serão exploradas. Vale citar que os proprietários dos sistemas, geralmente, não possuem consciência exata das falhas existentes, caso contrário, elas não perdurariam por muito tempo. Eles talvez não sejam capazes de perceber o quanto estão expostos ao resto do mundo.

Os pré-requisitos para um ataque cibernético são pessoas inteligentes mal intencionadas, denominadas de *hackers*, computadores com hardware de baixo custo, uma conexão a rede mundial de computadores ou a rede local do alvo desejado, conhecimento sobre o funcionamento do sistema de destino, suas vulnerabilidades e ferramentas capazes de explorá-las. Nenhum desses pré-requisitos são exclusividades dos Estados, embora alguns tenham mais facilidade que outros em sua aquisição.

A atribuição dos responsáveis por um ataque cibernético é um trabalho árduo, pois determinar a rede ou o equipamento específico que originou o ataque já é um desafio extremamente custoso e que, por si só, não é capaz de provar a responsabilidade de seu proprietário, pois há muitas formas de que o *hacker* altere a origem de seu ataque para outra pessoa. E ainda, mesmo que se consiga encontrar o atacante específico, ainda há que se provar a responsabilidade de suas ações por parte de algum Estado.

Outro trabalho complexo é conseguir prever os efeitos causados por um ataque cibernético, mesmo aquele que tenha sido direcionado contra um alvo bem definido. Os sistemas mudam constantemente; processos que dependem de danos colaterais dos sistemas afetados não são prontamente aparentes e não podem necessariamente ser inferidos de suas propriedades físicas. O custo final de, digamos, uma interrupção é proporcional ao tempo necessário para detectar, caracterizar e reverter seu dano, tudo isso pode variar muito. Mesmo depois de um ataque cibernético, pode não estar claro o que exatamente aconteceu, um ataque de corrupção de dados, por exemplo, perde muito de sua força se o alvo souber exatamente o que foi corrompido. Segundo LIBICKI (2011), o que um invasor acredita ter feito pode diferir do que aconteceu, o que, por sua vez, pode diferir do que o alvo percebeu que aconteceria.

3.2 Conceitos e componentes cibernéticos

Quando se fala em segurança cibernética, a maioria dos Estados ao iniciar seu processo de construção das Estratégias de segurança cibernética, inicia descrevendo a importância de “proteger suas informações”, implementar a “segurança de computadores” ou a “segurança das informações”. Em geral, esses termos contêm princípios básicos de proteção e conservação da confiabilidade, integridade e disponibilidade das informações. Para a segurança da informação pouco importa se os dados são digitais, impressos ou se possuem outra forma, ela concentra-se nos dados.

> A segurança pode ser definida como o estado de estar livre de perigo e não estar exposto a danos causados por acidentes ou ataques, ou pode ser definido como o processo para atingir esse estado desejável. O objetivo da segurança de computadores é aperfeiçoar o desempenho de uma organização em relação aos riscos aos quais ela está exposta. (BOSWORTH; KABAY; WHYNE, 2014, p. 46, tradução nossa).

Nota-se, no conceito, que não há uma preocupação com as informações armazenadas ou processadas pelo computador.

Conforme Sêmola (2003), segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Já a NBR ISO/IEC 27002:2013 identifica como atributos básicos para segurança da informação: confidencialidade, integridade, disponibilidade e quaisquer requisitos necessários para a informação.

Apesar dos termos abordarem de forma ligeiramente diferente o mesmo tema, frequentemente são permutados. Em sua maioria, ações não autorizadas que afetem a um ou mais princípios fundamentais ou atributos da segurança da informação, são consideradas crime em quase todos os Estados.

A crescente dependência por produtos e serviços de Tecnologia da Informação, a chegada da internet das coisas facilita a exposição de sistemas e redes de computadores à exploração maliciosa. Tal afirmação fica evidente na Figura 3.

Figura 3 - A "Internet das Coisas" aumenta a vulnerabilidade ao ataque

Fonte: North Atlantic Treaty Organization (2019)

A segurança da Tecnologia da Informação e Comunicações (TIC) está ligada às origens técnicas da segurança do computador e, ao mesmo tempo, relacionada aos princípios de segurança da informação. Desta forma engloba, além dos dispositivos conectados à internet, sistemas e equipamentos que não estejam conectados a nenhuma rede. É interessante frisar que o termo segurança de TIC exclui as questões de conteúdo ilegal, exceto quando este conteúdo danifique diretamente o sistema que está em verificação.

Por fim, no sentido de abranger os conceitos acerca do tema tratado, o presente estudo adota as seguintes conceituações contidas no Manual de Guerra Cibernética do Exército Brasileiro:

a) “AMEAÇA CIBERNÉTICA – causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse;”(BRASIL, 2017)
b) “ARTEFATO CIBERNÉTICO – equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos;” (BRASIL, 2017)
c) “ATIVOS DE INFORMAÇÃO – meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo

geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;" (BRASIL, 2017)

d) "CIBERNÉTICA – termo que se refere a comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação;" (BRASIL, 2017)
e) "DEFESA CIBERNÉTICA – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente;" (BRASIL, 2017)
f) "ESPAÇO CIBERNÉTICO – espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas;" (BRASIL, 2017e)
g) "FONTE CIBERNÉTICA – recurso que possibilita a obtenção de dados no espaço cibernético, utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A fonte cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de inteligência;" (BRASIL, 2017)
h) "GUERRA CIBERNÉTICA – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 AO adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sistemas de Informação. 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 às TIC;" (BRASIL, 2017)
i) "INFRAESTRUTURA CRÍTICA DA INFORMAÇÃO – subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do estado e a segurança da sociedade;" (BRASIL, 2017)

j) “PODER CIBERNÉTICO – capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder;” (BRASIL, 2017)
k) “RESILIÊNCIA CIBERNÉTICA – capacidade de manter as infraestruturas críticas da informação operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa;” (BRASIL, 2017)
l) “RISCO CIBERNÉTICO – probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado;” (BRASIL, 2017)
m) “SEGURANÇA CIBERNÉTICA – arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas;” (BRASIL, 2017)
n) “SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações;” (BRASIL, 2017)
o) “SETOR CIBERNÉTICO – um dos três setores de importância estratégica para a defesa nacional, de acordo com a Estratégia Nacional de Defesa, abrangendo as pessoas, instalações, infraestruturas e recursos tecnológicos, de nível estratégico, necessários para que as FA possam atuar em rede com segurança, tais como o Sistema Militar de Comando e Controle (SISMC2), sistemas de armas/vigilância e sistemas administrativos que possam afetar as atividades operacionais.” (BRASIL, 2017)

3.3 O aumento da importância da guerra cibernética no cenário internacional

Esta seção pretende apresentar algumas características da guerra cibernética e, mostrar o posicionamento de alguns Estados sobre o assunto, conjuntamente com as questões de segurança cibernética. Em primeiro lugar é importante frisar a necessidade da presença direta ou indireta de um ator estatal, para que se configure a guerra cibernética. Ao se falar da presença indireta, reforça-se uma característica comum e, ao mesmo tempo, valiosa no ambiente cibernético, o anonimato. Para o ataque ocorrido no

espaço cibernético, pouco importa a distância física entre o atacante e o atacado, já que este é capaz de se esconder em um equipamento localizado em qualquer parte do globo. Além destes aspectos, o atacante é capaz de facilmente esconder seus rastros, fato que dificulta o encontro da origem ofensiva. Outrossim, é comum o atacante estar inserido em estruturas de governo e sociais, transformando-se assim no que podemos chamar “guerra por procuração”. Nesse sentido, indivíduos (*hackers* ou *hacktivistas*) ou ainda grupos *hacker* acabam assumindo a autoria dos ataques e, ao mesmo tempo, isentando a culpa dos Estados a que pertencem.

Alguns dos principais países, como a China, adaptaram suas estratégias militares para as características do ambiente cibernético, conforme citado por WU (2006). Casos reais de “guerra cibernética” e estratégias explícitas formuladas por analistas governamentais e militares pelo mundo atraíram mais estudantes para o objeto do conflito no espaço cibernético.

Em 2007 um jornal militar russo declarou:

> isolar o terrorismo cibernético e o crime cibernético a partir do contexto geral da segurança da informação internacional é, em certo sentido, artificial e sem suporte... é principalmente a motivação que distingue atos de terrorismo cibernético, crimes cibernéticos e ataques cibernéticos militares... sem saber a motivação não se pode qualificar o que está acontecendo como criminoso, terrorista ou ato político-militar. Tanto que as fontes de ataques cibernéticos podem facilmente receber uma classificação como ações criminosas ou terroristas. (KLIMBURG, 2011, p. 41, tradução nossa).

Estudantes na área de segurança começaram a dar mais atenção ao espaço cibernético, depois que ele esteve envolvido em um domínio importante de um conflito entre Estados.

Um detalhe importante a se considerar na guerra cibernética é o fato dela só fazer sentido se produzir efeitos no mundo cinético, ou seja, se afetar alguém ou alguma coisa no mundo real. Tal afirmação é corroborada tendo por base um dos oito princípios propostos por Parks e Duggan (PARKS; DUGGAN, 2011): o princípio de Efeitos Cinéticos.

Libicki (2012) aponta que nos últimos 20 anos, houve muitos casos de crime cibernético e espionagem cibernética. Dentre os casos mais conhecidos, cita três ataques cibernéticos que poderiam chegar ao nível de uma guerra cibernética: os ataques DDOS contra a Estônia em 2007, um ataque semelhante à Geórgia em 2008, o worm Stuxnet (2009–2010). Frisa-se que apenas o caso do *Stuxnet,* não foi acompanhado por violência, fato que tende a criar suas próprias tensões. Em parte por esse motivo, nenhum deles gerou uma crise cibernética.

Apesar das dificuldades de se encontrar a origem dos ataques citados anteriormente, inclusive de se comprovar sua existência, o princípio dos efeitos cinéticos é facilmente identificado.

3.3.1 Ataque à Estônia

Em 2007 a Estônia sofreu uma campanha de ataques cibernéticos que, temporariamente prejudicou sua economia. Não há como se falar deste ataque, sem remontar o cenário da época.

> Para compreender a motivação destes ataques é necessário retornar ao final da Segunda Guerra Mundial. Com a Grande Guerra Patriótica o Exército Vermelho tirou a Estônia do domínio Nazista, forçando-a se integrar à União das Repúblicas Socialistas Soviéticas (URSS). Após o período de domínio Soviético, com a desintegração da URSS, a Estônia se tornou independente e estabeleceu novamente sua capital em Talin. Durante seu domínio, para que os povos do leste Europeu se lembrassem dos sacrifícios feitos para libertá-los dos nazistas, a URSS ergueu em muitas capitais da região grandes estátuas de um heroico soldado do Exército Vermelho. E assim também o fez em Tallin. (SÁ, MACHADO, ALMEIDA, 2018, p. 18).
>
> Tais estátuas eram vistas com muito apreço pelos líderes soviéticos. No entanto, aos olhos dos estonianos, a estátua erguida em Tallin representava um símbolo das cinco décadas de opressão que eles foram obrigados a passar como parte da URSS (CLARK; KNAKE, 2010). Assim, em 2007, atendendo aos sentimentos da população, o legislativo da Estônia aprovou a Lei das Estruturas Proibidas que determinava a remoção da estátua do soldado do Exército Vermelho, o que desagradou Moscou. Para evitar um incidente, o então presidente da Estônia vetou a lei. Nesse contexto, as pressões em torno da preservação, ou não do símbolo soviético aumentaram. (SÁ, MACHADO, ALMEIDA, 2018, p. 18).
>
> De um lado a opinião pública estoniana defendia a remoção da estátua e um grupo nacionalista a tentava destruir. De outro, grupos étnicos russos dedicados a protegê-la se tornavam cada vez mais ativos. Esse conflito culminou em uma revolta, conhecida como a Noite de Bronze (KAISER, 2015), que se seguiu da remoção da estátua para um cemitério militar. Foi quando o conflito migrou para o ciberespaço.(SÁ, MACHADO, ALMEIDA, 2018, p.19).

Nesse ponto, diversos ataques virtuais impactaram negativamente a infraestrutura de TIC da Estônia, fato que comprometeu seus serviço derivados. Considera-se que foi o maior ataque registrado até aquele momento. Nesse ínterim, o governo estoniano comunicou o caso ao conselho do Atlântico Norte, que investigou este atentado a soberania cibernética da Estônia e acabou por criar o CCD COE. A Estônia acusou o governo Russo da autoria dos ataques entretanto isso nunca foi provado. Libicki (2012) afirma que tal ataque dificilmente seria possível de ser realizado sem o apoio de um grande ator estatal.

Um dos fatos que dificulta a descoberta da origem destes ataques, por exemplo, foi a utilização de diversas redes fantasmas, chamadas de *botnets* ao redor do mundo.

> Aproximadamente um sexto de todo o tráfego DDOS direcionado contra a Estônia em 2007 veio de computadores nos Estados Unidos. O governo dos EUA deve e pode ser obrigado a tomar medidas para conter a inundação? Seus ISPs devem aceitar a responsabilidade de bloquear esses pacotes e seus governos devem indenizá-los contra clientes irritados se o fizerem? É possível parar pacotes incorretos em um endereço sob ataque sem interromper todos os pacotes? Os ISPs devem identificar proativamente os clientes cujos computadores se tornaram bots (isto é, sob o controle de um hacker) e negar a eles acesso à Internet até que se limpem? (LIBICKI, 2012, p. 24, tradução nossa).
> Talvez não. Tais obrigações podem não constituir uma prática doméstica econômica, mesmo que a Internet seja apenas um fenômeno dos EUA. Assim, chamando-os internacionalmente pode não fazer mais sentido. (LIBICKI, 2012, p. 24, tradução nossa).

Os estados podem criar suas próprias ações para reduzir as chances de que outro estado tenha um motivo legítimo ou quase legítimo de levar as coisas ao modo de crise. Até a Estônia em 2007 - um estado que não fez mais do que exercer seus direitos soberanos (para realocar um monumento de guerra) - teve a opção de fazer uma crise internacional a partir da onda de ataques distribuídos de negação de serviço (DDOS) em sites governamentais e comerciais. Na verdade, ela tinha uma crise e necessitava restaurar rapidamente os serviços da Internet. Mas, no final, decidiu não brigar com a Rússia. E, como resultado de algumas alterações de engenharia em suas redes, a Estônia é um alvo mais difícil hoje.

3.3.2 Guerra Russo-Georgiana

A Geórgia sofreu ataques cibernéticos similares aos da Estônia em 2008, como um elemento de sua guerra com a Rússia. Em situação diferente do caso anterior, os ataques cibernéticos à Geórgia precederam uma guerra convencional. Pode-se dizer que este foi a primeira vez que uma situação como esta ocorreu.

Os sites do Governo da Geórgia foram retirados do ar poucos dias antes do início da sua guerra com a Rússia, além disso, sua infraestrutura de TI também fora severamente danificada.

Sá, Machado e Almeida (2018) relatam assim os fatos ocorridos na Geórgia:

> Antes que os ataques cinéticos começassem, ataques cibernéticos já atingiam sites do governo georgiano. Ao longo do conflito, a Geórgia sofreu ataques DDoS direcionados aos seus meios de comunicação, com o objetivo de dificultar que os georgianos percebessem o que estava acontecendo. Os sistemas bancários, de cartões de crédito e de telefonia móvel foram afetados. A maioria dos roteadores que conectavam a Geórgia à Internet, via Turquia e Rússia, foram atacados. A Geórgia perdeu o acesso às fontes de informação e notícia externas. No auge da ofensiva, seis botnets foram mobilizadas para gerar o tráfego de ataque (CLARK; KNAKE, 2010). Embora alguns especialistas considerem que a coordenação entre os ataques cibernéticos e cinéticos tenha sido baixa (SHAKARIAN, 2011), e os russos alegarem que os ataques cibernéticos estavam fora do comando do

> Kremlin (CLARK; KNAKE, 2010), alguns eventos identificados sugerem ter havido tal coordenação. As instalações físicas da mídia e de sistemas de comunicação, por exemplo, não sofreram ataques cinéticos, apenas cibernéticos. Além disso, hackers russos atacaram um site usado para aluguel de geradores elétricos a diesel, provavelmente em complemento aos ataques convencionais que atingiram a infraestrutura elétrica do país (SHAKARIAN, 2011). É digno de nota que, segundo (SHAKARIAN, 2011), os objetivos de isolar e desgastar a Geórgia foram limitados em seu escopo, tendo os atacantes evitado causar danos permanentes às redes georgianas e aos seus sistemas SCADA. (SÁ, MACHADO, ALMEIDA, 2018, p. 20).

Entende-se que tais eventos abrem o caminho para a investigação do papel da guerra cibernética como membro integrante do teatro de operações da guerra do século XXI.

3.3.3 Stuxnet

Em Junho de 2010 uma empresa situada na BieloRússia, fazendo negócios no Iran, descobriu um vírus de computador extremamente sofisticado chamado *Stuxnet*. O *Stuxnet* era incrivelmente avançado, um *worm* que provavelmente levou anos para ser construído e foi desenvolvido com a capacidade de pular de um computador para outro até que chegasse a um alvo específico, que neste caso, foi o programa de enriquecimento nuclear do Iran, que parecia ser impenetrável. Por razões de segurança, ele foi construído com diversos níveis abaixo do nível do solo e não é conectado à Internet. Entretanto o vírus tinha que encontrar o caminho através de um grupo de computadores desconectados. Ele tinha que se adaptar às diversas medidas de segurança até chegar a um computador que fosse capaz de garantir o acesso à planta nuclear. Ele foi projetado de tal maneira que quando encontrasse seu alvo, secretamente manipularia os dados da planta até que estivesse tão comprometida a ponto de parar suas funções normais. Depois de atingir seus objetivos ele deveria se autodestruir sem deixar nenhum rastro.

O vírus foi aparentemente bem sucedido em encontrar seu alvo, que eram as instalações nucleares do Irã. Ele entrou nos sistemas operacionais de todas as instalações e, então, se modificou quando foi descoberto. Stuxnet foi aparentemente desenhado assumindo que algum funcionário da planta iria levar trabalho para casa em um *flash drive,* sendo infectado, e então sendo levado de volta a planta.

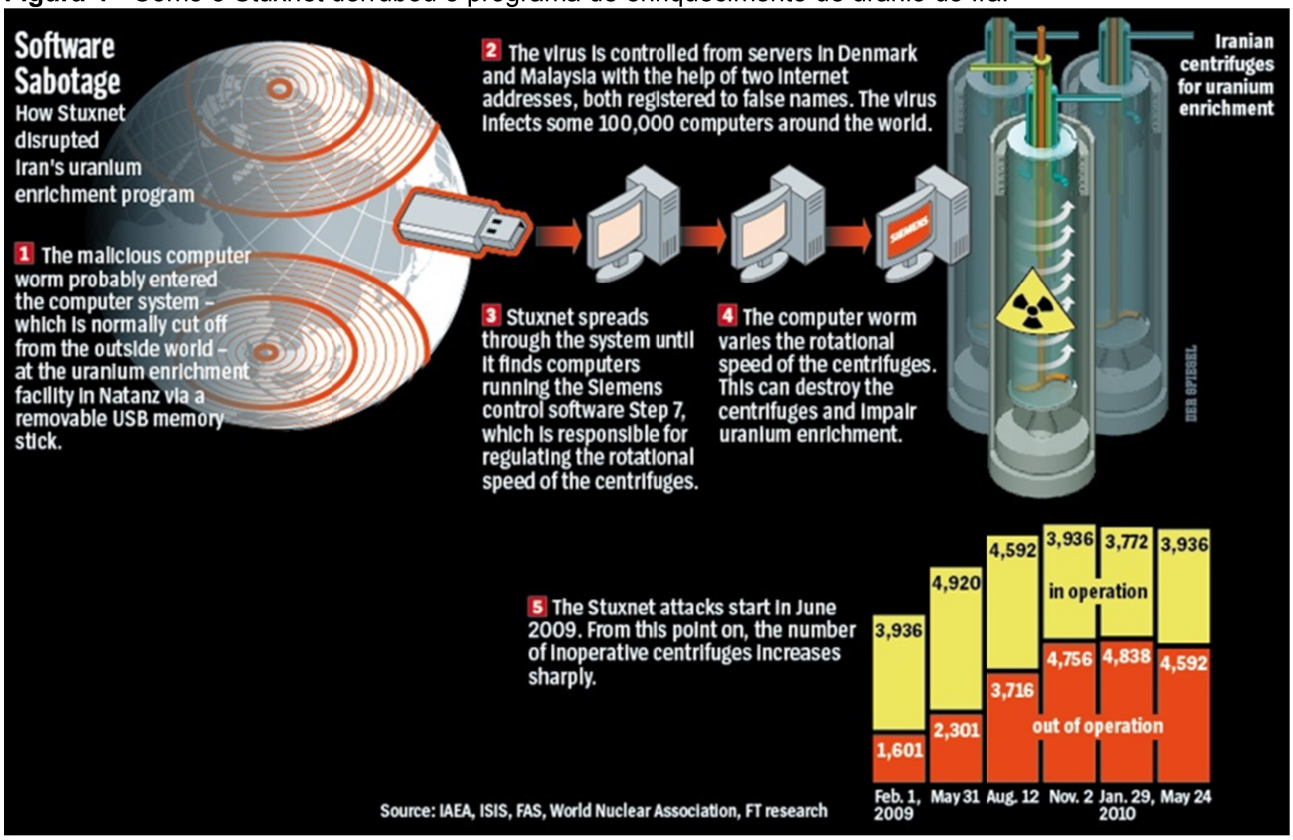
É interessante analisar o que o vírus foi capaz de fazer depois de invadir os sistemas operacionais das duas plantas. Depois de derrotar o sistema de segurança, o *worm* fez com que as centrífugas aumentassem sua rotação ao máximo e depois diminuia sua velocidade de forma abrupta danificando o conversor, as centrífugas e os

rolamentos, além de corromper o urânio que estava nos tubos. Ao mesmo tempo esta ação confundiu os engenheiros nucleares do Irã e os deixou tentando descobrir o que estava errado, porque os computadores de monitoramento não mostraram nenhum tipo de mal funcionamento. Estima-se que esta invasão levou mais de um ano, e foi capaz de deixar o programa iraniano em um verdadeiro caos e que o *worm cresceu e se adaptou* tornando-se extremamente sofisticado. A Origem do Vírus não foi identificada mas as evidências indicam uma instituição com uma capacidade muito sofisticada de atuar na guerra cibernética.

> O Stuxnet foi encontrado em 2010 e investigado por diversos especialistas ao redor do mundo (ZETTER, 2014), tanto da área de sistemas de controle industriais (LANGNER, 2011), quanto da área de segurança da informação (FALLIERE, 2011). As evidências e investigações apontam para a autoria conjunta de EUA e Israel (ZETTER, 2014). O Stuxnet é considerado uma prova de conceito de como as armas digitais podem afetar diretamente o mundo físico, sendo capazes de cumprir os mesmos propósitos estratégicos de ataques com armas cinéticas como mísseis e bombas. (SÁ, MACHADO, ALMEIDA, 2018, p. 22).

A Figura 4 apresenta a sequência realizada pelo Stuxnet.

Figura 4 - Como o Stuxnet derrubou o programa de enriquecimento de urânio do Irã.



Fonte: Rough Diplomacy (2017)

Por tudo apresentado, o Stuxnet é considerado até hoje uma arma cibernética, e demonstra como o espaço cibernético pode afetar diretamente o espaço cinético. Da mesma forma que o alvo fora as centrífugas, poderiam ser armas, satélites, sistemas de controle e planejamento.

4 SETOR CIBERNÉTICO

4.1 OTAN e a defesa cibernética

Em Setembro de 2014, a OTAN adotou uma política e um plano de ação aprimorados, visando acompanhar o cenário atual de mudanças rápidas e aprimorar seu sistema de defesa cibernética. De acordo com North Atlantic Treaty Organization (2018), esta política estabeleceu a defesa cibernética como parte da tarefa central da Aliança de defesa coletiva, confirmou que o direito internacional se aplica no espaço cibernético e intensificou a cooperação da OTAN com a indústria. A prioridade máxima é a proteção dos sistemas de comunicações próprios e operados pela Aliança.

Ainda de acordo com NATO (2018), a política de defesa cibernética da OTAN é complementada por um plano de ação com objetivos concretos e cronogramas de implantação em uma variedade de tópicos, desde desenvolvimento de capacidades, educação, treinamento e exercícios, e parcerias.

Nos dias 08 e 09 de Julho de 2016, ocorreu em Varsóvia, uma reunião que incluiu os 28 países-membros da OTAN e os países aliados, denominada Cimeira de Varsóvia.

Conforme NATO 2018, os aliados prometeram, na Cimeira de Varsóvia em 2016, reforçar as defesas cibernéticas das redes e infraestruturas nacionais, como uma questão prioritária. Com a adaptação contínua das capacidades de defesa cibernética da OTAN, como parte da adaptação em longo prazo da OTAN, isto reforçará a defesa cibernética e a resiliência global da Aliança.

Em Varsóvia, os Aliados também reafirmaram o mandato defensivo da OTAN e reconheceram o espaço cibernético como um domínio de operações em que a OTAN deve se defender tão eficazmente quanto no ar, em terra e no mar. Como a maioria das crises e conflitos tem hoje uma dimensão cibernética, entende-se que o tratamento do espaço cibernético como um domínio seja capaz de permitir à OTAN proteger e conduzir melhor as suas missões e operações.

A seguir, na continuação do presente capítulo, é apresentada a situação atual no campo cibernético de Brasil, Estados Unidos e Alemanha, assim como se destaca a tendência da criação de uma Força Armada exclusiva para o espaço cibernético. Conforme será demonstrado abaixo Estados Unidos e Alemanha já possuem seus comandos cibernéticos. Nota-se ainda que tal criação é corroborada pela OTAN, a partir do reconhecimento do espaço cibernético como um domínio de operações.

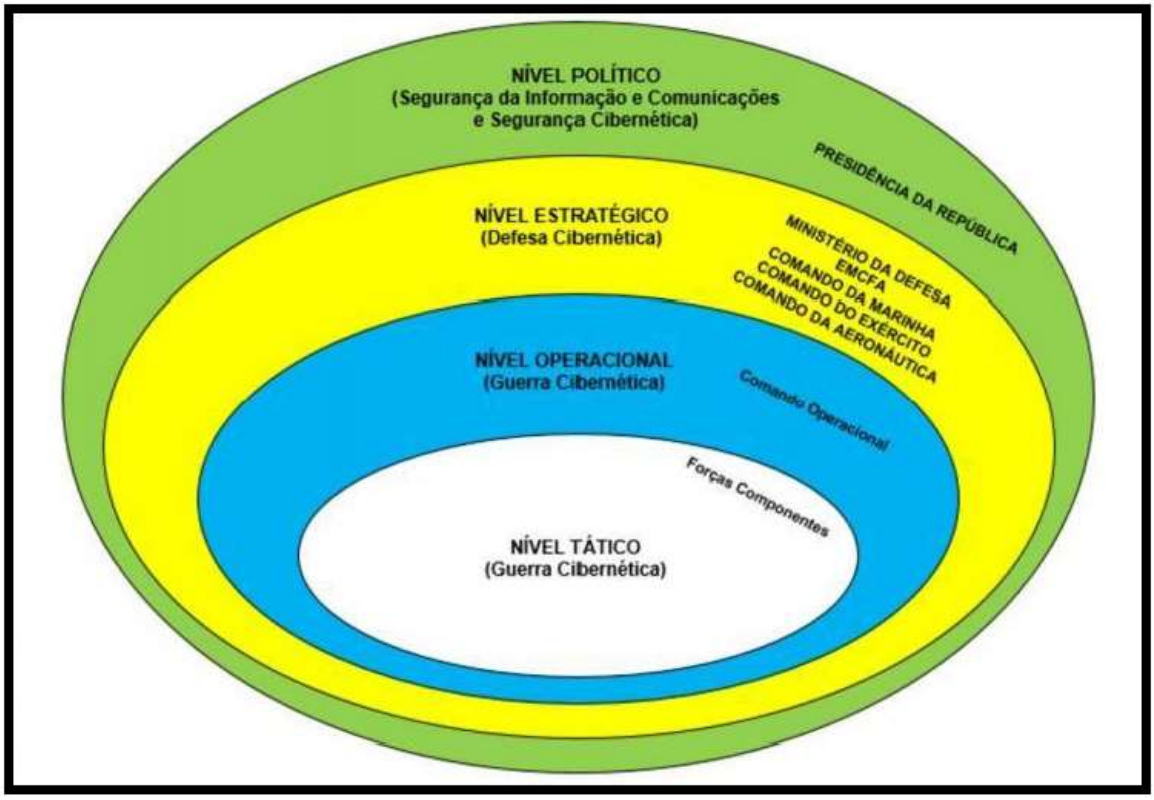
4.2 Brasil e a defesa cibernética

O Brasil pode ser classificado como uma potência sul-americana, por esta razão é uma vítima potencial de ataques cibernéticos oriundos de qualquer parte do globo. Isto ocorre porque além de grande população, o país possui dimensões continentais, e é considerado a 9ª maior economia do mundo (FUNDAÇÃO ALEXANDRE GUSMÃO, 2017); É possuidor ainda da maior bacia hidrográfica do planeta, a bacia Amazônica, tendo em sua floresta o maior bioma do país. Além disso, por ser a maior economia da América do Sul, possui forte influência política e econômica em seus vizinhos. Pelo exposto pode ser considerado um valioso alvo para ataques cibernéticos.

A partir do ano de 2008, com a publicação da END, o setor cibernético passou a ser reconhecido no Brasil e, acabou sendo dividido em três campos distintos: a segurança cibernética, a defesa cibernética e a guerra cibernética.

As ações no espaço cibernético foram então divididas de acordo com seu nível de decisão (conforme Figura 5):

Figura 5 - Níveis de decisão no Espaço Cibernético



Fonte: Brasil (2017, p. 15)

a) nível político – Segurança da Informação e Comunicações e Segurança Cibernética – coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais; (BRASIL, 2017)

b) nível estratégico – Defesa Cibernética – a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das Forças Armadas (FA), interagindo com a Presidência da República e a APF; e (BRASIL, 2017)

c) níveis operacional e tático – Guerra Cibernética – denominação restrita ao âmbito interno das FA. (BRASIL, 2017)

Os órgãos da APF que são responsáveis por auxiliar à Presidência da república nas atividades relativas ao Setor Cibernético estão apresentadas a seguir:

4.2.1 Conselho de Defesa Nacional (CDN)

O Conselho de Defesa Nacional (CDN), órgão consultivo do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do estado

democrático, tem sua organização e funcionamento disciplinados na Lei 8.183, de 11 de abril de 1991.

A execução das atividades permanentes necessárias ao exercício de competência constitucional do CDN é realizada pela Secretaria-Executiva do Conselho de Defesa Nacional, por intermédio do Gabinete de Segurança Institucional da Presidência da República. Cabe ao Ministro-Chefe do Gabinete de Segurança Institucional exercer a função de Secretário-Executivo do Conselho de Defesa Nacional. (BRASIL, 2019a)

4.2.2 Câmara de Relações Exteriores e Defesa Nacional (CREDEN)

A CREDEN é um órgão de assessoramento da Presidência da República em matérias relacionadas às relações exteriores e Defesa Nacional do Governo Federal. É presidido pelo Chefe do Gabinete de Segurança Institucional da Presidência da República – GSI PR.

4.2.3 Casa Civil da Presidência da República

A Casa Civil da Presidência da República está relacionada com o setor cibernético por meio do Instituto Nacional de Tecnologia da Informação ITI. O objetivo deste instituto é manter a infraestrutura de chaves públicas Brasileiras (ICP-Brasil), a qual é a primeira autoridade da cadeia de certificação digital.

Este certificado digital serve para dar uma identidade única para o cidadão, empresas e equipamentos, dentro do espaço cibernético. Por esta razão, associado a legislação vigente, da validade jurídica aos atos praticados através do seu uso.

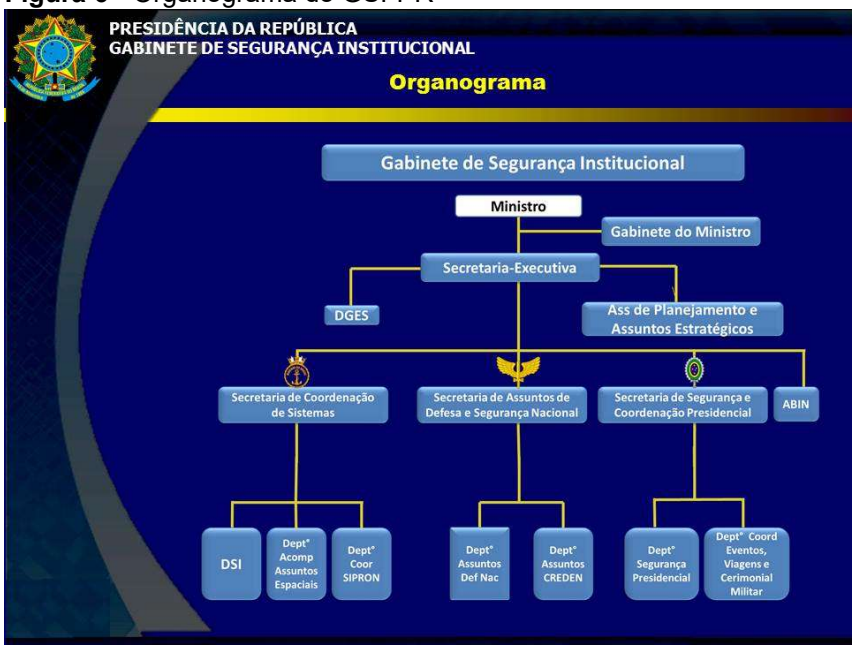
4.2.4 Gabinete de Segurança Institucional da Presidência da República

De acordo com o decreto Nr.° 9.668, de 02 Jan 19, ao GSI-PR, dentre outras atribuições, compete:

> V – planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas; (BRASIL, 2019b).

Para cumprir suas atribuições, o GSI-PR conta, no que tange à segurança cibernética com órgãos subordinados conforme Figura 6 e, descritos abaixo dentro de sua relevância para o presente estudo.

Figura 6 - Organograma do GSI-PR



Fonte: Brasil (2019)

4.2.5 Departamento de Segurança da Informação e Comunicações (DSIC)

De acordo com o art. 11 do decreto 9.668 de 2 de janeiro de 2019, compete ao DSIC:

"I – planejar, e supervisionar a atividade nacional de segurança da informação, no âmbito da administração pública federal, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;"

"II – formular e implementar políticas públicas de segurança da informação;"

"III – elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;"

"IV – manter Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo-CTIR Gov, de responsabilidade nacional, para a proteção cibernética;"

“V – coordenar e realizar ações destinadas à gestão de incidentes computacionais, no que se refere à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes computacionais de responsabilidade nacional;”

“VI – coordenar a rede de equipes de tratamento e resposta a incidentes computacionais-CSIRTs, formada pelos órgãos e pelas entidades governamentais;”

“VII – propor e participar de tratados, acordos ou atos internacionais relacionados à segurança da informação, em especial, ao tratamento e à troca de informação sigilosa;”

“VIII – assistir o Gabinete de Segurança Institucional da Presidência da República no exercício das funções de Autoridade Nacional de Segurança para o tratamento de informação classificada decorrente de tratados, acordos e atos internacionais;”

“IX – atuar como órgão central de credenciamento de segurança para o tratamento de informação classificada;”

“X – fiscalizar o credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para o tratamento da informação sigilosa;”

“XI – articular, para o estabelecimento de diretrizes para as políticas públicas de Segurança da Informação, com os governos dos Estados, do Distrito Federal e dos Municípios, com a sociedade civil e com órgãos e entidades do governo federal;” e

“XII – exercer outras atribuições determinadas pelo Secretário de Coordenação de Sistemas.”

Das competências acima elencadas, nota-se então a relevância deste Órgão no que tange a segurança da informação e comunicações, visto que, dentre outras atividades, em suma é ele quem regulamenta as atividades de segurança da informação e comunicações dentro da Administração Pública Federal (APF), realiza acordos internacionais e troca de informações sigilosas e Mantém o Centro de Tratamento e Resposta a Incidentes de Rede da APF (CTIR. Gov).

4.2.6 Agência Brasileira de Inteligência (ABIN)

A ABIN é um órgão cujo papel é fornecer ao presidente da República e a seus ministros informações e análises estratégicas, oportunas e confiáveis, necessárias ao processo de decisão.

É órgão central do Sistema Brasileiro de Inteligência (Sisbin), e sua missão é assegurar que o Executivo Federal tenha acesso a conhecimentos relativos à segurança do Estado e da sociedade, como os que envolvem defesa externa, relações exteriores,

segurança interna, desenvolvimento socioeconômico e desenvolvimento científico-tecnológico.

Conta ainda, em sua estrutura, com o Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (CEPESC), que é a área responsável por desenvolver programas e ferramentas capazes de garantir a transmissão segura de informações do Governo Federal.

Em relação ao campo cibernético há de se destacar, em suas atribuições, a avaliação de ameaças internas e externas à ordem constitucional, entre estas, a cibernética.

4.2.7 Breve histórico da defesa cibernética no âmbito das forças armadas

Por meio da Diretriz Ministerial n° 0014/2009, o Exército Brasileiro recebeu a atribuição de coordenar e integrar as ações pertinentes à Defesa Cibernética dentro das Forças Armadas.

A diretriz ministerial dividiu os trabalhos para sua implementação em 2 fases: a primeira fase contemplou a abrangência do tema e a proposição dos objetivos setoriais. Já a segunda fase, incluiu a proposição de ações estratégicas para a consecução dos objetivos setoriais, avaliando a adequabilidade das estruturas existentes nas Forças Armadas com vista à coordenação e integração do Setor Cibernético.

A Portaria Normativa n°666 de 4 de agosto de 2010, cria o Centro de Defesa Cibernética do Exército (CDCiber), o qual acabou sendo inaugurado apenas no ano de 2012.

A preocupação do governo brasileiro com a área cibernética fez surgir em 2015, com ativação em 2016, uma nova estrutura no setor cibernético brasileiro, o Comando de Defesa Cibernética – ComDCiber, unidade subordinada ao Comando do Exército. O principal objetivo desta nova unidade é planejar, coordenar, conduzir, integrar e supervisionar ações cibernéticas no âmbito da defesa, além de atuar como órgão central do Sistema Militar de Defesa Cibernética – SMDC.

O ComDCiber é estruturado da seguinte maneira:

“– Estado-Maior Conjunto (EMCj), voltado para a doutrina e planejamento estratégico de emprego conjunto das Forças Armadas em Defesa Cibernética, participando da elaboração dos Planos Estratégicos de Emprego Conjunto das Forças Armadas (PEECFA)”; (TECNOLOGIA & DEFESA, 2018)

“– Centro de Defesa Cibernética (CDCiber), como o braço operacional para as ações de Defesa Cibernética”; (TECNOLOGIA & DEFESA, 2018)

“– Departamento de Gestão e Ensino (DGE), voltado para as atividades de Gestão estratégica, ensino e capacitação de recursos humanos”; (TECNOLOGIA & DEFESA, 2018) e

“– Escola Nacional de Defesa Cibernética (ENaDCiber) como centro polarizador de ensino e pesquisa de Defesa Cibernética”. (TECNOLOGIA & DEFESA, 2018)

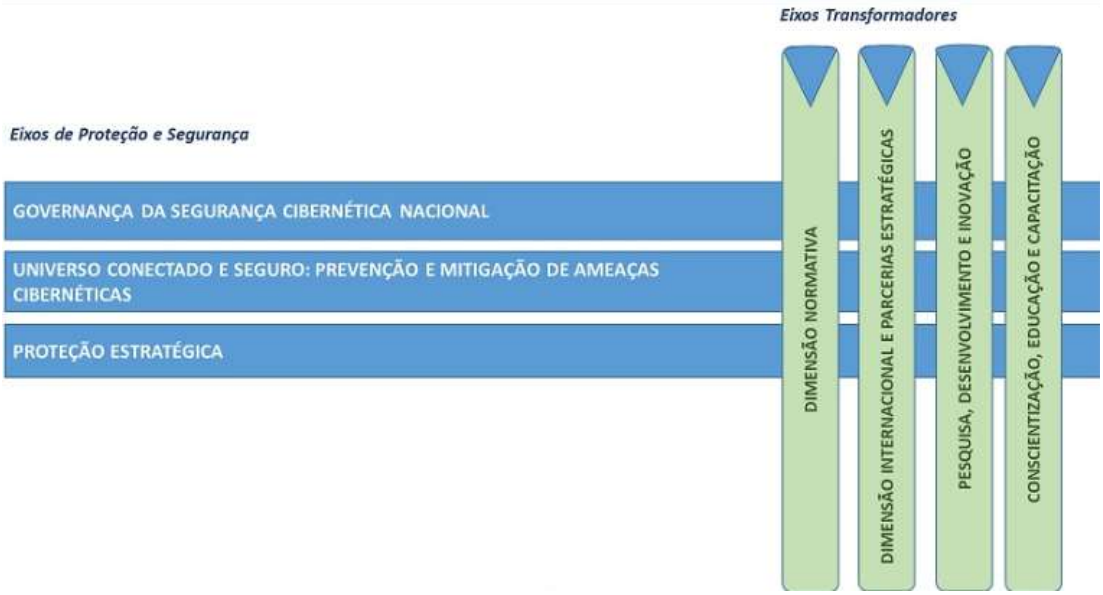
O ComDCiber ainda tem participação importante na integração entre os setores público, privados e o meio acadêmico. Exercícios simulados como o “Exercício Guardião Cibernético 2.0”, ocorrido em Julho de 2019, proporcionam um ambiente colaborativo com grande aproximação entre os setores envolvidos e buscam o desenvolvimento de capacidades de prevenção e solução de incidentes envolvendo ativos de informação de relevância ao Estado Brasileiro.

4.2.8 Estratégia cibernética brasileira

Em Outubro de 2018, foi criado pelo Gabinete de Segurança Institucional um grupo de trabalho interministerial, com vistas a se construir uma Estratégia Nacional de Segurança Cibernética. Participaram desse grupo empresas de Tecnologia da Informação e Comunicações, empresas de energia, universidades, centros de pesquisa, entre outros.

Em junho de 2019, este grupo apresentou sete eixos temáticos de atuação relacionados à segurança cibernética, conforme figura 7, com base nos principais problemas elencados no país.

Figura 7 - Eixos temáticos de atuação relacionados à segurança cibernética



Fonte: Brasil (2019a)

A Estratégia Nacional de Segurança Cibernética apresenta o posicionamento do Governo Federal sobre a segurança Cibernética. Já há o reconhecimento do Departamento de Segurança da Informação que os recursos de TI já envolvem toda a estrutura do Governo Federal, a atividade econômica, e a vida das pessoas em geral.

Segundo DSI 2019, desta forma, o GSI lançará no início do segundo semestre a consulta pública sobre a Estratégia, de modo que permita a participação de todos os atores envolvidos na temática. O DSI almeja a discussão das melhores práticas a serem adotadas pelo Brasil, com o objetivo de aumentar a resiliência brasileira às ameaças cibernéticas, tornar o País mais próspero e confiável no ambiente digital e fortalecer a atuação internacional brasileira em segurança cibernética.

Celles Cordeiro (2016) em seu estudo sobre uma nova taxonomia em relação às expressões de Poder Nacional, identifica como benefícios do isolamento do poder cibernético, em detrimento ao modelo atual:

> Uma capacidade mais objetiva de planejamento estratégico ao abranger a Complexidade do tema de maneira isolada permitindo um foco maior na Elaboração de políticas e estratégias para o setor por meio de uma visão holística do sistema, suplantando a visão setorial atual. (CORDEIRO, 2016, p.94).

E ainda:

> tem-se como entrave a evidente necessidade de criar uma estrutura para gerenciar, no nível estatal, tal organismo, principalmente para que haja uma hierarquia funcional dentro do aparato estatal sobre o tema bem como haja um interlocutor único sobre o assunto com o indivíduo e os agentes privados, elementos essenciais da questão. (CORDEIRO, 2016, p.94).

> Isso sem dúvida acarretaria em mudanças de curto, médio e longo prazo com resultados negativos de imediato (aumento da folha salarial e/ou desvio de função de servidores, por exemplo) cujos efeitos talvez só fossem sentidos depois de anos, o que torna a tarefa complexa do ponto de vista da opinião pública, e, consequentemente, do ponto de vista político. (CORDEIRO, 2016, p.94).

Em relação ao modelo atualmente existente, Cordeiro (2016) afirma:

> ….a premissa de que o cibernético pode ser subordinado às expressões atuais está errada. Sendo assim, o "meio" tornar-se-ia mais importante que o "fim", ocorrendo possivelmente uma inversão de valores e prioridades dentro do planejamento estratégico das expressões do Poder Nacional. (CORDEIRO, 2016, p.94).

Apesar do trabalho citado, observa-se que o Brasil ainda carece de discussões mais amplas acerca do tema.

4.3 Os Estados Unidos e a defesa cibernética

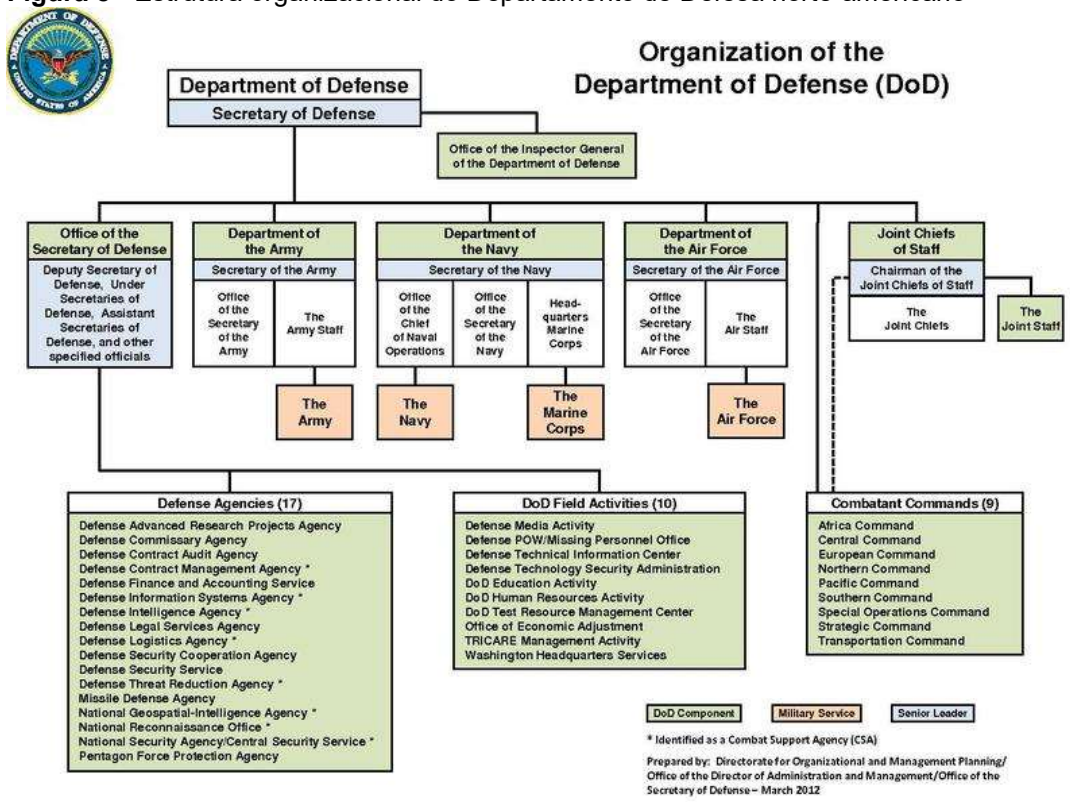
Com a chegada da Era da Informação e suas tecnologias, os Estados Unidos perceberam a necessidade consequente de projetar seu comando e controle e capacidades de informação em apoio de suas forças e na defesa dos interesses dos EUA globalmente. Para tal o Departamento de Defesa (em inglês, *Department of Defence* – DoD), equivalente ao Ministério da Defesa Brasileiro, também reconheceu a necessidade de proteger e defender seus sistemas vitais dos adversários e defender suas capacidades de informação nas operações militares.

Segundo Cruz Júnior (2013), os Estados Unidos têm como principal órgão responsável pela condução da política nacional de segurança da informação a *National Security Agency* (NSA). A NSA é a agência responsável por todas as questões afetas à segurança cibernética do governo norte-americano e compõe a estrutura do DoD.

Ainda segundo Cruz Júnior (2013), a NSA é ainda, a agência responsável pela segurança das comunicações e tecnologia da informação dos órgãos federais do governo norte-americano. Além disso, ela é a responsável por dar apoio ao DoD, à Comunidade de Inteligência (*U.S. Intelligence Community*), às agências de governo e aos parceiros na indústria com produtos e serviços relacionados ao espaço cibernético.

Na figura 8, é apresentado o arranjo institucional da defesa norte-americano.

Figura 8 - Estrutura organizacional do Departamento de Defesa norte-americano



Fonte: Wikimedia (2012)

Em junho de 2009 teve origem o Comando de Defesa Cibernética Norte-Americano (em inglês U.S. Cyber Command - USCyberCom), criado com a responsabilidade de coordenar as ações de prevenção e defesa cibernética norte-americanas.

O USCyberCom, como um Comando Unificado de Combatentes (CCMD), representa a mais recente evolução em uma série de projetos organizacionais para permitir as Redes de Informação do Departamento de Defesa (DoDIN) e otimizar as capacidades militares dos EUA no ciberespaço.

Em 1972, consultores do DoD alertavam sobre sérias vulnerabilidades na segurança de computadores e redes, e a importância do ciberespaço para a segurança nacional tornou-se uma preocupação premente após o fim da Guerra Fria.

Em 1995, o então diretor da Agência de Sistemas de Informação de Defesa (DISA), general Albert J. Edmonds, disse em um seminário na Escola de Governo John F. Kennedy, de Harvard, que as redes militares norte-americanas eram vulneráveis a ataques remotos. Essas preocupações aumentaram drasticamente à medida que exercícios cibernéticos como o ELIGIBLE RECEIVER 97 demonstravam vulnerabilidades na rede de defesa e destacavam o risco potencial associado à exploração da rede. Durante esse período, também ficou claro que as entidades estrangeiras eram cada vez

mais capazes de sondar as redes militares dos EUA e que elas poderiam interromper as operações militares. (UNITED STATES CYBER COMMAND, 2019)

Conforme UNITED STATES CYBER COMMAND (2019), o USCyberCom cumpre sua missão, por meio do uso de componentes cibernéticos retirados do serviço militar. Desde 2009, os serviços militares já começaram a reorganizar suas unidades cibernéticas com o intuito de criar unidades centrais, além daquelas que eram atribuídas à *USStratCom*. Essas unidades deveriam funcionar como comandos de componentes cibernéticos de serviços.

Em 2011 foi publicada pelos Estados Unidos sua Estratégia Internacional para o Espaço Cibernético (ESTADOS UNIDOS DA AMÉRICA, 2011). Em sua introdução, o documento reforça a relevância do tema para o desenvolvimento da humanidade e relaciona os benefícios da TI a um ambiente confiável e seguro.

O documento ainda deixa claro que os Estados Unidos não o consideram como somente uma visão do futuro para o espaço cibernético, mas também uma agenda para que se chegue nesse futuro. Ele demonstra a todos os interessados, seja países, sociedade civil, setor privado ou usuários, a necessidade de cooperação para que juntos seja possível preservar o caráter do espaço cibernético, bem como reduzir as suas vulnerabilidades.

Entretanto, um ponto importante a ser ressaltado é que o documento deixa clara a possibilidade de utilização de meios militares visando assegurar o seu direito de defesa. Dessa forma, ficam claras possíveis consequências de acontecimentos ocorridos no ambiente cibernético, fora do mundo virtual.

Ainda demonstrando sua crescente preocupação com o tema, o Presidente Americano Donald J. Trump, em agosto de 2017, acatou a recomendação do seu secretário de defesa, promovendo o USCyberCom de um comando sub-unificado do Comando Estratégico dos Estados Unidos (em inglês U.S. Strategic Command – USStratCom) a um comando Unificado de Combatentes responsável direto pelas operações no espaço cibernético. Com isso o USCyberCom tornou-se o 10° Comando de Combatentes Unificado na estrutura do DoD. Esta decisão pode ser ainda considerada como o reconhecimento da natureza mutável da guerra.

Em complemento à Estratégia Internacional, os Estados Unidos publicaram em setembro de 2018, sua Estratégia Nacional Cibernética. Este documento foca como os EUA irão:

a) “Defender a pátria protegendo redes, sistemas, funções e dados”; (ESTADOS UNIDOS DA AMÉRICA, 2018)
b) “Promover a prosperidade americana alimentando uma economia digital segura e próspera e promovendo uma forte inovação interna”; (ESTADOS UNIDOS DA AMÉRICA, 2018)
c) “Preservar a paz e a segurança fortalecendo a capacidade dos Estados Unidos – em conjunto com aliados e parceiros – de impedir e, se necessário, punir aqueles que usam ferramentas cibernéticas para fins maliciosos”; (ESTADOS UNIDOS DA AMÉRICA, 2018) e
d) “Expanda a influência americana no exterior para ampliar os princípios fundamentais de uma Internet aberta, interoperável, confiável e segura”. (ESTADOS UNIDOS DA AMÉRICA, 2018)

Para os Estados Unidos, o sucesso desta estratégia será alcançado quando as vulnerabilidades de segurança cibernética forem efetivamente gerenciadas por meio da identificação e proteção de redes, sistemas, funções e dados como: detecção de resiliência contrarresposta e recuperação de incidentes; destruir, desordenar ou até desestabilizar atividades cibernéticas contra os interesses dos Estados Unidos até que sejam reduzidas ou impedidas; atividade que são contrárias ao comportamento responsável no espaço cibernético e são dissuadidas através da imposição de custos por intermédio de meios cibernéticos e não-cibernéticos; e quando os Estados Unidos estiverem posicionados para usar recursos cibernéticos e alcançar os objetivos de segurança nacional.

Por fim, um aspecto fundamental destacado ao longo do documento é a luta contínua contra adversários estratégicos, casos de Rússia e China, por exemplo, e terroristas e criminosos. Dentre os riscos destacados está o uso de ferramentas cibernéticas para minar a economia e democracia, roubar a propriedade intelectual e semear discórdia em seus processos democráticos.

4.4 A Alemanha e a defesa cibernética

Nos últimos anos a comunidade europeia vem sentindo a instabilidade mundial, principalmente pela falta de liberdade, por crises e conflitos. Como exemplo cita-se o início dos conflitos na Síria em 2011, onde a partir de então, iniciou-se a chamada crise migratória. Segundo Deutsche Welle (2018), em 2015 a Alemanha abriu sua fronteira,

recebendo 890 mil solicitações de refúgio em apenas um ano, fato que ocasionou a reintrodução dos controles de fronteira.

Essa mudança nas condições de segurança, fez com que o Governo Federal Alemão em 2016 redefinisse seus interesses, suas prioridades e seus objetivos da política de segurança nacional, fato que culminou na publicação do seu: “LIVRO BRANCO – SOBRE A POLÍTICA DE SEGURANÇA ALEMÃ E O FUTURO DO *BUNDESWEHR* (Forças Armadas Alemãs)”.

Ao se analisar os últimos dez anos, observamos que diversos conflitos vêm ocorrendo na Europa, como é o caso ocorrido entre Rússia e Ucrânia. Ao mesmo tempo o aumento de ataques associados ao Estado Islâmico representa uma ameaça direta para o Estado Alemão e os demais países Europeus.

De acordo com Alemanha (2016), o espaço cibernético está se tornando cada vez mais um teatro de conflitos; a internet não é apenas uma força para o bem – ideologias de ódio e violência também se espalham por lá.

A Tabela 1 mostra que, em 2016, a Alemanha foi considerada a quarta maior economia do mundo. Tal fato fez com que este país assumisse um importante papel político mundial e, ao mesmo tempo, fosse um alvo cobiçado de ataques cibernéticos.

Tabela 1 - World economic outlook database (abril de 2017)

Produto Interno Bruto (PIB), em bilhões de US$, 2016

#	País	US$ bilhões
1º	Estados Unidos	18.569,10
2º	China	11.218,28
3º	Japão	4.938,64
4º	Alemanha*	3.466,64
5º	Reino Unido	2.629,19
6º	França	2.463,22
7º	Índia	2.256,40
8º	Itália	1.850,74
9º	Brasil	1.798,62
10º	Canadá	1.529,22
11º	Coreia do Sul	1.411,25
12º	Rússia	1.280,73
13º	Austrália	1.258,98
14º	Espanha	1.232,60
15º	México	1.046,00

Fonte: Fundação Alexandre De Gusmão (2017)

A segurança Alemã baseia-se em dois pilares: uma forte e resoluta Aliança do Atlântico Norte e uma União Europeia unida e resiliente. O País acredita ainda que só será capaz de obter sucesso nos desafios dessa era com o fortalecimento desses dois pilares.

Conforme Alemanha (2016), à medida que as demandas sobre o Bundeswehr crescem em variedade e volume, as demandas sobre seu pessoal também aumentarão. A Bundeswehr precisa do melhor equipamento possível e de financiamento sustentável para enfrentar com eficácia desafios como a guerra híbrida, o terrorismo transnacional, os ataques cibernéticos e as pandemias e, ao mesmo tempo, cumprir as exigências de uma defesa nacional e coletiva mais forte. No futuro, ele deve ter uma gama abrangente e moderna de recursos à sua disposição. Também deve impulsionar a inovação e ser um parceiro confiável e confiável para seus aliados.

As forças armadas de qualquer País são um importante instrumento de sua política de segurança e defesa. No caso alemão, sua missão é baseada em diretrizes constitucionais, bem como nos valores, interesses e prioridades estratégicas daquele País.

Segundo Alemanha (2016), a missão do Bundeswehr, como parte da abordagem de todo o governo, é:

a) Defender a soberania e a integridade territorial da Alemanha e proteger seus cidadãos;
b) Contribuir para a resiliência do Estado e da sociedade contra ameaças externas;
c) Apoiar e garantir a capacidade da Alemanha para tomar medidas em matéria de política externa e de segurança;
d) Contribuir em conjunto com parceiros e aliados para combater as ameaças à nossa sociedade aberta e ao seu comércio mundial livre e seguro e rotas de abastecimento;
e) Contribuir para a defesa de nossos aliados e para a proteção de seus cidadãos;
f) Promover a segurança e a estabilidade num quadro internacional e
g) Reforçar a integração europeia, a parceria transatlântica e a cooperação multinacional.

Dentre as tarefas associadas às Forças Armadas Alemãs, é interessante citar:

a) Defesa nacional e coletiva no quadro da OTAN e da UE, incluindo realização de tarefas de defesa em território alemão, bem como medidas de dissuasão em todos os domínios;
b) Derrotar o terrorismo e defender-se contra ameaças híbridas;
c) Consolidar a capacidade de defesa transatlântica e europeia e conduzir medidas para tranquilizar e apoiar os Aliados como parte da solidariedade da Aliança a fim de proteger a Alemanha, os seus cidadãos e parceiros e impedir potenciais adversários;
d) A luta contra o terrorismo transnacional, contra ameaças do domínio cibernético e da informação e contra novos perigos híbridos;

Em seu Livro Branco encontra-se ainda alguns passos necessários para aprimorar e preparar as Forças Armadas para o domínio cibernético e da informação. O governo Alemão enxerga que suas Forças Armadas possuem alto valor agregado neste campo, para atores estatais e não estatais e, deste modo, para se tornar um instrumento efetivo de defesa cibernética, deve estar apto a enfrentar ataques complexos. A defesa contra tais ataques exige capacidades defensivas e ofensivas de alto valor que devem ser continuamente exercidas e desenvolvidas. Devido à velocidade da inovação e à natureza global das ameaças cibernéticas, deve ser adotada uma abordagem abrangente. Para tal, a busca de parcerias internacionais, a cooperação com instituições industriais e de pesquisa, fará com que o *Bundeswehr* possa permanecer ágil e capaz.

Este livro ressalta ainda que para que as Forças Armadas possam realizar suas tarefas, todos devem:

a) Desenvolver capacidades nacionais, em outras palavras, promover uma abordagem de todo o governo e cooperar com instituições de pesquisa, indústria e parceiros;
b) Desenvolver as capacidades cibernéticas da *Bundeswehr*, consolidando a arquitetura de segurança de seu sistema de Tecnologia da Informação e tornando-a mais resiliente;
c) Tornar os sistemas de armas, postos de comando e armamentos mais robustos, usando, entre outras coisas, as principais tecnologias nacionais;
d) Recrutar o melhor pessoal através da criação de carreiras atraentes no espaço cibernético, conceber estratégias inovadoras de recrutamento de pessoal e estabelecer novas parcerias e programas de cooperação; e

e) Reunir as várias responsabilidades e estruturas para uma robusta acumulação de capacidades, agrupar as capacidades de TI para digitalizar as forças armadas e criar pontos centrais de contato para outros ministérios e parceiros multinacionais.

Em 26 de abril de 2016, o Ministério da Defesa Alemão apresentou sua decisão de criar um braço de suas Forças Armadas, o Comando do Espaço Cibernético e de Informação – KdoCIR. Em Outubro do mesmo ano, o KdoCIR passa a existir como um departamento do Ministério da Defesa, indo ao status de novo Força em abril de 2017. A figura 9 apresenta a foto do prédio do KdoCIR.

Figura 9 - KdoCIR

Fonte: Cyber Und Informationsraum (2019)

Com base em Cyber und informationstraum (2019), o Comando do Espaço Cibernético e de Informação, com seu ambiente de trabalho inovador e atraente, aborda os desafios complexos do espaço cibernético e de informações. Em uma área que é, em última análise, um resultado da crescente digitalização da sociedade, a equipe do comando, por definição, ocupa muitos tópicos desafiadores e modernos. Assim como o exército, a força aérea e a marinha são responsáveis pelas dimensões da terra, do ar e do mar, eles são responsáveis pela dimensão do ciberespaço e do espaço da informação.

Ainda com base em Cyber und informationstraum (2019), em um nível com os inspetores das outras cinco áreas organizacionais, o Inspetor Cibernético e o Espaço de Informação tem total responsabilidade pela dimensão do espaço cibernético e da informação. Em julho de 2017, ele assumiu a responsabilidade por 15.000 membros da divisão.

O novo comando iniciou-se com uma equipe de 260 pessoas, com previsão de atingir 14,5 mil posições até o ano de 2021. Esses 260 membros iniciais garantem a liderança dos militares.

Segundo o porta-voz do Ministério da Defesa, “A expansão das capacidades cibernéticas é uma contribuição essencial para a postura geral de segurança do governo e oferece oportunidades adicionais para prevenir conflitos e lidar com crises para incluir ameaças híbridas”. (Forças Armadas da Alemanha terão comando de defesa cibernética, 2017)

Reservistas sempre foram parte integrante da Bundeswehr e indispensáveis para a segurança da República Federativa da Alemanha. Já em 2017, a Bundeswehr abriu novos caminhos com o seu conceito de fornecer apoio à comunidade cibernética e abriu o caminho para ganhar experiência civil em defesa cibernética. A figura 10 ilustra esse conceito.

Figura 10 - As diferentes maneiras para a comunidade cibernética

Fonte: O Autor.

O conceito é deliberadamente muito amplo e vai além de uma reserva que consiste apenas em reservistas “clássicos”. A comunidade cibernética se abre para novos grupos-alvo e está aberta a um grupo maior de pessoas do que antes.

5 DISCUSSÃO

A inserção do espaço cibernético como teatro de operações na guerra, ainda preserva alguns aspectos observados por Clausewitz, quais sejam a natureza político e social. Entretanto, novas características são associadas a essa natureza, principalmente uma origem difícil de ser determinada podendo vir de qualquer parte do globo, a possibilidade de um ataque ser orquestrado por uma pessoa ou grupo ideológico, financiamento de atacantes por Estados, dentre outros. Outro ponto a ser destacado é

que os ataques cibernéticos podem ocorrer a qualquer instante, dificultando a delimitação do início e fim do conflito.

Diversos estudiosos perguntaram como se prevenir ou se defender de ataques cibernéticos no futuro, eles incluíram a dissuasão como uma abordagem possível. De acordo com LONG (2008), estratégias de dissuasão nos remetem a Guerra da Peloponeso e o assunto teve uma grande repercussão durante a Guerra Fria, quando os Estados Unidos e a União Soviética tentaram evitar uma guerra nuclear. Desde aquele alto nível conceitual, analistas aplicaram conceitos de dissuasão a problemas de segurança contemporâneos, como o terrorismo, com, pelo menos, algum sucesso. Existem ainda dúvidas se a dissuasão pode ser utilizada no espaço cibernético.

Além de sua potencial eficácia, a dissuasão é um método muito mais barato que a manutenção contínua do conflito. Assim como no caso da Estônia em 2007, a guerra cibernética é capaz de gerar custos substanciais às suas vítimas. Quando combinados com operações convencionais, dependendo do alvo a ser atingido, ataques cibernéticos podem custar vidas. Se comparados com os custos de uma parada temporária do mercado financeiro, vazamento de informações ou paralisações de infraestruturas críticas de um Estado, os custos para implantação de um poder dissuasório podem ser considerados mínimos. Enquanto o conflito impõe custos humanos e materiais, a dissuasão oferece uma forma escapatória desses custos.

5.1 Ataques Ciber-Cinéticos

Conforme Sá, Carmo, Machado (2017); o objetivo de um ataque ciber-cinético é o impacto direto em plantas físicas, provenientes de alterações realizadas no domínio cibernético. Neste sentido podemos extrapolar o conceito e dizer que o ataque ciber-cinético engloba desde dispositivos de internet das coisas a sistemas de controle e automação que, não necessariamente, sejam industriais. Em relação ao Poder AeroEspacial podemos, por exemplo, citar os seguintes alvos:

- Sistemas de controle e automação de aeronaves, o que inclui, por exemplo, piloto automático:

> O piloto automático (em inglês: Autopilot) foi projetado tendo como objetivo prover aos pilotos descanso físico e mental durante voos com etapas de longa duração, permitindo assim, que eles possam focar em atividades em que a automação não pode intervir, como por exemplo, na comunicação bilateral com órgãos de Controle de Trafego Aéreo (ATC) e no monitoramento das condições meteorológicas e

> acompanhamento do planejamento de voo (COLLINSON, 2011). Sistemas automáticos, como o piloto automático, trazem consigo diversos benefícios, como por exemplo, maximização da Segurança Operacional, redução no consumo de combustível e incremento na performance da aeronave mesmo quando em condições meteorológicas não favoráveis (COLLINSON, 2011). (BORGES, 2017, p. 16).

Autothrust/Autothrottle:

> O sistema de autothrust geralmente é acionado no início da decolagem de modo a limitar a potência dos motores para a de máximo empuxo ou um valor mais baixo, dependendo de algumas variáveis como, por exemplo, o peso da aeronave no momento da decolagem, comprimento de pista disponível e temperatura local. O objetivo desse sistema é minimizar o desgaste do motor, aumentar a eficiência e reduzir o consumo de combustível. A potência de decolagem desejada é selecionada através do manete de potência. Nas aeronaves antigas, os pilotos apenas empurravam os manetes de potência a frente e obtinham assim o máximo empuxo dos motores e por vezes sobreaqueciam os motores. Na grande maioria das aeronaves atuais, já não é possível obter nada além do que o empuxo necessário para uma determinada fase de operação dos motores devido ao constante monitoramento por parte dos computadores da aeronave (BILLINGS, 1997). (BORGES, 2017, p. 17).

Fly-by-wire (FBW)

> Fly-by-wire é um sistema que substitui os controles de voo convencionais de uma aeronave por uma interface eletrônica. Os movimentos realizados pelos pilotos, nos controles de voo da aeronave, são convertidos em sinais eletrônicos e, então, transmitidos por fios aos FCCs que irão determinar como mover os atuadores de cada superfície de controle para assim obter uma resposta rápida e amortecida, respeitando o envelope de voo9 (COLLINSON, 2011, p. 187) (BORGES, 2017, p. 19).

Glass Cockpit

> As decisões mais importantes a serem tomadas durante o voo ocorrem na cabine de comando, onde estão todas as informações relativas aos sistemas da aeronave são disponibilizadas aos pilotos por meio de telas e monitores chamados de glass cockpit. (BORGES, 2017, p. 22).

- Sistemas de combates aéreos, onde sensores e armas são conectados a computadores e redes – ainda que locais.
- Sistemas de controle de lançamento de satélites.

Há de se deixar claro que não é intenção do presente trabalho esgotar todas as possibilidades de alvos de um eventual ataque ciber-cinético ao Poder AeroEspacial, mas sim demonstrar a ampla gama de sistemas sujeitos a tal tipo de ataque.

Uma medida de segurança muito comum nos meios militares, é a utilização do *air-gapping,* a qual consiste no isolamento da rede de controle destes sistemas de outros tipos de rede, como por exemplo a INTERNET, sem a conexão física entre as mesmas. O

próprio caso do Stuxnet, apresentado anteriormente, demonstra que esta medida também pode ser vencida.

Este fato deixa claro a necessidade de adoção de medidas de segurança, que não sejam exclusivamente técnicas, afim de mitigar eventuais possibilidades de ataque a estes sistemas, estando isolados ou não por *air-gap*. Passamos então a discutir algumas possibilidades acerca do presente assunto.

5.1.1. Políticas para mitigação de ataques.

A presente seção apresenta a discussão de algumas políticas para a segurança do Poder AeroEspacial em relação aos ataques ciber-cinéticos. Considerando que o enfoque deste estudo é a segurança e defesa cibernética, todas as análises serão neste domínio. Mais especificamente, concentrar-se-á na qualificação de pessoal.

5.1.1.1 qualificação de pessoal

Para se conseguir níveis aceitáveis de segurança cibernética, é imprescindível o envolvimento de todos os atores do Poder AeroEspacial, bem como sua capacitação. Embora pareça um público pequeno, abrange muitas pessoas com formações e conhecimentos bem heterogêneos. Isto torna, a qualificação do pessoal do Poder AeroEspacial quanto à segurança de suas parcelas no espaço cibernético uma tarefa extremamente desafiadora, o que recai sobre o desenvolvimento de políticas de conscientização e capacitação. É notório que tais políticas devem atingir não somente os recursos humanos da Força Aérea Brasileira, mas também os setores industriais e infraestruturas pertencentes ao Poder AeroEspacial.

Pelo que foi exposto é desejável, que já nas escolas de formação militares, os sistemas de Ensino contenham disciplinas capazes de englobar conceitos sobre o funcionamento e a segurança do domínio cibernético e ainda, de sistemas híbridos.

> A exemplo da discussão apresentada em (SCHNEIDER, 2013; CONKLIN; CLINE; ROOSA, 2014) - onde a educação sobre segurança cibernética visa um público mais abrangente do que nos casos do Poder Naval e da Marinha Mercante - o desafio maior está em promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo, no que concerne à segurança cibernética e de sistemas híbridos. Isto porque a formação técnico-profissional de seu pessoal conta com a participação de um grande número de instituições e estabelecimentos de ensino, públicos e privados. Deste modo, e com base na discussão apresentada em (SCHNEIDER, 2013), é razoável concluir não ser trivial solucionar a questão através de um processo amplo de aprimoramento curricular - ainda que necessário. Neste caso, soa ser adequado apoiar estes setores através de programas de treinamento e conscientização promovidos, a priori, pelos órgãos do Estado responsáveis pela Segurança e Defesa cibernética

> no Brasil – i.e. o Gabinete de Segurança Institucional e o Comando do Exército, respectivamente. (SÁ, MACHADO, ALMEIDA, 2018, p. 39).

No caso do Poder AeroEspacial brasileiro, parece ser coerente a adoção de um modelo centralizado de capacitação para suprir as necessidades de sua indústria e infraestrutura, especialmente no que tange a segurança dos tipos de sistema aqui apresentados.

6 CONSIDERAÇÕES FINAIS

O presente trabalho foi conduzido com o objetivo geral de responder a questão problema**:** Como as novas ameaças, geradas pela guerra cibernética em encontro com as guerras cinética e eletrônica, podem afetar o Poder Aeroespacial?

Com vistas a responder esta questão, e realizar o devido diagnóstico da situação encontrada no Brasil, Alemanha e Estados Unidos, inicialmente, foram estudados os fundamentos da guerra até a inclusão do espaço cibernético em sua conduta.

Passou-se então a busca do primeiro objetivo específico, através da caracterização das diversas gerações da guerra. Foi verificado então que as teorias da Guerra passaram por três gerações até na quarta geração encampar os conceitos de redes de computadores. O estudo demonstrou que nas guerras de primeira geração, o foco é o princípio da massa, onde há a concentração de um maior potencial de combate em determinado ponto e momento considerados decisivos. A guerra de segunda geração teve início durante a primeira guerra mundial, e entra em voga o poder de fogo, onde os estrategistas teóricos acreditavam que a artilharia conquista e a infantaria ocupa. A guerra de terceira geração foi produto da primeira guerra mundial e é conhecida como guerra da manobrabilidade, representando o conceito da tática e mobilidade. Enfim a guerra de quarta geração chega onde o Estado perde o monopólio sobre a guerra, passando a descentralização e a iniciativa a serem as características principais. Nesta geração podem-se incluir os computadores e suas redes.

Alcançou-se o segundo objetivo específico através da verificação de que o desenvolvimento tecnológico adquiriu relevante importância na doutrina militar, assim como nas políticas de Estado, principalmente graças a incorporação do espaço cibernético, que além de representar um fator de poder, gerou diversas vulnerabilidades a serem exploradas e defendidas.

Com isso, mesmo sendo considerado um assunto relativamente novo para as relações internacionais e para os Estados, o setor cibernético adquire maior evidência no cenário mundial, gerando o surgimento de novas políticas, estratégias, decisões e investimentos. O aumento na quantidade de ataques sofridos por países e autoridades tem feito o tema progredir rapidamente e, assim cada vez mais recursos financeiros têm sido alocado na área. Nota-se ainda o aumento da preocupação dos Estados, por meio de declarações públicas, com sua segurança cibernética e com a proteção de suas infraestruturas críticas. Considerando-se a impossibilidade de um sistema de defesa cibernético eficaz sem a participação de toda a população, bem como de países amigos, verifica-se cada vez mais o incentivo da participação de toda a população e da qualificação de recursos humanos para a área.

Quando se trata sobre guerra, o campo cibernético insere características peculiares ao teatro de operações tradicional, pois mesmo sem invalidar alguns elementos tradicionais, o ataque cibernético é capaz de potencializar os efeitos de ataques em uma guerra tradicional, como no caso da Geórgia em 2008. Tal fato faz com que haja mudanças acerca dos estudos sobre segurança internacional, relações de poder e a própria guerra em si. Isso ainda pode ser observado com a análise dos modelos das gerações de guerra hoje existentes.

O uso de armas cibernéticas facilitou o ataque a objetivos até então dificilmente pensados. Isto fica evidenciado após os ataques como os ocorridos aos poços de petróleo durante a Guerra do Golfo nos anos 90 poderiam ser realizados sem a responsabilização efetiva de algum Estado. Nesse viés um ataque cibernético realizado com sucesso, vale-se do anonimato e da ausência de distância física existente no espaço cibernético.

Outro ponto relevante e, conforme citado ao longo do presente estudo é a necessidade de cooperação entre Estados, entre Estados e empresas públicas ou privadas, entre empresas, dentre outros. A própria Organização do Tratado do Atlântico Norte – OTAN reforça este ponto em seu manual de estrutura nacional de segurança cibernética. Somente assim, acredita-se ser possível identificar e combater as vulnerabilidades assim como determinar seus riscos e ameaças.

Com a fundamentação teórica em Guerra Cibernética, levada a efeito, ficou em destaque a presença de um estado no qual tal teoria tem se mostrado mais consolidada e está sendo colocada em prática e um estado que tem papel relevante dentro da OTAN e tem se destacado nas ações quanto ao campo cibernético.

Para auferir o terceiro objetivo específico, foi realizada uma apresentação da estrutura de defesa cibernética do Brasil, Alemanha e Estados Unidos. Pode-se dizer que, no Brasil, a publicação da Estratégia Nacional de Defesa de 2008 foi o grande marco da inclusão do campo cibernético no processo de securitização brasileira. O GSI/PR e o Ministério da Defesa (MD) coordenam as ações neste setor, cabendo ao Exército Brasileiro a atuação e consolidação da defesa cibernética brasileira. Estas ações firmaram a capacidade cibernética brasileira perante o restante do mundo, assim como indicaram a preocupação do Estado Brasileiro na defesa de seus interesses neste espaço cibernético.

Reforça-se que o Brasil optou, num primeiro momento, por manter a sua “força cibernética”, sob o comando do Exército Brasileiro. Entretanto conforme apontado por Codeiro (2016), tal decisão pode gerar uma inversão nas políticas e necessidades do Estado Brasileiro.

Entretanto, em comparação com Estados Unidos e Alemanha, que são considerados grandes *players* nesta área, foi identificado que o modelo adotado no Brasil apresenta aspectos diferentes dos modelos adotados pelos outros dois países. Neste sentido, a representatividade de Estados Unidos e Alemanha no campo cibernético, permite verificar que o Brasil ainda carece de muitos esforços para atingir um patamar relevante nesta área. Todavia, durante a pesquisa, foram identificados trabalhos de relevo acadêmico, a exemplo de Silva Filho (2015), Silva (2015) e Coutinho (2015) que exemplificam os esforços realizados no sentido da garantia da soberania tecnológica no espaço cibernético.

Já no caso da Alemanha, apenas em 2016, o governo alterou sua política de segurança, incluindo especial atenção ao campo cibernético. Ainda em 2016 o Ministério da Defesa Alemão criou seu mais novo braço armado, o KdoCir, o qual foi efetivado em 2017. Nessa esteira a Alemanha busca a expansão de sua capacidade cibernética, com vistas a melhorar a postura geral de segurança do governo, prevenindo conflitos e ajudando a lidar com as ameaças híbridas.

Os Estados Unidos começaram a atuar na área cibernética, tendo a NSA a frente de suas ações. Desde cedo demonstram sua preocupação com Rússia e China, países notoriamente reconhecidos como líderes na esfera cibernética. Em agosto de 2017, os EUA retiraram o Comando de Defesa Cibernética de dentro da NSA e o promoveram a um comando unificado que está na mesma categoria das divisões do Pentágono.

Como destaque, observa-se a grande preocupação que Alemanha, EUA e Brasil, especialmente os dois primeiros, possuem com relação à estruturação de suas defesas estratégicas contra-ataques cibernéticos, indicando que este tipo de defesa é uma de suas principais necessidades estratégicas.

Durante o estudo observou-se ainda uma tendência mundial, a criação de uma quarta força armada, a cibernética. Outros países que não foram abordados no presente estudo, tal como a França, já possuem seu comando militar de defesa cibernética.

Ao alcançar o objetivo proposto, tornou-se evidente a necessidade de futuras pesquisas que se aprofundem em outros campos, tais como uma pesquisa voltada a forma sobre como a certificação e homologação de softwares e produtos pode apoiar o desenvolvimento da segurança cibernética em relação ao Poder AeroEspacial.

Por fim, neste estudo, discutiu-se como a guerra cibernética em conjunto com a guerra cinética pode ter impacto direto no Poder Aeroespacial. Foram apresentados três casos clássicos que envolvem ataques multidomínio e caracterizam o princípio dos efeitos cinéticos. A partir daí, apresentou-se possíveis alvos dentro do Poder Aeroespacial. A discussão apresentada, indica que este tipo de ataque é factível.

Neste sentido, a discussão foi realizada em políticas voltadas para a segurança do domínio cibernético, permeando a qualificação de pessoal e o combate às vulnerabilidades em produtos que, de alguma maneira, envolvam o setor cibernético. No que concerne à qualificação de pessoal, encoraja-se a adoção de um modelo apoiado nos sistemas de ensino, já existentes, complementado pela atuação de um órgão centralizado de capacitação sobre segurança cibernética. O Sistema de Ensino da Aeronáutica, com currículos continuamente atualizados quanto ao assunto, se encarregaria da capacitação do pessoal do Poder Aeroespacial, como já ocorre atualmente. Já um órgão centralizado de capacitação sobre segurança cibernética se encarregaria de promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo. É importante frisar que a presente discussão não tem a pretensão de esgotar a questão, mas contribuir de forma abrangente para a segurança desses sistemas.

O espaço cibernético ainda é um espaço a ser explorado, pois possui enorme capacidade de transformar as relações de poder entre países e, consequentemente, as relações internacionais. Diferentemente do ocorrido durante a Guerra Fria, a corrida no espaço cibernético não se restringe às grandes potências, mas se vale de diversos atores de menor ou nenhuma expressão no cenário internacional.

Desta forma, conclui-se, pelos estudos desenvolvidos no decorrer deste trabalho, que há a necessidade de desenvolvimento de políticas capazes de auxiliar na promoção da segurança dos sistemas cibernéticos e híbridos do Poder Aeroespacial.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). Portal ABIN: perguntas frequentes – aabin. Disponível em: http://www.abin.gov.br/fale-com-a-abin/perguntas-frequentes-2/a-abin/. Acesso em: 30 jul. 2019.

ALEMANHA. Departament of Defense. **The 2016 White Paper**: On German Security Policy and The Future of The Bundeswehr. Berlin: Stauffenbergstrabe 18, 2016. Disponível em: https://www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf. Acesso em: 24 Maio 2019.

ANDRADE, M. M. D. **Como Preparar Trabalhos Para Cursos de Pós-Graduação**: noções práticas. 5. ed. São Paulo: Atlas, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a gestão da segurança da Informação. 1. ed. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: Informação e documentação – Referências - Elaboração. 2. ed. Rio de Janeiro, 2018.

BRASIL é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa. **Estadão**, São Paulo, 1 fev. 2010. Disponível em: http://politica.estadao.com.br/noticias/geral,brasil-e-um-dos-paises-mais-vulneraveis-a-ataques-ciberneticos-diz-pesquisa,504613. Acesso em: 03 jan. 2018.

BERNERS-LEE, T. **Information management:** a proposal. Genebra: CERN, 1989. Disponível em: https://www.w3.org/History/1989/proposal.html. Acesso em: 20 out. 2019.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 050/3SC, de 21 de dezembro de 2015. Aprova a reedição da Norma de Sistema do Comando da Aeronáutica que estabelece a estrutura e as competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica (NSCA 7-7). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n° 236, f. 11824, 23 dez. 2015.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria nº 278/GC3, de 21 de junho de 2012. Aprova a reedição da Doutrina Básica da Força Aérea Brasileira (DCA 1-1). **Boletim do Comando da Aeronáutica,** Rio de Janeiro, n° 121, f. 4394, 26 jun. 2012.

BRASIL. Comando do Exército. Comando de Operações Terrestres. Portaria nº 42 - COTER, de 8 de junho de 2017. Aprova o Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 2017. **Boletim do Exército**, Brasília, DF, n. 25, 23 jun. 2017. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf. Acesso em: 08 maio 2019.

BRASIL. Conselho de Defesa Nacional. Portaria n° 14, de 11 de maio de 2015. Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética

da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008. **Diário Oficial da União**, Brasília, DF, n° 88, 12 maio 2015a. Disponível em: http://www.gsi.gov.br/arquivos/4_estrategia_de_sic.pdf. Acesso em: 08 maio 2019.

BRASIL. Decreto Legislativo n° 373, de 25 de setembro de 2013. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem nº 83, de 2012**. Diário Oficial da União**, Brasília, DF, 2013. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 06 ago. 2018.

BRASIL. Decreto n° 9.668, de 2 de janeiro de 2019. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares – RMP. **Diário Oficial da União**, Brasília, DF, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9668.htm#art8. Acesso em: 03 mar. 2019.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação. **Concluída a última etapa das reuniões da Estratégia Nacional de Segurança Cibernética**. 2019a. Disponível em: http://dsic.planalto.gov.br/noticias/concluida-a-ultima-etapa-das-reunioes-da-estrategia-nacional-de-seguranca-cibernetica. Acesso em: 20 jul. 2019.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Qual é a estrutura do CDN?**. Disponível em: http://www.gsi.gov.br/imagens-acesso-a-informacao/estrutura-cdn.pdf. 2019b. Acesso em: 20 jul. 2019.

BRASIL. Ministério da Defesa. Portaria Normativa n° 1.691/EMCFA/MD, de 05 de agosto de 2015. Dispõe sobre a Doutrina para o Sistema Militar de Comando e Controle (MD31-M03) 3. ed., 2015. **Diário Oficial da União**, Brasília, DF, n° 149, 06 ago. 2015b.

BRASIL. Ministério da Defesa. Portaria Normativa n° 3010/MD, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. **Diário Oficial da União,** Brasília, DF, n° 224, 19 Nov. 2014. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 08 maio 2019.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde**: segurança cibernética no Brasil / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; Org. Claudia Canongia e Raphael Mandarino Junior. Brasília, DF: GSIPR/SE/DSIC, 2010. 63 p. Disponível em: http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf. Acesso em: 08 maio 2019.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. **Relatório**: XIII Encontro Nacional dos Estudos Estratégicos. Brasília, DF, 2013a. Disponível em: http://www.biblioteca.presidencia.gov.br/presidencia/dilma-vana-rousseff/publicacoes/orgao-essenciais/secretaria-de-assuntos-estrategicos/relatorio-do-xiii-encontro-nacional-de-assuntos-estrategicos. Acesso em: 08 maio 2018.

BORGES, V. A. **A influência da automação na operação das aeronaves comerciais.** Trabalho de Conclusão de Curso, Centro Federal de Educação Tecnológica de Minas Gerais, Minas Gerais, Brasil, 2017. Disponível em: http://www.eng-automacao.araxa.cefetmg.br/wp-content/uploads/sites/152/2018/01/TCC-VINICIUS-Vers%C3%A3o-Definitiva-EAI-2017.pdf. Acesso em: 28 nov. 2019.

BOSWORTH, S; KABAY, M.E.; WHYNE, E. **Computer Security Handbook**. 6. ed. New Jersey: John Wiley & Sons Inc, 2014.

CASTELLS, M. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

CENTRO de Tratamento e Resposta a Incidentes Cibernéticos de Governo. Portal CTIR.GOV: Sobre o Ctir.Gov. Disponível em: http://www.ctir.gov.br/sobre-CTIR-gov.html#missao. Acesso em: 17 maio 2018.

CHOUCRI, N. **Cyberpolitics in International Relations**. Cambridge: MIT Press, 2012.

CLAUSEWITZ, C. V. In: HOWARD, M.; PARET, P. **On War.** Princeton: UP, 1989. p. 6.

COMMONS, A. G. A Cibernética é o Novo Domínio Aéreo: A Superioridade nos Domínios em Megacidades. Military Review – **Revista Profissional do Exército dos EUA,** Ft. Leavenworth, n. 2, Tomo 73, segundo trimestre 2018. Disponível em: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/segundo-trimestre-2018-pdf-completo-edicao-brasileira.pdf. Acesso em: 16 jul. 2019.

CONHEÇA os principais episódios da crise migratória na Europa. **Portal G1**, Rio de Janeiro, 24 jun. 2018. Disponível em: https://g1.globo.com/mundo/noticia/conheca-os-principais-episodios-da-crise-migratoria-na-europa.ghtml. Acesso em: 17 jun. 2019.

CORDEIRO, L.E.P. C. As **Expressões do Poder**: uma nova taxonomia. 2016. Dissertação (Mestrado em Ciências Aeroespaciais) - Programa de Pós-Graduação em Ciências Aeroespaciais, Universidade da Força Aérea, Rio de Janeiro, 2016.

COSTA, C. R. A. D. Evolução da Arte da Guerra – Das Gerações da Guerra Moderna aos Conflitos Assimétricos. **Jornal das Relações Internacionais**, Curitiba, PR, n. 2, v.1, 22 jun. 2017. Disponível em: http://jornalri.com.br/artigos/evolucao-da-arte-da-guerra-das-geracoes-da-guerra-moderna-aos-conflitos-assimetricos. Acesso em: 18 jun. 2018.

COUTINHO, M. A. **Uma Proposta de Modelo Seguro para Gestão de Identidade em Sistemas Móveis de Pagamentos Eletrônicos**. 2015. Dissertação (Mestrado) - Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Universidade Federal

do Rio de Janeiro, Rio de Janeiro, 2015. Disponível em: https://www.cos.ufrj.br/uploadfile/1433990326. Acesso em: 28 nov. 2019.

CRUZ JÚNIOR, S. C. D. A. Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual. Texto para Discussão, Brasília, DF, 2013.

CYBER UND INFORMATIONSRAUM. Das Kommando Cyber-und Informationsraum. Disponivel em: https://cir.bundeswehr.de/portal/a/cir/start/kdocir/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zizSxNPN2Ngg18DZyNTA0cncz8LYxMDA0NnM30wwkpiAJKG-AAjgb6wSmp-FAM8xxmhEMVKQfpR-VlViWWKFXkF9UkpNaopeYDHKhfmRGYl5KTmpAfrIjRKAgN6LcoNxREQAQirMY/dz/d5/L2dBISEvZ0FBIS9nQSE. Acesso em: 29 jul. 2019.

DEUTSCHE WELLE (DW). Alemanha tem nova queda em pedidos de refúgio. Disponível em: https://www.dw.com/pt-br/alemanha-tem-nova-queda-em-pedidos-de-ref%C3%BAgio/a-42172762. Acesso em: 29 jul. 2019.

ESTADOS UNIDOS DA AMÉRICA. **Departament Of Defense**. National Military Strategy For Cyberspace Operations. Washington, 2006. Disponivel em: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-023.pdf. Acesso em: 25 set. 2018.

ESTADOS UNIDOS DA AMÉRICA. **The White House.** International Strategy for Cybersapace. Washington, 2011. Disponivel em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 31 maio 2019.

ESTADOS UNIDOS DA AMÉRICA. **The White House.** National Cyber Strategy of The United States of America. Washington DC, 2018. Disponivel em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 08 maio 2019.

FORÇAS Armadas da Alemanha terão comando de defesa cibernética. **Portal G1.** Rio de Janeiro, 31 mar. 2017. Disponível em: https://g1.globo.com/tecnologia/noticia/forcas-armadas-da-alemanha-terao-comando-de-defesa-cibernetica.ghtml. Acesso em: 10 jun. 2019.

FUNDAÇÃO ALEXANDRE DE GUSMÃO (FUNAG). Instituto de Pesquisa de Relações Internacionais. **As 15 maiores economias do mundo.** Disponível em: http://www.funag.gov.br/ipri/index.php/o-ipri/47-estatisticas/94-as-15-maiores-economias-do-mundo-em-pib-e-pib-ppp. Acesso em: 03 jun. 2019.

GIBSON, W. **Burning Chrome.** Reprint (29 de julho de 2003). Voyager, 2003.

KLIMBURG, A. Mobilising Cyber Power. **Survival**, 2011. v. 53, p.41-60. Disponivel em: http://web.clas.ufl.edu/users/zselden/coursereading2011/Klimcyber.pdf. Acesso em: 24 maio 2019.

LIBICKI, M. C. Cyberwar as a Confidence Game. **Strategic Studies Quarterly**. SPRING, 2011. Vol. 5, N. 1 p. 132-147. Disponivel em: https://www.jstor.org/stable/26270514. Acesso em: 13 ago. 2018.

LIBICKI, M. C. Crisis and Escalation in Cyberspace. Califórnia: RAND, 2012. Disponivel em: https://www.rand.org/pubs/monographs/MG1215.html. Acesso em: 13 ago. 2018.

LONG, A. **Deterrence From Cold War to Long War**: lessons from six decades of Rand deterrence research. Califórnia: RAND, 2008. Disponivel em: http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf. Acesso em: 20 maio 2019.

MANDARINO JÚNIOR, R. **Um Estudo Sobre a Segurança e Defesa do Espaço Cibernético Brasileiro**. 2009. Monografia (Especialização em Ciência da Computação: gestão da segurança da informação e comunicações) - Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, DF, 2009.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). Cyber defence. Belgium, 2018. Disponivel em: https://www.nato.int/cps/en/SID-714ABCE0-30D8F09C/natolive/topics_78170.htm. Acesso em: 16 ago. 2019.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). NATO’s role in cyberspace. Belgium, 2019. Disponivel em: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html. Acesso em: 16 ago. 2019.

PASSOS, R.D.F. **Clausewitz e a política** - uma leitura da guerra. 2005. Dissertação (Mestrado em Ciências Militares) - Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2015.

PINHO, J. B. **Jornalismo na internet**: planejamento e produção da informação online. São Paulo. Summus, 2003.

RAMOS, M.S.M. **Ciberguerra e a Política de Cooperação com a OTAN**. 2015. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Roraima, Boa Vista, RO, 2015.

ROUGH DIPLOMACY. **Remote Control:** Stuxnet. Disponível em: https://www.roughdiplomacy.com/stuxnet/. Acesso em: Acesso em: 20 maio 2019.

ROSA, C. E. V. **Poder Aéreo**: Guia de Estudos. Rio de Janeiro: Luzes, 2014.
SANTOS, M. **Evolução do poder aéreo**. Belo Horizonte, MG; Itatiaia, RJ: Instituto Histórico-Cultural da Aeronáutica, 1989.

SÁ, A. O.; DA COSTA CARMO, L. F. R.; MACHADO, R. CS. Covert attacks in cyber-physical control systems. **IEEE Transactions on Industrial Informatics**, v. 13, n. 4, p. 1641-1651, 2017.

SÁ, A. O.; MACHADO, R.C.S; ALMEIDA, N. N.; O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 24, n. 3, p. 14-39, Set/Dez 2018.

SEMOLA, M. **Gestão da Segurança da Informação**: uma Visão Executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SILVA FILHO, J. B. **Detecção de Anomalias em Fluxos de Redes de Computadores Utilizando Técnicas de Redes Neurais e Estimadores Lineares**. 2015. Dissertação (Mestrado) - Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2015. Disponível em: https://www.cos.ufrj.br/uploadfile/publicacao/2581.pdf. Acesso em: 28 nov. 2019.

SILVA, V. L. P. **Identificação de anomalias em fluxos de rede utilizando previsões em series temporais pelo método de holt-Winters na proposta de modelo seguro para gestão de identidade em sistemas moveis de pagamentos eletrônicos.** 2015. Dissertação (Mestrado) - Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2015. Disponível em: https://www.ravel.ufrj.br/sites/ravel.ufrj.br/files/publicacoes/dissertacoes/dissertacao_vander_anomalia_2015-09-22.pdf. Acesso em: 28 nov. 2019.

SIQUEIRA, M. B. Giulio Douhet: pioneiro, profeta e teórico do poder aéreo ainda atual**. Idéias em Destaque**, Rio de Janeiro, n. 34, p. 9-36, Set/Dez. 2010. Disponível em: http://www2.fab.mil.br/incaer/images/eventgallery/instituto/Ideias/Textos/ideias_34.pdf. Acesso em:31 maio 2019.

TECNOLOGIA & DEFESA. 10 perguntas para o general Okamura: comandante da Defesa Cibernética do Exército Brasileiro, 2018. Disponível em: http://tecnodefesa.com.br/10-perguntas-para-o-general-okamura-comandante-da-defesa-cibernetica-do-exercito-brasileiro/. Acesso em: 01 set. 2019.

UNITED STATES CYBER COMMAND (USCYBERCOM). Portal U.S. Cyber Command: Cyber Command History. Disponivel em: https://www.cybercom.mil/About/History/. Acesso em: 31 maio 2019.

VEIGA, R. D. Q. **A Defesa Cibernética (DEF_CIBER) na Visão da Força Aérea Brasileira.** Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2012.

WIENER, N. **Cibernética e sociedade**: o uso humano de seres humanos. São Paulo: Cultrix, 1984.

WIKIMEDIA. Organization of the Department of the Defense. Disponível em: https://upload.wikimedia.org/wikipedia/commons/7/73/DoD_Organization_March_2012.pdf. Acesso em: 30 maio 2019.

WU, C**. An Overview of the Research and Development of Information Warfare in China in Cyberwar, Netwar, and the Revolution in Military Affairs.** New York: Palgrave MacMillan, 2006.