

BRASIL FRENTE ÀS AMEAÇAS CIBERNÉTICAS E A SUA ATUAL CAPACIDADE DE DEFESA

RAFAEL PENNING DAS NEVES¹; MIRELE THURMER KUHN²; CHARLES
PENNAFORTE³

¹Universidade Federal de Pelotas – rafael.neves@ufpel.edu.br

²Universidade Federal de Pelotas – mirele.tkuhn@gmail.com

³Universidade Federal de Pelotas – charles.pennaforte@ufpel.edu.br

1. INTRODUÇÃO

Este trabalho está sendo desenvolvido no âmbito do Grupo de Pesquisa CNPq Geopolítica e Mercosul (GeoMercosul) e do Laboratório de Geopolítica, Relações Internacionais e Movimentos Antissistêmicos (LabGRIMA), dentro do projeto de pesquisa “A Cibersegurança como cenário das disputas geopolíticas contemporâneas: dimensões, perspectivas e análises”. O atual trabalho busca a compreensão acerca da capacidade de enfrentamento do Brasil frente às ameaças cibernéticas no sistema internacional, por conta das dinâmicas de inserção no novo mundo de conexões, cuja tendência é de transferência das guerras de poder materiais para as tecnológicas.

Os períodos que antecedem o século XXI adentram as pautas de política de defesa por parte dos Estados com o surgimento da Escola de Copenhague em 1990 e a teoria da securitização no espectro de assegurar a integridade das instituições e dos territórios nacionais no contexto que sucedeu a Guerra Fria. Compreendendo o entendimento de ameaça, caracterizada por um agente como o Estado, de maneira mais extrema pela politização, a convergência tende a securitizar a questão. (BUZAN; WAEVER; DE WILDE, 1998)

Portanto, a visão de que o ciberespaço como advento informacional e ferramenta globalizada também insere a relação de territorialidade e a acessibilidade das questões cibernéticas, tal qual desempenham-se trocas e práticas no ambiente virtual que reverberam sobre as regulações frente ao papel do Estado, sobretudo as ameaças e a tipificação de crimes previstos pela legislação nacional perpetrados no meio cibernético - outrora - passíveis de neutralização ou sanção.

Neste contexto, o Brasil vem propondo suas estratégias no âmbito de defesa pela institucionalização, produzindo documentos na premissa de lapidar a concepção da defesa nacional, dispendo de uma nova visão sobre a proteção de dados e informações. Aspectos que PAGLIARI et al. (2020) aduzem a interposição de diretrizes formuladas pelo governo brasileiro e apresentadas para que haja a caracterização das estratégias ao setor de defesa, destacando-se a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa e sobretudo o Livro Branco de Defesa (LBD).

Correspondendo ao vislumbre e a determinação de conceitos que levam as Forças Armadas a sintetizar sua estratégia frente às ameaças que podem surgir e afetar a infraestrutura crítica da sociedade civil e também do próprio governo brasileiro, os princípios norteadores são determinados pela Doutrina Militar de Defesa Cibernética (BRASIL, 2014) e que elenca: Princípio do Efeito; Princípio da Dissimulação; Princípio da Rastreabilidade; Princípio da Adaptabilidade.

2. METODOLOGIA

A fim de encontrar uma compreensão lógica para o problema de pesquisa, se faz necessária a elaboração de uma investigação a partir da análise de dados de caráter quantitativo e qualitativo, desenvolvendo-se por meio da verificação documental e de revisão bibliográfica, utilizando-se tanto fontes de caráter primário, como discursos governamentais do período estudado, quanto secundário em livros, artigos científicos e imprensa em geral.

No decorrer do projeto, com o método de definição e análise, serão apresentadas as teorias do conhecimento incluídas na pesquisa, como a influência e perspectiva dos movimentos antissistêmicos das Relações Internacionais, além da exposição dos princípios expressados que compõem os eventos estudados. Com utilização do método histórico para identificação e compreensão dos principais cenários do objeto de pesquisa, e de pesquisas bibliográficas de registros dos eventos e seus desenvolvimentos com o objetivo de encontrar e avaliar as particularidades das condições encontradas. Nos esforços de compreensão acerca do lugar ocupado pelo Brasil no sistema internacional, esta pesquisa é estruturada pela chamada Análise do Sistema Mundo (ASM), considerando o sistema-mundo como uma unidade básica de análise social e um sistema histórico (PENNAFORTE, 2011). Conforme Immanuel Wallerstein (2004), a trajetória do sistema-mundo contemporâneo é marcada por um processo de declínio da hegemonia estadunidense, cujos principais motores, a partir de uma leitura dialética, residem nas características de sua própria ascensão. Longe de assumir um caráter linear, o movimento de "aterrissagem forçada da água" se notabilizou por uma série de avanços e retardos (WALLERSTEIN, 2004, p. 21), dinâmica expressa em diferentes episódios como a Guerra do Vietnã, as Revoluções Mundiais de 1968, a Queda do Muro de Berlim e os ataques terroristas de 11 de Setembro de 2001. O aprofundamento da perda de legitimidade da liderança estadunidense abriu novas perspectivas quanto ao futuro do mundo no século XXI. A perspectiva de um reordenamento a partir da emergência de novo (s) ator(es) hegemônico(s) e a configuração de novos polos regionais reafirma a importância do Brasil estar melhor preparado para o enfrentamento das novas novas de ameaças oriundas das disputas geopolíticas no âmbito do espaço cibernético.

Sendo assim, a pesquisa procurará responder às seguintes indagações: sob o ponto de vista da arquitetura de defesa cibernética, o Brasil dispõe de mecanismos para fazer frente às ameaças oriundas deste novo cenário? O Brasil está preparado para enfrentar esse cenário de embates geopolíticos entre as grandes potências, cujos reflexos podem criar sérios problemas para os Estados?

3. RESULTADOS E DISCUSSÃO

A pesquisa encontra-se em sua fase inicial, especificamente na coleta e análise de dados com o intuito de garantirmos uma abordagem coerente aos objetivos propostos. Contudo, face à análise de material já obtido é possível observar assimetrias qualitativas com países do chamado Centro Sistêmico, em especial com os EUA. O Brasil precisa acelerar o desenvolvimento de suas capacidades de defesa no âmbito cibernético como forma de garantir proteção para essas novas ameaças.

4. CONCLUSÕES

A pesquisa será desenvolvida ao longo do 2º semestre de 2022 e durante 2023, quando finalizada, os resultados serão publicados em revistas indexadas.

Contudo, foi já possível verificar pontos de fragilidades na capacidade do Brasil enfrentar a gama de dilemas propostos pela nova realidade da cibersegurança. A dificuldade enfrentada pelo Ministério da Defesa no âmbito orçamentário é um aspecto relevante de nossas debilidades.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Doutrina Militar de Defesa Cibernética**. Ministério da Defesa: Brasília, 1ª Edição, 2014. Disponível em:

<https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 17 de agosto de 2022.

BUZAN, B.; WAEVER, O.; DE WILDE, J. **Security: A New Framework for Analysis**. Colorado: Lynne Rienner Publishers, p. 239, 1998.

PAGLIARI, G. C.; PINTO, D. J. A.; VIGGIANO, J. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: Um estudo prospectivo. In: OLIVEIRA, M. A. G. (Org.) **Defesa cibernética e mobilização nacional**. Recife: Ed. UFPE, 2020. p. 153–174. Disponível em: <<https://reductidc.com.br/assets/files/Defesa-cibernetica-e-mobilizacao-nacional.pdf>>. Acesso em: 17 de agosto de 2022.

PENNAFORTE, C. **Análise dos Sistemas-Mundo**: uma pequena introdução ao pensamento de Immanuel Wallerstein. Rio de Janeiro: CENEGRI - Centro de Estudos em Geopolítica e Relações Internacionais, 2011.

WALLERSTEIN, I. **O declínio do poder Americano**. Rio de Janeiro, Contraponto, 2004.