Research, Society and Development, v. 9, n. 9, e590997313, 2020
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v9i9.7313

Políticas de segurança e defesa do ciberespaço brasileiro a partir do “manual de campanha - Guerra Cibernética”

Defense and security policies of the brazilian's cyberspace from the “campaign manual - Guerra Cibernética”

Política de seguridad y defensa del ciberespacio brasileño a partir del “manual de campaña - Guerra Cibernética”

Recebido: 06/08/2020 | Revisado: 20/08/2020 | Aceito: 28/08/2020 | Publicado: 30/08/2020

Kellin Caroline Martins
ORCID: https://orcid.org/0000-0002-7584-5783
Universidade de Santa Cruz do Sul, Brasil
E-mail: kellin@mx2.unisc.br
Camilo Darsie
ORCID: https://orcid.org/0000-0003-4696-000X
Universidade de Santa Cruz do Sul, Brasil
E-mail: camilodarsie@unisc.br

Resumo

Com a constante evolução da tecnologia, as sociedades tornaram-se cada vez mais dependentes das ferramentas tecnológicas, sendo que muitas delas compõem o que é chamado de ciberespaço. Apresenta-se, portanto, uma pesquisa que teve como objetivo entender o posicionamento do Estado brasileiro em relação à Segurança e Defesa do Ciberespaço Nacional. Neste sentido, foi realizada pesquisa bibliográfica e análise documental. A pesquisa bibliográfica operou com conhecimentos acerca do ciberespaço e das teorias das Relações Internacionais enquanto a análise documental esmiuçou o Manual de Campanha - Guerra Cibernética, publicado em 2017. Ao finalizar o processo, destaca-se que o Estado brasileiro possui uma limitada documentação em relação tema e nestes poucos documentos, não ficam evidentes as estratégias eficientes para conter ameaças relacionada à defesa do ciberespaço nacional, pois trata-se de um documento prescritivo e não estratégico. Deste modo fica evidente que o Estado brasileiro está refém de situações quais podem ameaçar a soberania do se ciberespaço, fazendo-se necessário encarar com mais importância e atenção questões ligadas à segurança e defesa cibernética no Brasil.

Palavras-chave: Ciberespaço; Segurança nacional; Defesa nacional; Guerra cibernética**.**

Abstract

With the constant evolution of technology, societies have become increasingly dependent on technological tools, many of which make up what is called cyberspace. Therefore, is presented a research that aims to understand the positioning of the Brazilian State in relation to Security and Defense of National Cyberspace. In this sense, bibliographic research and documentary analysis were carried out. The bibliographic research operated with knowledge about cyberspace and International Relations theories while the documentary analysis detailed the Campaign Manual – Guerra Cibernética, published in 2017. At the end of the process, it is highlighted that the Brazilian State has limited documentation regarding theme and in these few documents, efficient strategies to contain threats related to the defense of national cyberspace are not evident, as it is a prescriptive and non-strategic document. In this way, it is evident that the Brazilian State is hostage to situations which may threaten the sovereignty of its cyberspace, making it necessary to face issues related to cyber security and defense in Brazil with more importance and attention.

Keywords: Cyberspace; National security; National defense; Cyber war**.**

Resumen

Con la evolución constante de la tecnología, las sociedades se han vuelto cada vez más dependientes de las herramientas tecnológicas, muchas de las cuales constituyen lo que se llama ciberespacio. Por tanto, se presenta una investigación que tiene como objetivo comprender el posicionamiento del Estado brasileño en relación con la seguridad y defensa del ciberespacio nacional. En este sentido, se realizó investigación bibliográfica y análisis documental. La investigación bibliográfica funcionó con conocimiento sobre el ciberespacio y las teorías de las relaciones internacionales, mientras que el análisis documental detallaba el Manual de campaña - Guerra Cibernética, publicado en 2017. Al final del proceso, se destaca que el Estado brasileño tiene una documentación limitada sobre tema y en estos pocos documentos, las estrategias eficientes para contener las amenazas relacionadas con la defensa del ciberespacio nacional no son evidentes, ya que es un documento prescriptivo y no estratégico. De esta manera, es evidente que el Estado brasileño es rehén de situaciones que pueden amenazar la soberanía de su ciberespacio, por lo que es necesario enfrentar los problemas relacionados con la seguridad y defensa cibernéticas en Brasil con más importancia y atención.

Palabras clave: Ciberespacio; Seguridad nacional; Defensa nacional; Guerra cibernética.

1. Introdução

O ambiente cibernético é considerado um dos mais promissores para o desenvolvimento de práticas ilegais que podem ser caracterizadas por meio de crimes financeiros, terrorismo, disputas bélicas, entre outras. Este ambiente é propício ao desenvolvimento de atos ilícitos especialmente por garantir entraves relativos à responsabilização dos criminosos devido à impossibilidade e/ou dificuldade de serem encontradas provas materiais de irregularidades, bem como a localização dos criminosos.

No contexto das Relações Internacionais, os ataques cibernéticos podem ser promovidos por Estados que visam eliminar os concorrentes considerados mais fracos e, assim, moldar o Sistema Internacional a seus favores. Tais práticas privilegiam, consequentemente, aqueles países entendidos como mais fortes. Essa dinâmica é um dos modos de violência que caracterizam as guerras, tanto as mais tradicionais quanto as contemporâneas. Assim, "[...] é a violência organizada promovida pelas unidades políticas entre si. A violência só é guerra quando exercida em nome de uma unidade política" (Bull, 2002, p. 211).

Neste contexto, é importante considerar que por meio de uma guerra cibernética ocorre a atualização e o desenvolvimento de sistemas que têm como tarefa a invasão e o controle de governos, empresas, pessoas físicas ou quaisquer outros alvos. Partindo disto, emergem e/ou fortalecem-se táticas bélicas, em principio desconhecidas, caracterizadas pela espionagem, sabotagem e manipulação de informações por meio de tecnologias de conexão em rede. Por isso, a segurança do ciberespaço tem ganhado cada vez mais atenção dos Estados e passou a ser inserida nas agendas de muitos governos e organizações internacionais.

A segurança e defesa dos ciberespaços nacionais pode ser definida, portanto, como investidas ligadas ao gerenciamento, proteção e manutenção de redes de computadores e de transmissão de informações em que são desenvolvidos, salvos e distribuídos os segredos e demais informações de diferentes países.

Partindo disto, este artigo apresenta uma análise descritiva do posicionamento do governo brasileiro em relação às políticas de segurança e defesa do ciberespaço nacional, a partir da análise do "Manual de Campanha - Guerra Cibernética", de 2017. Este é um dos principais documentos que estipulam e regulam tais práticas de segurança e defesa no Brasil. Para tanto, são apresentadas, em sequência, questões teóricas pertinentes, a metodologia seguida e uma discussão sobre documento tendo em vista preceitos das Relações Internacionais.

2. Ciberespaço

O ciberespaço é a integração dos meios globais de informação, ou seja, uma dimensão com capacidade imensa e impossível de ser plenamente administrada devido à enorme quantidade de informações que contém. As tecnologias contemporâneas servem de estrutura para o ciberespaço, oportunizando maior capacidade de comunicação, criação de ambientes virtuais para socialização, sistematização e mercado de informações e conhecimento (Levy, 1993, 1999).

Guimarães Júnior (2004) descreve o ciberespaço como um fenômenos social interdisciplinar que é motivado pela conexão de diversas tecnologias de informação. Assim, é composto por “redes sociais” que constituem e/ou fortalecem “culturas locais” por meio de sistemas técnicos. O ciberespaço, portanto, muda rapidamente, sobretudo em virtude dos propósitos dos usuários da rede que são dinâmicos e numerosos (Boff & Fortes, 2014).

Lazzarin, Netto & Souza (2015, p. 24) argumentam que em função "da rede mundial de computadores, conhecida como Internet, e dos programas de computador que viabilizam a comunicação e a interatividade com ela" emergiram, desde os anos de 1990, novos meios de abertura no espaço para o estabelecimento de relações e de valores sociais, tendo em vista a abundância de informações que oportuniza aos usuários o alcance de diferentes mundos.

Atualmente, considerando-se as rápidas e dinâmicas de transformação desta dimensão, acumulam-se ameaças da mesma forma que ocorre o crescimento de atores que se utilizam de práticas como hacking e cracking para praticarem atos criminosos Kumar & Agarwal (2018) explicam que hacking é o ato de invadir ou entrar em sistemas, resultando em melhorias ou sabotagem. Apesar do hacking nem sempre ser danoso, na atualidade, liga-se frequentemente o hacking a ataques feitos por hackers, entre eles, as atividades ilegais, os crimes cibernéticos ligados a vantagens financeiras, o roubo (ou coleta) de informação e a espionagem.

Na mesma linha de raciocínio, Negi (2011) explica que o cracking tem como objetivo “quebrar” senhas de redes de Wi-Fi e contas de usuários para colher dados e piratear programas. O “cracking” é o ato ilegal de “quebrar” senhas, diferentemente do “hacking” que tem intenções boas ou ruins (Academy, 2016). Assim, o “cracking” é caracterizado por más intensões, se caracterizando como uma atividade criminosa. As práticas desleais, como a dispersão de vírus, a clonagem de números de cartões de crédito, a eliminação de arquivos e o roubo de dados pessoais para venda são desempenhadas pelos “crackers”.

Muitas vezes, tais atos são considerados verdadeiras ações de guerra, pois agem atrapalhando e impedindo todas as práticas institucionais de um país. Assim, é relevante

destacar que no ciberespaço, a formação de grupos detentores de informações é um diferencial na balança de poder do mundo. Segundo Velloso (2008, p. 128), "[...] o ciberespaço não se constitui, por si mesmo, em garantia de conquista de democracia, igualdade e ou liberdade." Para o autor, apesar dos novos fatores temporais e territoriais, as desigualdades de força continuam se destacando, não apenas no sentido físico, mas, também, de um modo simbólico com um significado mais amplo.

Nunes (2012) argumenta que o ciberespaço faz com que se crie um ambiente de responsabilidade coletiva, onde os direitos e deveres acerca da segurança devem seguir a lógica e as noções que constituem a Segurança e Defesa do Estado, de cada país. Medeiros, Carvalho & Goldoni (2019) dizem que o ciberespaço é um novo meio de controle que interfere e constitui as relações de poder, pois as fronteiras do espaço físico, no ciberespaço, não servem para impossibilitar o fluxo de informações relevantes e/ou secretas. Isso ocasiona uma desterritorialização, já que os fluxos de informações são interconectados, mesmo estando em diferentes territórios.

Assim, da mesma maneira que a maioria dos países se preocupam, atualmente, com seus ambientes cibernéticos, o Brasil está engajado no desenvolvimento de melhores práticas em relação ao seu. O sistema internacional já está no patamar da geoestratégia do ciberespaço, sendo assim, ele é considerado um elemento do interesse geopolítico dos Estados (Balão, 2014, p. 219). Nesse contexto, o autor defende:

> Quer no contexto nacional, regional (multinacional) ou internacional (transnacional), a boa governação do ciberespaço dependerá, sempre, das relações de cooperação que, efetivamente, se conseguirem estabelecer entre os vários atores responsáveis, sobretudo, pela alimentação e manutenção do sistema.

O ciberespaço brasileiro tem seu gerenciamento executado de forma descentralizada, sendo dividido para várias entidades do setor público. Cada instituição tem uma forma distinta, alinhada aos seus valores e missões, de colaborar com a defesa do ciberespaço do país. Deste modo, criou-se um sistema adequado para a defesa do território cibernético brasileiro (Silva Filho & Moraes, 2012).

Dentre as entidades que contribuíram para a construção de elementos de segurança para o ciberespaço brasileiro estão a Presidência da República, o Ministério da Defesa e o Gabinete de Segurança Institucional da Presidência da República. As três entidades criaram documentos que visam a securitização do ciberespaço brasileiro por meio de movimentos ordenados e previamente planejados. Dentre os documentos, destacam-se as seguintes: o

Marco Civil da Internet (Lei n° 12.965/2014), criado pela então Presidente Dilma Rousseff, no ano de 2014, a Doutrina Militar de Defesa Cibernética (MD 31-M07), a Política Cibernética de Defesa (PCD) e a Estratégia Nacional de Defesa (END) (Silva Filho & Moraes, 2012).

Tais documentos, quando articulados, direcionam as discussões acerca da segurança do ciberespaço nacional de modo a inseri-las no contexto das estratégias de defesa de Estado, relevantes para as discussões internacionais, conforme apresentado na sequência.

3. Segurança e Defesa do Ciberespaço Nacional

O Estado tem como objetivo fornecer segurança para todas as dimensões que lhe envolvem e, portanto, é necessário que os diferentes gestores de segurança disponibilizem estratégias eficazes. Assim a discussão insere-se no contexto das questões acerca da defesa. Dependendo do ambiente em que são desenvolvidas, segurança e defesa podem ser operadas a partir dos mesmos meios e funções, porém, são práticas diferentes. Quando as estratégias de garantia de segurança são direcionadas para o ambiente interno de um Estado, denomina-se Segurança Pública e quando são voltadas para o ambiente externo, internacional, chama-se de Defesa Nacional. No segundo caso, considera-se o poder militar, com apoio da esfera política, sobretudo se/ou quando a diplomacia não revolver os impasses por meios de reuniões, acordos ou tratados (Lopes, 2017).

Na edição do Livro Branco de Defesa Nacional do Brasil, publicado em 2012 e elaborado pela Lei Complementar nº 136, de 25 de agosto de 2010, são apresentados assuntos relativos à defesa nacional e às atribuições do Ministério da Defesa. Assim, foram estipuladas premissas para o programa que precisam ser seguidas quais sejam, “[...] contemplar multidisciplinaridade e dualidade das aplicações; fomentar a base industrial de defesa; induzir a indústria nacional a produzir sistemas inovadores; e produzir componentes críticos nacionais” (Livro Branco de Defesa Nacional do Brasil, 2012, p. 68-69).

A Defesa Nacional é administrada pelo Ministério da Defesa, órgão público federal responsável por organizar os interesses de defesa, colaborando para assegurar a soberania nacional, com poderes para manter a ordem nacional, colaborando, também para a defesa dos interesses nacionais e auxiliando a introdução do Brasil no cenário das relações internacionais. O Ministério da Defesa também é visto como “[...] um ator político responsável por fomentar a cooperação com os demais setores governamentais que tenham

relação com a defesa do País, alinhando projetos de defesa com os programas desenvolvidos por outras áreas do governo." (Livro Branco de Defesa Nacional do Brasil, 2012, p. 55).

Para a Defesa Nacional, os setores cibernético, espacial e nuclear são considerados de extrema importância para as estratégias de defesa (Livro Branco de Defesa Nacional do Brasil, 2012). Determinado pela Diretriz Ministral do Ministério da Defesa (no 14/2009), o setor cibernético de estratégia nacional é de responsabilidade do Exército, tendo como prioridade promover o desenvolvimento e qualificação tecnológica, também científica do País (Diretriz Ministral do Ministério da Defesa n. 14, 2009).

O mesmo documento aponta que em vista de possíveis ameaças ao ciberespaço nacional, a defesa do ciberespaço brasileiro, passou a ser uma preocupação, já que apresenta perigos relativos às infraestruturas fundamentais, às operações e ao domínio de sistemas e órgãos ligados a segurança nacional. Assim, o setor de defesa cibernética dispõe de vários elementos interorganizacionais e intraorganizacionais, com uma rede interdisciplinar que fornece inúmeros produtos e serviços tecnológicos, com o desenvolvimento e capacitação de pessoal, elaboração de pesquisa científica. A introdução do Setor Cibernético, perante a supervisão do Exército tem o intuito de manter o sigilo e a liberdade, com subjetividade e efetividade de todas as informações que percorrem e são armazenadas nas redes do governo.

Sendo assim, é importante destacar que para o Centro de Defesa Cibernética (CDCiber), gerenciado pelo Exército, juntam-se interesses de organizações governamentais já atuantes, no esforço da "[...] melhoria da capacitação dos recursos humanos; atualização doutrinária; fortalecimento da segurança; respostas a incidentes de redes; incorporação de lições aprendidas; e proteção contra-ataques cibernéticos". Dentro do CDCiber há um subprojeto implementado no ano de 2012, com término previsto para 2023, que considera a capacidade de evolução do setor para Comando de Defesa Cibernética das Forças Armadas e propõe a criação da Escola Nacional de Defesa Cibernética (Livro Branco de Defesa Nacional do Brasil, 2012, p. 69).

O Ministério da Defesa estabeleceu, um espaço para se pensar e estrategizar sobre questões ligadas ao ciberespaço brasileiro, interligando o Ministério da Defesa e as Forças Armadas na defesa do ciberespaço do Brasil (Doutrina Militar de Defesa Cibernética - MD31-M-07, 2014). Logo em seguida, criou-se o Manual de Campanha EB70-MC-10.232 - Guerra Cibernética (Manual de Campanha, 2017).

A Doutrina Militar de Defesa Cibernética determinou não somente o que é espaço cibernético, mas também o que significa defesa cibernética, no Brasil, conforme abaixo:

> conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente; e Espaço Cibernético – espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (Brasil, 2014, p. 22).

Segundo Carvalho (2011), todos os setores estatais deverão cooperar para aumentar a competência da segurança nacional levando em conta, em especial, duas questões do Setor Cibernético: a) a capacidade da segurança em setores com infraestruturas comprometidas; b) aprimoramento de meios, ferramentas e estratégias que diminuam a fragilidade dos sistemas de contra-ataques da Defesa Nacional tem para ataques cibernéticos.

Tal situação evidencia que ainda existem pontos a serem atentados no que se refere à segurança e à defesa do ciberespaço brasileiro. Apesar das investidas iniciais, pelo que pode ser observado em argumentos de especialistas é que, em comparação à outros Estados, o Brasil necessita investir maiores esforços para se colocar, de forma equilibrada, no sistema internacional. Um dos meios para tanto, é o documento intitulado Manual de Campanha – Guerra Cibernética. A partir disto, a seguir, são esclarecidos os percursos da investigação e a formatação do Manual, de 2017.

4. Metodologia

A investigação se baseou nos parâmetros que definem as pesquisas qualitativas, sendo desenvolvida por meio de análise documental com caráter descritivo.

Silveira & Córdova (2009) explicam que a pesquisa qualitativa é caracterizada por alguns aspectos, como: a objetivação de um fenômeno; o estabelecimento de uma ordem nas ações de explicar, assimilar e esclarecer o fenômeno, a definição da relação do global e local do fenômeno em questão, na diferenciação correta do mundo social em relação ao mundo natural, o respeito a interação entre os objetivos investigados e suas referências teóricas e de suas experiências e a busca por resultados autênticos e confiáveis.

Na pesquisa descritiva, as informações exploradas, mencionadas e estudadas, são relacionadas e analisadas pelos pesquisadores. Assim, “incluem-se, entre as pesquisas descritivas, a maioria daquelas desenvolvidas nas ciências humanas e sociais, como as

pesquisas de opinião, mercadológicas, os levantamentos socioeconômicos e psicossociais" (Prodanov & Freitas, 2013, p. 52). Desta forma, entende-se que,

> [...] tal pesquisa observa, registra, analisa e ordena dados, sem manipulá-los, isto é, sem interferência do pesquisador. Procura descobrir a frequência com que um fato ocorre, sua natureza, suas características, causas, relações com outros fatos. Assim, para coletar tais dados, utiliza-se de técnicas específicas, dentre as quais se destacam a entrevista, o formulário, o questionário, o teste e a observação.

Tais pesquisas podem ser desenvolvidas por meio de documentos. Assim, na análise documental ocorre a utilização de um documento como instrumento de busca. São utilizadas fontes primárias, tais como "relatórios de pesquisas ou estudos, memorandos, atas, arquivos escolares, autobiografias, reportagens, cartas, diários pessoais, filmes, gravações, fotografias, entre outras matérias de divulgação". Os documentos também podem ser oficiais, públicos e/ou privados, sendo que, no segundo caso, é necessária a autorização de seus proprietários (Kripka, Scheller & Bonotto, 2015, p. 59). A análise documental procura retirar as informações de um documento original, buscando apresentar o conteúdo de forma resumida, porém fazendo uma análise fundamentada (Kripka et al., 2015).

> A pesquisa documental trilha os mesmos caminhos da pesquisa bibliográfica, não sendo fácil por vezes distingui-las [...]. A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão etc. (Fonseca, 2002, p. 32).

Partindo disto, O Manual de Campanha – Guerra Cibernética, de 2017, é um documento público, composto por prefácio, seguido por 5 capítulos e referências. O primeiro capítulo é introdutório e apresenta um pequeno resumo da finalidade e das considerações finais. No capítulo 2, encontram-se os fundamentos relativos à segurança e defesa do ciberespaço nacional. Ele está dividido em 7 subcapítulos: Considerações Gerais, A Guerra Cibernética e o Conceito Operativo do Exército, os Conceitos Básicos, os Princípios de Emprego, as Características da Guerra Cibernética, as Possibilidades de Guerra Cibernética e as Limitações da Guerra Cibernética.

No capítulo 3 são definidas as Estruturas e Responsabilidades na Guerra Cibernética. É dividido em três subcapítulos: Considerações Gerais, a Visão Sistêmica e as Capacidades do Sistema de Guerra Cibernética do Exército. Nos capítulos seguintes 4 e 5, é contextualizada á Guerra Cibernética.

O capítulo 4 discorre sobre Guerra Cibernética no contexto das funções de combate, por meio de quatro subcapítulos: Considerações Gerais, Atividades da Guerra Cibernética, Atividades, Tarefas e Ações da Guerra Cibernéticas e A Integração da Capacidade Cibernética com as Funções de Combate.

Por último, o capítulo 5, explica o que é A Guerra Cibernética nas Operações Terrestres. Ele é dividido em seis subcapítulos: Considerações Gerais, Operações Combinadas, Operações Ofensivas, Operações Defensivas, Operações de Cooperação com Agências e Operações de Informação.

5. Políticas de Segurança e Defesa a Partir do Manual de Campanha – Guerra Cibernética

O Manual de Campanha - Guerra Cibernética foi criado com a finalidade de determinar os princípios da Doutrina de Guerra Cibernética do Exército Brasileiro, viabilizando, assim, o estudo de questões ligadas ao ciberespaço dentro do próprio Exército. Diante disto, o Estado brasileiro busca regular suas ações de poder para se equiparar a outros países, em termos de forças, caso aconteçam crises diplomáticas. Articula-se, ainda, à Doutrina Militar de Defesa Cibernética para atuar com as Forças Armadas na direção de defender o espaço cibernético brasileiro. O manual aborda, portanto, o nível tático que é de designação do Exército, requerendo que os comandantes compreendam e saibam como agir dentro do ciberespaço (Manual de Campanha - Guerra Cibernética, 2017).

O Ministério da Defesa divide as ações sobre o espaço cibernético em três níveis: o nível político, o nível estratégico e o nível operacional e tático. O nível político é chamado de Segurança da Informação e Comunicação (SIC) e Segurança Cibernética. Tais ações são gerenciadas pela Presidência da República, juntamente com a administração pública federal, assim como as questões de infraestrutura de informações (Manual de Campanha - Guerra Cibernética, 2017).

O nível estratégico lida com as questões da Defesa Cibernética. Sua responsabilidade é do Ministério da Defesa, do Estado-Maior Conjunto das Forças Armadas (EMCFA) e do alto comando das Forças Armadas, que compartilham dados com a Presidência da República e com a administração pública federal. O nível operacional e tático lida diretamente com a Guerra Cibernética, sendo designado exclusivamente para as Forças Armadas.

Pelo viés das Relações Internacionais, destaca-se que as instituições têm força para regularem as relações de poder dentro do sistema internacional, promovendo (ou buscando

promover) um equilíbrio de poderes por meio da diplomacia. Para tanto, se torna relevante que os Estados tratem dos dilemas de segurança - guerra e paz – a partir dos recursos que possuem, mesmo que de forma preventiva (Butterfiel, 1953). Morgenthau (2003) e Waltz (2002), argumentam que o Estado é visto como ator principal, sendo racional e único interessado nas questões ligadas a segurança estatal, onde somente seus interesses sobressaem. Por isso, a apropriação dos conhecimentos táticos precisa ser desempenhada pelos responsáveis técnicos do próprio governo e merece atenção e sigilo especiais.

Ao denotar a importância de se objetivar as ações no ciberespaço nacional, o Manual refere que os princípios tradicionais de uma guerra se aplicam também às atividades cibernéticas. Todavia, nas atividades cibernéticas atribui-se outros quatro princípios importantes: Efeito, Dissimulação, Rastreabilidade e Adaptabilidade (Manual de Campanha - Guerra Cibernética, 2017).

O Princípio do Efeito reflete as vantagens estratégicas, operacionais e táticas que podem afetar o mundo físico, ou seja, serem planejadas e executadas online de modo a causar impactos off-line. O Princípio da Dissimulação determina as ações que precisam ser utilizadas para se ocultar/encobrir as ações no ciberespaço, impossibilitando o rastreamento de ações no ciberespaço por outros países. O Princípio da Rastreabilidade é oposto ao Princípio da Dissimulação, pois ele intenciona a aplicação de ações para a identificação de práticas estrangeiras. O último, Princípio da Adaptabilidade, consiste na eficiência da adaptação e versatilidade da guerra cibernética dentro das mudanças do ciberespaço. Mantendo-se assim proativa, mesmo com mudanças imediatas e repentinas (Manual de Campanha - Guerra Cibernética, 2017).

As políticas que envolvem uma guerra cibernética apresentam características semelhantes às da defesa cibernética, porém são impostas nos níveis operacionais e tático. Destacam-se, aqui, oito características da guerra cibernética: 1) Insegurança Latente; 2) Alcance Global; 3)Vulnerabilidade das Fronteiras Geográficas; 4) Mutabilidade; 5) Incerteza; 6) Dualidade; 7) Função de Apoio; 8) Assimetria.

A Insegurança Latente entende que nenhum sistema operacional é completamente seguro e, portanto, considera que as informações serão sempre cobiçadas e desprotegidas. O Alcance Global opera sobre o alcance de uma guerra cibernética tendo em vista o número de países que podem ser atingidos ao mesmo tempo, visto que não existem limitações físicas no ciberespaço. Juntamente com a característica anterior, a Vulnerabilidade das Fronteiras Geográficas direciona atenção aos mecanismos de defesa Estatais em um contexto sem barreiras (Manual de Campanha - Guerra Cibernética, 2017).

A Mutabilidade e a Incerteza são políticas de segurança e defesa nacional que consideram a inexistência de manuais de ética de comportamento no ciberespaço. Não há leis e/ou padrões de funcionamento que condicionem o ciberespaço, assim, emergem incertezas que podem gerar conflitos diplomáticos. A Dualidade entra na guerra cibernética como uma ferramenta usada pelos atacantes para interagir e buscar a fragilidade dos sistemas dos adversário. Ela serve para projetar futuros ataques ou para encontrar fragilidades a fim de corrigi-las (Manual de Campanha - Guerra Cibernética, 2017).

A Função de Apoio é usada para fortalecer operações militares, juntamente com a Assimetria que visa desequilibrar as forças de ataque por meio da introdução de unidades tecnológicas que auxiliam no ataque aos inimigos (Manual de Campanha - Guerra Cibernética, 2017).

Como pode ser visto, tais políticas são fundamentais no contexto de segurança e defesa do ciberespaço brasileiro. Hobbes (2002) supõe que os Estados só podem confiar em si próprios, não podendo confiar em outros Estados ou instituições, pois eles só teriam pensariam para o si próprio. E os Estados só conseguiriam garantir sua segurança com a maximização do seu poder, sobretudo o poder vindo do setor militar. Assim, tais políticas são manejadas pelo órgão chamado Sistema de Guerra Cibernética do Exército (SGCEx). Ele é composto por “[...] um conjunto de instalações, equipamentos, doutrinas, procedimentos, tecnologias, serviços e pessoal essencial para realizar atividades de guerra cibernética” e, mais uma vez, é exclusivamente pensado e gerenciado por atores governamentais (Manual de Campanha - Guerra Cibernética, 2017).

Dentro das capacidades de operação do SGCEx estão a proteção cibernética, a capacidade de paralisar ataques e ações exploratórias contra os sistemas do governo. A proteção cibernética visa criar camadas de defesa para dificultar a entrada e ação de oponentes no seu sistema. Gomes, Cordeiro e Pinheiro (2016, p. 14) explicam que a primeira coisa que devemos entender quando falamos de proteção na rede de dados é aceitar que não existe ferramenta que gere uma proteção da totalidade das redes.

Para os autores, existem três contramedidas fundamentais para se ter uma melhor proteção, os autores designam três verbos para isso "[...] prevenir, detectar e responder". Sendo assim, ter um plano de resposta para com os ataques cibernéticos é essencial, mas estes devem conter ações de prevenção, as quais devem incluir "[...] ações de prevenção e detecção de vulnerabilidades e medidas repressivas, que são as respostas propriamente ditas aos incidentes" (Gomes, Cordeiro & Pinheiro, 2016, p. 14).

Deste modo, mostra-se a importância de se ter um plano, uma estratégia capaz de consertar toda e qualquer vulnerabilidade do sistema, estabelecendo diversas barreiras para dificultar quaisquer modos de invasão. Já Wight (1966, p. 105) argumenta que a proteção no contexto internacional pode ser vista como:

> [...] o exercício do direito à autodefesa e à coerção é justificado de forma mais completa quando ele é levado a cabo pelos membros da sociedade internacional coletivamente, ou pela maioria deles, ou por um deles autorizado pelos demais. Mas isso não exclui a possibilidade de uma ação em separado por uma potência individual ignorando a aprovação das outras potências (tradução nossa).

Por conseguinte, todo sistema de proteção serve para constranger ataques e deve estar atento a diversos níveis de ameaças. Para Kunrath (2014), qualquer indivíduo com um computador ou rede por meio da qual possa acessar a internet pode vir a envolver-se em um ataque. Neste sentido, o ataque cibernético é a capacidade de realizar ações contra os sistemas computacionais do oponente. Estas ações visam danificar, corromper, destruir ou parar os sistemas do oponente sem que seja identificado.

Gomes et al. (2016, p. 12) evidenciam que “as vulnerabilidades existentes na internet, no entanto, não abrem caminho somente para os Estados travarem guerras entre si”. Desse modo, essas vulnerabilidades que existem na internet são causadoras de temores, medos para os Estados, podendo ser elas um estopim para o início de uma guerra. Gomes et al. (2016) destacam a importância de que o resultado destes ataques cibernéticos depende da integração das estruturas de apoio cibernético do país, sendo ela a internet, deste modo quanto mais avançado tecnologicamente o país maior será o seu poder de ataque.

Trento (2008) explica que os estados são dominados pelo medo ao utilizar o termo "temor hobbesianos" e assim, destaca um dos pontos centrais da visão de outro teórico sobre o tema, Butterfield (1953). O "temor hobbesiano" caracteriza o "temor mútuo", um temor ligado pela desconfiança, em que há suspeita das atitudes, levando a precipitação de ataques, ocasionando guerras sem que haja motivos consistentes.

Esse temor mútuo entre os Estados repercute em algo chamado de "dilema de segurança", a partir do qual cada Estado, ao conhecer o poder militar dos outros, mesmo sendo capaz de realizar ataques ou práticas de defesa, prefere não arriscar. Diferentemente do ataque, na exploração cibernética, o invasor pode não ações e continuar explorando o sistema oponente, averiguando dados, despercebidamente (Gomes et al., 2016). A exploração cibernética é a capacidade de realizar ações exploratórias para buscar informações, a fim de

buscar dados precisos nos sistemas oponentes, sem que sejam rastreadas. Esta ação também possibilita descobrir antecipadamente possíveis ataques (Portaria Normativa n. 3.810/MD, 2011).

O manual destaca, também, a possibilidade de operações combinadas, que são acordos entre países. Essas operações requerem acordos e coordenação formais para estas missões. Missões conjuntas requerem grande interação entre as partes para com conflitos gerados por diferenças políticas, podendo até alguns países recusarem participar destas ações conjuntas com o receio de tais ações afetarem a soberania do seu ciberespaço (Portaria Normativa n. 3.810/MD, 2011).

No Brasil, desde o ano de 2011, a Doutrina de Operações Conjuntas (2011) propõe que operações combinadas são adotadas no intuito de ludibriar oponentes. Deste modo, são seguidos planos e operações de disfarce, em parceria com os níveis estratégico, operacional e tático. Esse disfarce, também conhecido como Dissimulação, pode ser alcançado por meio de uma "guerra eletrônica, camuflagem, desinformação, operações psicológicas, defesa cibernética e ações divisionárias (demonstrações e fintas), entre outras" (Portaria Normativa n. 3.810/MD, 2011, p. 46).

Considerando possíveis ações que levariam a uma guerra cibernética, devem-se ter o discernimento do Comando Operacional, e ser aprovado pelo Governo, deste modo pode haver a interferência das Operações Psicológicas, Operações Especiais, Inteligência com a Defesa Cibernética, para haver uma orientação tanto como se ter uma observação das ações (Portaria Normativa n. 3.810/MD, 2011).

A análise do Manual de Campanha - Guerra Cibernética, permite ver que as guerras estão em constante evolução, juntamente com o mundo. Desta forma Bull (2002, p. 252) levanta a ideia de que:

> Política Mundial [World Politics] seria, de modo geral, um nome mais apropriado para a nossa disciplina do que Relações Internacionais. [...] Eu aceito a afirmação de que hoje em dia existe um sistema político global do qual o "sistema internacional" composto por Estados é apenas uma parte (mesmo que seja a parte mais importante), e que muitas das questões que são levantadas nesse sistema político global [...] não podem ser satisfatoriamente tratadas no âmbito de uma visão que restringe nossas atenções às relações entre Estados soberanos. Para lidarmos com elas adequadamente, precisamos considerar, ao lado dos Estados, não apenas organizações de Estados, globais ou regionais, mas organizações internacionais não-governamentais, grupos transnacionais e subnacionais, indivíduos [...].

Parindo disto, os Estados considerados soberanos devem tentar organizar e gerenciar os meios de segurança mais eficazes para seus territórios, materiais ou cibernéticos. No caso destes meios serem fragilizados e/ou falharem, é necessário que hajam estratégias de segurança e defesa, conforme indicam os preceitos das Relações Internacionais que envolvem o tema.

O Manual de Campanha - Guerra Cibernética foi criado, justamente, para garantir a base dos protocolos a serem seguidos no caso do Brasil entrar em uma guerra cibernética. Assim, saber por onde começar, qual comando e de onde as ordens devem partir, são ações fundamentais aos técnicos envolvidos.

6. Considerações Finais

Ao longo deste texto foram expostas as normativas do Manual de Campanha - Guerra Cibernética, tendo em vista a relação com as políticas de segurança e defesa do ciberespaço nacional. Desde o início esclareceu-se a importância de haver um documento com regularizações devidas para com o ciberespaço.

Apresentou-se uma explanação do tema de modo a mostrar que o ciberespaço global é um novo meio de se controlar as relações de poder. Assim, os países com tecnologia mais avançada têm vantagens sobre ele. O governo brasileiro, desde que os primeiros movimentos de atenção ao ciberespaço foram feitos, trabalha na direção de regular seus mecanismos de segurança e defesa. O Manual de Campanha - Guerra Cibernética, de 2017, é o documento em que são demostradas as políticas acerca do tema.

Assim, ao ser analisado, a partir dos preceitos das Relações Internacionais, revela a necessidade de se haver um governo forte e coerente para a tomada de decisões que envolvam a segurança e a defesa do ciberespaço brasileiro. Conforme exposto, é evidente que as instituições, governo devam ter força para regularem as relações de poder dentro do sistema internacional, para que deste modo se tenha um equilíbrio de poder e não se haver guerras.

De todos os aspectos e informações obtidas a partir da pesquisa em documentos, manuais, emendas do governo, indicam que apesar da facilidade de acesso a eles, os mesmos não têm uma linguagem clara e simples do assunto, deixando muitas vezes confuso.

Por fim, entende-se que o tema, embora novo para muitos Estados e para as Relações Internacionais, está ganhando cada vez mais relevância nas decisões, políticas, por meio do investimento em estratégias por parte dos países. Neste contexto, o Brasil demonstra interesse em ser um líder no assunto, mas precisa investir pesado no desenvolvimento e investimento

do setor, pois no momento está destinado a ser somente um coadjuvante, deixando a liderança do assunto para as grandes potências.

Dentro do campo militar, a cibernética já vem sendo vista como uma quinta dimensão, direcionada para combate, junto com as demais: marítima, terrestre, aérea e espacial. Deste modo, o espaço cibernético já está orientando novas maneiras de combate e negociação entre as nações e esta dinâmica é justamente o que torna emergente a necessidade de outras discussões sobre o tema.

Referências

Academy (2016). Avast Academy. Recuperado de https://www.avast.com/pt-br/c-academy

Balão, S. M. R. (2014). As NTIC, o Ciberespaço e a "Imagem do Poder" -Uma análise ostrogorskiana da Política Global contemporânea. Agenda Política, 2(1), 204-233.

Boff, S. O., & Fortes, V. B. (2014). A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis), Florianópolis-SC, 68, 109-127. Recuperado de http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100006&lng=en&nrm=iso

Bull, H. (2002). A Sociedade Anárquica: Um Estudo da ordem na política mundial. Brasília: Ed. UnB/IPRI.

Butterfield, H. (1953). Christianity, diplomacy and war. London: Epworth.

Carvalho, P. S. M. (2011). Conferência de abertura: o setor cibernético nas forças armadas brasileiras. In Barros, O. S. R., Gomes, U. M., & Freitas, W. L. (Orgs.). Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos. Recuperado de http://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf

Diretriz Ministerial n. 014 de 2009. Brasília: MD. Recuperado de https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf

Doutrina Militar de Defesa Cibernética – MD 31-M07 de 2014. Brasília: MD. Recuperado de http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_201 4.pdf

Fonseca, J. J. S. (2002). Metodologia da pesquisa científica. Fortaleza: UEC.

Gomes, M. G. F. M., Cordeiro, S. S., & Pinheiro, W. A. (2016). A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). Revista Militar de Ciência e Tecnologia, Rio de Janeiro, 33(2), 11-18.

Guimaraes Júnior, M. J. L. (2004). De pés descalços no ciberespaço: tecnologia e cultura no cotidiano de um grupo social on-line. Horizontes Antropológicos, Porto Alegre, 10(21),123-154. Recuperado de http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832004000100006&lng=en&nrm=iso

Kripka, R. M. L., Scheller, M., & Bonotto, D. L. (2015). La investigación documental sobre la investigación cualitativa: conceptos y caracterización. Revista de Investigaciones UNAD, 14(2), 55-73. Recuperado de http://hemeroteca.unad.edu.co/index.php/revista-de-investigaciones-unad/article/view/1455

Kumar, S., & Agarwal, D. (2018). Hacking Attacks, Methods, Techniques and Their Protection Measures. International Journal of Advance Research in Computer Science and Management, (4), 2353-2358. Recuperado de https://www.researchgate.net/publication/324860675_Hacking_Attacks_Methods_Techniques_And_Their_Protection_Me

Lazzarin, F. A., Netto, C. X. A., & Sousa, M. R. F. (2015). Informação, memória e ciberespaço: considerações preliminares no campo da Ciência da Informação no Brasil. Transinformação, Campinas, 27(1), 21-30. Recuperado de http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-37862015000100021&lng=en&nrm=iso

Lévy, P. (1993). As Tecnologias da Inteligência: o futuro do pensamento na era da informática. Rio de Janeiro: Editora 34. Recuperado de https://wp.ufpel.edu.br/franciscovargas/files/2015/03/LEVY-Pierre-1998-Tecnologias-da-Intelig%C3%AAncia.pdf

Lévy, P. (1999). Cibercultura. (C. I. da Costa, Trad.). São Paulo: Editora 34. Recuperado de https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf

Livro Branco de Defesa Nacional do Brasil de 2012. Brasília: MD. Recuperado de www.camara.gov.br/internet/agencia/pdf/LIVRO_BRANCO.pdf

Lopes, G. V. (2017). Relações Internacionais Cibernéticas (CiberRI): O Impacto dos Estudos Estratégicos sobre o Ciberespaço nas Relações Internacionais. In Congresso Latino Americano de Ciência Política, Montevidéu. Anais... Montevidéu. Recuperado de https://tinyurl.com/y6wentvp

Manual de Campanha - Guerra Cibernética de 2017. Brasília: MD. Recuperado de https://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf/

Medeiros, B. P., Carvalho, A. C., & Goldoni, L. R. F. (2019). Uma análise sobre o processo de securitização do ciberespaço. Coleção Meira Mattos: revista das ciências militares, Rio de Janeiro, 13(46), 45-66. Recuperado de http://ebrevistas.eb.mil.br/index. php/RMM/article/view/1889

Morgenthau, H. J. (2003). A política entre as nações: a luta pela guerra e pela paz. Brasília: Editora Universidade de Brasília. Recuperado de http://funag.gov.br/loja/download/0179_politica_entre_as_nacoes.pdf

Negi, Y. (2011). Pragmatic Overview of Hacking & Its Counter Measures. In Proceedings of 5th National Conference, INDIACom-2011 Computing For Nation Development. Recuperado de https://www.bvicam.ac.in/news/INDIACom%202011/263.pdf

Nunes, P. (2012). A Definição de uma Estratégia Nacional Cibersegurança. Nação e Defesa, 133(5), 113-127.

Portaria Normativa nº 3.810/MD, de 8 de dezembro de 2011. Dispõe sobre a “Doutrina de Operações Conjuntas”. In: Doutrina de operações conjuntas. Brasília: MD. Recuperado de http://www.esg.br/images/manuais

Prodanov, C. C., & Freitas, E. C. Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. (2a ed.). Novo Hamburgo – RS: Universidade Feevale. Recuperado de http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf

Silva Filho, E. B., & Moraes, R. F. (Orgs.). (2012). Defesa nacional para o século XXI: política internacional, estratégia e tecnologia militar. Rio de Janeiro: IPEA.

Silveira, D. T., & Córdova, F. P. (2009). A Pesquisa Científica. In Gerhardt, T. E., & Silveira, D. T. (Orgs.). Métodos de pesquisa. Porto Alegre: Plageder UFRGS.

Trento, M. (2008). O tema da guerra na Escola Inglesa das Relações Internacionais. Contexto Internacional, 30(1), 171-208.

Velloso, R. V. (2008). O ciberespaço como ágora eletrônica na sociedade contemporânea. Ciência da Informação, 37(2), 103-109.

Waltz, K. N. (2002). Teoria das Relações Internacionais. (M. L. F. Gayo, Trad.). Lisboa-PT: Gradiva.

Wight, M. (1966). Western values in International Relations? In Butterfield, H., & Wight, M. (Ed.). Diplomatic investigations. London: Allen & Unwid.

Porcentagem de contribuição de cada autor no manuscrito

Kellin Caroline Martins – 70 %

Camilo Darsie – 30 %