CIBERSEGURANÇA NO BRASIL CONTEMPORÂNEO: DESAFIOS NO PROCESSO DE REESTRUTURAÇÃO DAS POLÍTICAS DE SEGURANÇA E DEFESA (2020-2024)

RAFAEL PENNING[1]; CHARLES PENNAFORTE[2]

[1]*Universidade Federal de Pelotas – penning.rafael@gmail.com*
[2]*Universidade Federal de Pelotas – charles.pennaforte@ufpel.edu.br*

1. INTRODUÇÃO

Esse trabalho consiste na apresentação dos resultados finais do projeto de pesquisa "A cibersegurança como cenário das disputas geopolíticas contemporâneas: dimensões, perspectivas e análises", desenvolvido junto ao Grupo de Pesquisa CNPQ Geopolítica e Mercosul (GeoMercosul) e no Laboratório de Geopolítica, Relações Internacionais e Movimentos Antissistêmicos (LabGRIMA). A pesquisa buscou compreender quais ações o Brasil está tomando para responder à progressão da inserção de suas políticas de ciberdefesa no presságio de conflitos em domínio tecnológico.

Esses esforços visam promover uma nova abordagem sobre a proteção de dados e informações, refletindo um compromisso com o fortalecimento da segurança cibernética no país. Nesse contexto, o Brasil tem desenvolvido suas estratégias de defesa por meio de políticas públicas de prevenção e participação, elaborando documentos com o objetivo de aprimorar a concepção da defesa nacional. Reflete-se o esforço do governo em consolidar uma estratégia eficaz diante das potenciais ameaças que podem comprometer a infraestrutura crítica da sociedade brasileira no âmbito civil, público e privado, com a determinação de que as esferas de defesa estejam preparadas para enfrentar desafios cibernéticos e garantir a segurança nacional em um cenário de crescente interdependência tecnológica. A pesquisa responderá duas questões: em suas ações de defesa cibernética, o Brasil progrediu em políticas públicas para responder às ameaças desse novo cenário? Quais são as iniciativas governamentais e a participação dos atores da sociedade nesse processo?

2. METODOLOGIA

Para responder o problema de pesquisa, foi essencial a condução de uma investigação com base na análise de dados qualitativos. Essa análise desenvolveu-se por meio da verificação documental e da revisão bibliográfica, utilizando tanto fontes primárias, como discursos governamentais do período estudado, quanto fontes secundárias, como livros, artigos científicos e reportagens da imprensa em geral.

Fazendo uso do método histórico para identificar e compreender os principais cenários relacionados ao objeto de pesquisa, além de análise bibliográficas e textos acerca de registro de eventos e seus respectivos desenvolvimentos, busca-se avaliar as particularidades do engajamento das políticas do Estado brasileiro em relação à pauta de cibersegurança. No intento de vislumbrar o papel do Brasil como partícipe do sistema internacional, esta pesquisa estruturou-se com base na Análise do Sistema-Mundo (ASM), que considera o sistema-mundo como a unidade básica da análise social e um sistema histórico (PENNAFORTE, 2020).

De acordo com Wallerstein (2004), o sistema-mundo contemporâneo tem passado por um processo de declínio da hegemonia dos Estados Unidos, cujas

origens, em uma análise dialética, podem ser atribuídas às características inerentes à própria ascensão estadunidense. Essa leitura é corroborada pela contribuição de Arrighi (1996), que identifica na atual crise da hegemonia dos EUA sinais de um deslocamento de poder no sistema-mundo. A posição central dos Estados Unidos tem sido crescentemente questionada em outras temáticas, à medida que novas potências econômicas, como a China, emergem e estão desempenhando novos diálogos no âmbito da cibersegurança.

Portanto, advindo desse contexto, empreende-se a possibilidade de um reordenamento global que elucide o surgimento de novos atores hegemônicos e a formação de novos polos, em âmbito regional, de poder. Com isso, reforçamos a importância do Brasil posicionar-se e preparar-se para um cenário de disputas geopolíticas em domínio virtual.

3. RESULTADOS E DISCUSSÃO

A relevância da cibersegurança no contexto brasileiro se reflete em movimentos e esforços realizados na esfera política doméstica, que culminaram em reconhecimento por parte da União Internacional de Telecomunicações (UIT). Segundo essa organização, o Brasil ocupa a terceira posição no continente americano, atrás dos Estados Unidos e do Canadá (BRASIL, 2021). Através da Estratégia Nacional de Segurança Cibernética (2020), verifica-se que apenas 11% dos órgãos federais brasileiros possuem uma estrutura e governança eficiente em termos de cibersegurança, embora 100% das instituições federais, estaduais e municipais realizem atividades que envolvem infraestrutura digital potencialmente crítica (BRASIL, 2020).

No que tange aos investimentos na área, observa-se uma significativa redução de recursos. Em 2013 previa-se um orçamento de aproximadamente R$ 100 milhões para a defesa cibernética, conforme discurso de Celso Amorim, no qual admitiu fragilidades na segurança da informação (G1, 2013). No entanto, o Plano Plurianual 2020-2023 omitiu o tema, alocando apenas R$ 6,3 milhões ao Comando de Defesa Cibernética (CDCiber), órgão que enfatiza a necessidade de R$ 60 milhões para desenvolver e implementar medidas essenciais à ampliação da área no âmbito governamental (AGÊNCIA SENADO, 2019).

As instituições governamentais têm destacado essa discussão, de avanço na política de ciberdefesa, em resposta à crescente informatização no cotidiano. Com a digitalização acelerada de produtos e serviços em diversos setores, a 1ª Reunião do Comitê Nacional de Cibersegurança (CNCiber), realizada em 20 de março deste ano, reflete a continuidade do diálogo entre governo, instituições, empresas e sociedade civil. Durante o encontro, foi proposta a realização de reuniões trimestrais e futuras atualizações na Política Nacional de Cibersegurança (PNCiber), com ênfase na construção de estratégias de cooperação técnica internacional para o fortalecimento da resiliência cibernética.

No atual mandato de Lula da Silva, retomam-se as discussões sobre segurança da informação, com foco em ações efetivas para articular a legislação e ampliar a proteção das infraestruturas críticas. Ressalta-se a necessidade de fortalecer a cooperação na criação de mecanismos para mitigar ameaças cibernéticas de impacto generalizado. Durante a pandemia de COVID-19, o Brasil modernizou suas infraestruturas cruciais, implementando políticas como o trabalho em nuvem híbrida e intensificando a participação das empresas no processo de digitalização. Diante de uma concorrência acirrada e de alta fragmentação, o setor de segurança cibernética apresenta oportunidades

significativas para prestadores de serviços, à medida que um número crescente de empresas adota a digitalização.

4. CONCLUSÕES

O histórico de redução de investimentos, exemplificado pela queda no orçamento destinado à defesa cibernética, é um alerta para a vulnerabilidade do país. Em 2013, Celso Amorim, então ministro da Defesa, já admitia fragilidades nessa área, com previsão de um orçamento de R$ 100 milhões. No entanto, o Plano Plurianual 2020-2023 indicou uma queda drástica desse valor, alocando apenas R$ 6,3 milhões ao Comando de Defesa Cibernética (CDCiber), muito abaixo dos R$ 60 milhões apontados como necessários.

Esses desafios são especialmente preocupantes à luz da crescente digitalização das atividades econômicas, governamentais e sociais. Com a expansão da internet das coisas (IoT), o uso intensivo de big data e a automação de processos, as ameaças cibernéticas se tornam mais complexas e diversificadas, exigindo uma abordagem proativa e bem estruturada por parte do governo brasileiro. A baixa expectativa em relação aos investimentos necessários para enfrentar essas ameaças compromete não apenas a segurança das informações, mas também a capacidade do Brasil de se posicionar de forma segura em um mundo cada vez mais digitalizado.

Com o aumento da demanda por serviços que neutralizem ataques cibernéticos, observa-se também uma elevação significativa das ações contra as infraestruturas de dados no Brasil. De acordo com a Mordor Intelligence (2024) no primeiro trimestre deste ano, o país registrou mais de 5 milhões de ataques cibernéticos, um aumento expressivo em comparação ao ano de 2023, seguindo uma tendência semelhante à observada nas infraestruturas dos Estados Unidos. O mercado brasileiro de cibersegurança está estimado em US$3,34 bilhões para este ano, com projeções de crescimento para US$5,46 bilhões nos próximos cinco anos (MORDOR INTELLIGENCE, 2024). Apesar do aumento na procura por soluções de segurança, a oferta ainda permanece incerta, o que representa uma oportunidade para as empresas que desejam transferir suas operações para a Internet. Esse cenário é favorecido pelo desenvolvimento da infraestrutura de redes, possibilitando a busca por soluções que atendam às normas estabelecidas pela legislação brasileira.

A expansão de parcerias e aquisições estratégicas têm fortalecido o portfólio do setor de cibersegurança, oferecendo recursos e serviços personalizados em uma infraestrutura mais robusta. Com a crescente implementação de dispositivos IoT, as empresas tornam-se mais vulneráveis, pois o aumento dos pontos de fragilidade facilita o acesso de invasores a ativos digitais. Essa realidade exige uma atenção especializada para proteger esses sistemas. Para manter a segurança e preservar os interesses comerciais, torna-se essencial a adoção de medidas rigorosas contra ameaças externas. Essa necessidade está gerando uma tendência de maior integração entre as indústrias que utilizam IoT, diversificando as exigências e os níveis de soluções de segurança, o que abre espaço para que empresas do setor de cibersegurança concorram nesses novos segmentos.

É essencial destacar que a cooperação técnica e as parcerias estratégicas revelam um grande potencial para fortalecer políticas de defesa mais assertivas, especialmente com a participação ativa dos stakeholders nas interações que promovem a transformação, pesquisa e desenvolvimento de ferramentas voltadas

para a proteção das infraestruturas brasileiras. Diante disso, torna-se evidente a necessidade de investir em pesquisa, desenvolvimento e capacitação técnica de profissionais no setor de cibersegurança. Em relatório recente aponta-se um déficit de 441 mil profissionais de segurança cibernética no Brasil (MORDOR INTELLIGENCE, 2024), o que demonstra a urgência de formar especialistas que possam atuar em um campo em constante evolução, desenvolvendo estratégias comparadas e ampliando a capacidade de defesa da informação no país.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ARRIGHI, G. **O Longo Século XX**. Dinheiro, Poder e as Origens do Nosso Tempo. São Paulo: UNESP, 1996.

BRASIL. Agência Senado. **Governo negligencia defesa cibernética do país, aponta relatório da CRE**. Brasília, DF, 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/12/12/governo-negligencia-defesa-cibernetica-do-pais-aponta-relatorio-da-cre>. Acesso em: 05 de outubro de 2024.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. **Aprova a Estratégia Nacional de Segurança Cibernética**. Brasília, DF, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em: 06 de outubro de 2024.

BRASIL. Gabinete de Segurança Institucional. **Comitê Nacional de Cibersegurança promove sua primeira reunião**. Disponível em: <https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/2024/comite-nacional-de-ciberseguranca-promove-sua-primeira-reuniao>. Acesso em: 25 mar. 2024.

BRASIL. Ministério da Economia. **Brasil melhora posição no ranking mundial de cibersegurança**. Brasília, DF, 2021. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/2021/julho/brasil-melhora-posicao-no-ranking-mundial-de-ciberseguranca>. Acesso em: 03 de outubro de 2024.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** 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.

BRASIL sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado. **Security Report**, 01 de março de 2023. Disponível em: <https://www.securityreport.com.br/overview/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022/>. Acesso em: 29 de abril de 2023.

MORDOR INTELLIGENSE. **Brazil Cybersecurity Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)**, 2024. Disponível em: <https://www.mordorintelligence.com/industry-reports/brazil-cybersecurity-market>. Acesso em: 15 mar. 2024.

NÉRI, Felipe. **No Senado, Celso Amorim admite vulnerabilidades na defesa cibernética**. G1, Brasília, 10 de Julho de 2013. Política. Disponível em: <https://g1.globo.com/politica/noticia/2013/07/ministro-da-defesa-admite-vulnerabilidades-na-defesa-cibernetica.html>. Acesso em: 04 de Outubro de 2024.

PENNAFORTE, C. **Movimentos Antissistêmico e Relações Internacionais**: uma perspectiva teórica para compreender o sistema-mundo. Pelotas, Editora UFPEL, 2020.

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