RICRI
RELAÇÕES INTERNACIONAIS

Desafios do século XXI: A ascensão do cyberpower e a definição de uma estratégia brasileira para o cyber

Érica Beatriz Guedes Corado [*†] Levi Manoel dos Santos [‡]

†Universidade de Brasília - UnB
‡Universidade Federal do ABC - UFABC
*Autor correspondente. E-mail: ericacorado11@gmail.com

Resumo

A ascensão do *cyber* trouxe novos desafios para os Estados na proteção de suas soberanias e da segurança de suas populações. A tecnologia está cada vez mais ligada à projeção de poder no Sistema Internacional, fazendo da Segurança Cibernética um campo de interesse global. Embora não haja uma guerra cibernética declarada, ataques frequentes a sistemas críticos de Estados, empresas e organizações geram medo. Este estudo visa compreender os principais conceitos de *cyber* - *cyberpower*, *cyberspace*, *cyberwar*, etc. - e sua importância para as Relações Internacionais atualmente. Igualmente, busca-se entender os caminhos estratégicos do Brasil no campo cibernético e os desafios enfrentados. Para tal, a metodologia adotada foi o estudo de caso descritivo. Ademais, tratando-se dos métodos de coleta de informação, utiliza-se a Revisão Sistemática de Literatura. Em novembro de 2009, o Ministério da Defesa designou o Exército para conduzir o setor cibernético, com capacidades operativas de proteção, ataque e exploração cibernética. A estratégia brasileira enfrenta limitações na identificação e atribuição de responsabilidades por ataques cibernéticos. A análise da estratégia de Defesa Cibernética revela que as instituições ainda não estão totalmente preparadas para enfrentar conflitos no espaço cibernético, destacando a necessidade de aprimoramento das capacidades de resposta e proteção.

Palavras-chaves: Planejamento Estratégico, *Cyberpower*, Brasil, Globalização

1. Introdução

Ao fim da II Guerra Mundial, o Sistema Internacional (SI) atravessou uma série de mudanças fundamentais. A agenda internacional passou a incluir vários novos temas, como Direitos Humanos e Meio Ambiente. Ademais, com o advento da Globalização, o SI tornou-se ainda mais interdependente e conectado, de modo que acontecimentos em um Estado podem influenciar todos os outros. Keohane e Nye (2001), em *"Power and Interdependence"*, sugerem, a partir da teoria da Interdependência Complexa que, nesse contexto, os atores são incentivados a cooperar em várias questões e a reconhecer

a insuficiência do unilateralismo para alcançar alguns objetivos em comum. Uma das manifestações disso é o papel que aparelhos eletrônicos e o virtual, em geral, passaram a ter no dia a dia de milhões de pessoas no planeta.

Esse novo cenário influencia diretamente a dinâmica das prioridades dos Estados. O arrefecimento da dicotomia *High Politics* e *Low Politics*[1] e o surgimento de uma agenda internacional mais diversificada também suscitaram novos debates para os acadêmicos de Relações Internacionais (RI). Por isso, o advento do *cyber* não pode ser ignorado nas atuais análises em RI. Na verdade, existe a necessidade de dar mais profundidade aos debates desenvolvidos nesse sentido, especialmente no que diz respeito ao poder [2]. Para mais, o Brasil não pode se atrasar nessas discussões, uma vez que o *cyber* é uma das mais relevantes pautas para o século XXI e para o futuro das RI. Tratar destas questões é fundamental para a projeção do Brasil no Sistema Internacional.

Sendo assim, esse trabalho busca responder à seguinte pergunta de pesquisa: "Qual o percurso do *Cyberpower* do Brasil e quais os principais desafios para o setor no âmbito nacional?". O objetivo deste estudo é compreender os principais conceitos envolvendo o *cyber* - *cyberpower*, *cyberspace*, *cyberwar*, etc. - e a sua importância para o campo das RI na atualidade; bem como, a partir disso, entender quais são os principais caminhos traçados no campo estratégico brasileiro acerca do *cyber* e quais são os principais desafios para o setor.

Para responder à pergunta de pesquisa aqui proposta, a metodologia adotada foi o estudo de caso descritivo que, como argumentam Baxter e Jack (2008, p.548), é usado para descrever uma intervenção ou fenômeno e o contexto da vida real em que ocorreu. Nesse caso, o desenvolvimento da trajetória do *cyberpower* no Brasil. Ademais, tratando-se dos métodos de coleta de informação, a ferramenta utilizada neste trabalho é a Revisão Sistemática de Literatura. Segundo Galvão e Ricarte (2019, p.58), esta é "uma modalidade de pesquisa, que segue protocolos específicos, e que busca entender e dar alguma logicidade a um grande corpus documental, especialmente verificando o que funciona e o que não funciona num dado contexto". Ainda, optou-se por uma revisão sistemática de caráter misto, que objetiva identificar, selecionar, avaliar e sintetizar simultaneamente estudos qualitativos, estudos quantitativos e estudos mistos; bem como leva em consideração tanto fontes primárias como secundárias (Galvão e Ricarte 2019).

No que se diz respeito à teoria e conceitualização, este estudo adota sumariamente os preceitos da corrente neoinstitucional e da teoria da Interdependência Complexa. Deste modo, a argumentação aqui desenvolvida toma como base, principalmente, os

1. De modo geral, segundo Sato (2010, p.43), "Throughout nearly four decades, during the cold war, the analysis often mentioned the existence of an international agenda divided into two levels - high politics and low politics. While high politics referred to the issues directly related to strategic security, the term low politics was used to refer to other issues like trade and development, education and other topics which are not directly associated to concerns about the strategic security of countries, especially major world powers. Important changes in international relations, however, have made this form of organization of the international agenda gradually lose its meaning."

2. Para este trabalho, considera-se o conceito de poder, com base nos estudos de Nye (2021, p.2), como "a capacidade de afetar os outros para obter os resultados desejados". O autor, além disso, evidencia que "há muitos fatores que afetam nossa capacidade de conseguir o que queremos, e eles variam conforme o contexto do relacionamento"(Nye 2021, p.2). Deste modo, o autor argumenta que existem diferentes tipos de poder, destacando as noções de *Hard Power*, de *Soft Power* e de *Smart Power* (Nye 2017).

debates desenvolvidos por Nye (2011) em seu livro "*The Future of Power*" e por Keohane e Nye (2001) em "*Power and Interdependence*". Além disso, autores como Sheldon (2019) e Pecequilo (2012) são resgatados para o desenvolvimento da argumentação.

Este trabalho está dividido em duas sessões, além de uma introdução e uma conclusão. O primeiro capítulo busca trazer um resgate teórico-conceitual acerca dos principais conceitos envolvendo o *cyber*, o que é fundamental para compreender o objeto de pesquisa, assim como a argumentação desenvolvida posteriormente. O segundo capítulo, por sua vez, trata da política estratégica brasileira para o *cyberpower*, os principais atores envolvidos e, por fim, quais são os desafios diante do país no campo do *cyber*.

2. A Ascensão do *Cyberpower*: Um Novo Tempo para as Relações Internacionais

O primeiro computador, o *Electronic Numerical Integrator and Computer*, foi desenvolvido em 1946 pelo Exército estadunidense. Em um primeiro momento, este dispositivo tinha como objetivo identificar alvos de artilharia rapidamente (Sheldon 2019). No entanto, desde então, os computadores passaram a integrar nossas vidas para além de aspectos militares, de modo que se tornaram essenciais para as mais diversas atividades do dia a dia de milhões de indivíduos ao redor do globo. Essa tendência se intensificou ainda mais a partir do surgimento da *World Wide Web*, a Internet - que foi um produto da paranoia vivenciada na Guerra Fria e também expressava objetivos militares estadunidenses e as tensões envolvendo a segurança internacional no período (Ruthfield 1995). Neste sentido, o *Advanced Research Projects Agency Network* (ARPA) criado pela *Advanced Research Projects Agency* (ARPA), agência de defesa dos Estados Unidos, delimitou o início da internet. Em "*The Future of power*", Nye (2011) argumenta que o surgimento da rede foi uma resposta à necessidade estratégica de garantir a rede de comunicações frente a um potencial conflito militar nuclear, uma vez que sistemas centralizados poderiam ser facilmente destruídos.

Deste modo, estas tecnologias "produziram mudanças surpreendentes e indeléveis nas sociedades modernas, na economia global e na condução da política e da guerra" (Sheldon 2019, p.291). Atualmente, uma enorme parcela da população - especialmente a partir dos anos 2000 - passou a ter acesso a computadores, *smartphones*, à internet, entre outros dispositivos que permitem a comunicação instantânea entre pessoas localizadas em qualquer lugar do globo, bem como acesso à informação em uma escala jamais vista até então. Por isso, muitos autores, como Nye (2011), consideram que estamos diante de uma "Revolução Informacional". Assim, argumenta-se que:

> "A principal característica desta Revolução da Informação não é a velocidade das comunicações entre os ricos e poderosos: Por mais de 130 anos, a comunicação instantânea por telégrafo tem sido possível entre a Europa e a América do Norte. A mudança crucial é a enorme redução no custo de transmissão de informações"(Nye 2011, p.115, tradução nossa).

Nesse sentido, levando em consideração que informação e comunicação são dois aspectos fundamentais para a projeção de poder, "a disseminação da informação significa que o poder será mais amplamente distribuído e as redes informais minarão o

monopólio da burocracia tradicional" (Nye 2011, p.116). Ou seja, os novos meios de acesso à informação e comunicação criam um espaço inédito que permite que relações de poder se estabeleçam: o *cyberspace*. Para Kuehl (2009), "cyberspace é um domínio operacional enquadrado pelo uso de eletrônicos para [...] explorar informações por meio de sistemas interconectados e sua infraestrutura associada" (Kuehl, 2009 *apud* Nye 2011, p.122, tradução nossa).

Outro aspecto importante do *cyberspace* é que, devido à difusão de poder que esta esfera permite, bem como o fácil acesso a ferramentas, uma série de novos atores transnacionais ganha espaço nesse meio, desde ONGs até grupos terroristas. Assim, mesmo que existissem anteriormente ao *cyberspace*, esses atores alcançaram uma nova escala de projeção e relevância na agenda internacional. Essa realidade aprofunda ainda mais a interdependência existente no Sistema Internacional. Na política mundial, interdependência "[...] refere-se a situações caracterizadas por efeitos recíprocos entre países ou entre atores de diferentes países. Esses efeitos frequentemente resultam de transações internacionais — fluxos de dinheiro, bens, pessoas e mensagens através de fronteiras internacionais." (Keohane e Nye 2001, p.7, tradução nossa). Portanto, no cerne da Interdependência Complexa está o reconhecimento da interconexão entre as dimensões política, econômica e social. Deste modo, os Estados não são mais entidades isoladas engajadas apenas em trocas políticas. Na verdade, estão imersos em uma rede complexa, onde ações em uma dimensão podem repercutir em outras (Saaida 2024).

Deste modo, para além dos tradicionais meios de projeção de poder - a terra, o ar e o mar -, entende-se que existe um novo espaço onde atores do SI podem interagir. No entanto, é importante evidenciar que, como argumenta Nye (2011), o "*cyberspace* não vai substituir o espaço geográfico e não vai abolir a soberania do Estado, mas, [...] vai coexistir e complicar muito o que significa ser um Estado soberano ou um país poderoso no século XXI" (Nye 2011, p.121-122, tradução nossa).

Nesse sentido, um conceito importante para entender como se dão as dinâmicas de poder no *cyberspace* é o de *cyberpower*. Para Nye (2011),

> "Definido comportamentalmente, o *cyberpower* é a capacidade de obter resultados preferidos por meio do uso dos recursos de informação eletronicamente interconectados do domínio cibernético. O *cyberpower* pode ser usado para produzir resultados preferidos no *cyberspace*, ou pode usar instrumentos cibernéticos para produzir resultados preferidos em outros domínios fora do *cyberspace*"(Nye 2011, p.123, tradução nossa).

Sendo assim, *cyberpower* pode ser compreendido como a capacidade de transformar elementos particulares do *cyberspace* - especialmente aqueles que envolvem a disseminação de informação e comunicação - em estratégia (Sheldon 2019). Deste modo, "esse efeito estratégico se manifesta, em última análise, nos processos cognitivos dos seres humanos, mas também pode se manifestar indiretamente nos domínios estratégicos da terra, do mar, do ar e do espaço, bem como no próprio *cyberspace*" (Sheldon 2019, p.294, tradução nossa).

No *cyberspace*, existe uma grande diversidade de atores, que, muitas vezes, são anônimos. Além disso, a distância física torna-se uma barreira a menos e ataques no meio virtual são de baixo custo e podem ser promovidos tanto por um adolescente, como

por um grupo terrorista ou um Estado. Por isso, argumenta-se que "a dependência em sistemas cibernéticos complexos para apoiar atividades militares e econômicas cria novas vulnerabilidades em grandes estados que podem ser exploradas por atores não estatais" (Nye 2011, p.125, tradução nossa).

Fica evidente, então, que a ascensão do *cyber* fez surgir novos desafios para os Estados nacionais na proteção de suas soberanias e na garantia da segurança de suas populações como um todo. Assim, "o domínio cibernético é único por ser feito pelo homem, recente e sujeito a mudanças tecnológicas ainda mais rápidas do que outros domínios" (Nye 2011, p.124).Para mais:

> "O que distingue o poder no domínio cibernético não é que os governos estejam fora de cena, como previram os primeiros cyber libertários, mas que diferentes atores possuem diferentes recursos de poder e que a lacuna entre atores estatais e não estatais está diminuindo em várias instâncias. Mas a redução relativa dos diferenciais de poder não é o mesmo que equalização. Grandes governos ainda têm mais recursos"(Nye 2011, p.132, tradução nossa).

Por fim, esse cenário recente e complexo que conta com uma enorme variedade de atores leva diversos autores a desenvolver argumentos sobre *cyberwar*: quais seriam suas características, especificidades e abrangência. De acordo com Sheldon (2019, p.295, tradução nossa), "alguns autores argumentam [...] que a ascensão do *cyberspace* mudou significativamente o caráter da guerra, tornando qualquer incidente cibernético maligno conduzido contra um estado ou sua sociedade ou economia uma nova forma de conflito". No entanto, o *cyberpower* impõe limitações de atuação, de modo que, ainda de acordo com Sheldon (2019), parece ser improvável que guerras possam ocorrer apenas no âmbito do *cyberspace*. Em suma, "uma vez que o *cyberpower*, neste contexto, é usado para atingir objetivos definíveis como parte de uma estratégia geral, talvez seja mais correto falar de "*cyberpower* na guerra, ou guerra por meios cibernéticos", em vez do termo mais enganoso *cyberwar*"(Sheldon 2019, p.295, tradução nossa).

Quando pensamos na projeção do *cyberpower*, através de um ambiente atrelado a um fator tecnológico, é importante levar em consideração que se trata de um fator que é moldado pelas ações humanas, e passa a ser estudado como uma força associada mais diretamente ao *soft power*. Essas forças estão cada vez mais relacionadas com as novas dimensões de conflito dentro do Sistema Internacional. Neste sentido, "estes recursos *soft*, principalmente o tecnológico, serão utilizados para a transformação e administração das condicionantes naturais e demográficas descritas, melhorando a posição relativa das nações que os detêm" (Pecequilo 2012).

O fator tecnológico está cada vez mais relacionado à projeção de poder no Sistema Internacional, pois permite, para além do domínio dos recursos disponíveis para os Estados, aumentar o potencial de uso destes recursos, como alguns Estados assim o fazem por meio do exercício militar, econômico e político. Este fator também está cada vez mais relacionado com o campo econômico. Os países que possuem maior arsenal tecnológico também conseguem se projetar com mais facilidade e obter maior influência política. Desta forma, um país que não detém poder tecnológico, tampouco consegue se colocar como detentor de poder dentro do sistema.

Atualmente, não existe um cenário de guerra cibernética declarado entre os Estados, contudo, são frequentes os ataques aos sistemas críticos dos estados, empresas e organizações, que criam uma sensação de medo, com ataques anônimos e de difícil atribuição de responsabilidade. Um exemplo prático disso, no Brasil, ocorreu quando o site WikiLeaks divulgou documentos oficiais na Agência de Espionagem Americana que revelaram que os Estados Unidos monitoravam as ações da então presidenta Dilma Rousseff junto aos seus assessores[3]. Ou seja, se trata de uma gama infinita de atores que disputam o poder dentro deste espaço, vazando e atacando até mesmo organizações estatais, enquanto Estados também se monitoram entre si. O que evidencia essa relação de interdependência cada vez mais complexa no SI. Demonstrando isso, o próximo capítulo discutirá os principais riscos, fragilidades e desafios de pensar nos próximos objetivos do *cyberpower* brasileiro.

3. A Estratégia Brasileira para o *Cyber*: Um Futuro de Desafios

No contexto internacional, várias correlações de forças atuaram para demonstrar a relevância da discussão acerca do *cyber* e da defesa cibernética, de forma a refletir inúmeros eventos governamentais globais a respeito do assunto, apontando uma preocupação mundial crescente acerca dos impactos destrutivos do uso do *cyber* para cometer crimes, espionar, realizar ações ativistas, apoiar o terrorismo ou até corroborar em atos de guerra.

Entre estas ações, podem-se destacar algumas que deram mais voz ao assunto dentro de diversos países, como por exemplo a ratificação pelo Estado brasileiro, em 2023[4], da Convenção de Budapeste, ocorrida em 2001[5], que propôs um tratado internacional sobre crimes perpetrados pela internet. Para mais, a publicação de estratégias nacionais de segurança cibernética que aconteceram na primeira década dos anos 2000 em diversos países da Europa como Estônia, 2005; Finlândia, 2008; Eslováquia, 2008; República Tcheca, 2011; França, 2011; Alemanha, 2011; Lituânia, 2011; Luxemburgo, 2011; Países Baixos, 2011; e Reino Unido, 2011; e também a criação, em 2009, do U.S. Cyber Command (USCyberComm) - órgão este subordinado ao Comando Estratégico estadunidense responsável pela coordenação de ações para a prevenção e defesa cibernética (Silva e Murakawa 2023).

Neste sentido, observa-se um movimento onde a pauta de segurança cibernética passa a tomar proporções internacionais e se torna um campo de interesse de todos os atores do SI, visto que todos eles passam de alguma maneira a dividir e também disputar esse campo. Ainda, é possível perceber a utilização de termos como *cyberwar*, ou Guerra Cibernética, já discutido brevemente na seção anterior. Contudo, diz respeito a uma categoria de análise que não se consolidou por não apresentar as mesmas características de uma "guerra" tradicional[6], mas que, na verdade, denomina outro tipo de conflito

3. Disponível em G1. Lista revela 29 integrantes do governo Dilma espionados pelos EUA. G1 Política, 6 jul. 2015. Disponível em: https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html. Acesso em: 19 nov. 2025.

4. Apesar de ter sido ratificada pelo Brasil apenas em 2023, a Convenção de Budapeste já estava em vigência desde 2004, quando atingiu 5 ratificações.

5. BRASIL. Decreto nº 11.491, de 4 de agosto de 2023. Disponível em: https://www.planalto.gov.br/ccivil$_{03}$/$_{Ato}$2023 − 2026/2023/*Decreto*/*D*11491.*htm*.*Acessoem* : 4*ago*.2024.

6. Para Waltz (2004), as causas mais importantes da guerra são a natureza e o comportamento do homem.

que envolve a tecnologia e o campo virtual e não necessariamente perpassa o campo terrestre. Em uma guerra tradicional, o conflito pode acontecer quando há invasão de um território por forças militares. Já em uma "guerra cibernética", o conflito acontece através de ataques orquestrados à rede de dados do oponente, além de ter objetivos diferentes de uma ocupação territorial, como a espionagem de dados, desestabilização ou vazamento de informações (Bernardes 2022). No entanto, vale considerar que, apesar de se tratar de uma ameaça virtual, ainda pode se desdobrar para uma ameaça física, materializada e não somente em uma esfera virtual (Marinho et al. 2022).

Nesse sentido, a guerra cibernética poderia ser comparada à guerra irregular, que é "uma forma de beligerância que transcende os estreitos limites do campo militar, destaca-se a atuação de forças predominantemente nativas e faz-se referência à guerra de guerrilhas, à subversão, à sabotagem e ao terrorismo" (Visacro 2009, p.265).

A partir dessa nova relação de forças estabelecidas através da inserção do espaço cibernético como eixo estratégico no cenário internacional, se propõe uma reflexão sobre como isso pauta o planejamento estratégico de defesa do Estado brasileiro, de forma a se discutir as principais decisões a partir daí e também a constituição de uma estratégia para a defesa cibernética do Brasil frente a um escalonado grau de risco que se insere no mundo através da inserção do *cyberspace*. No contexto doutrinário da defesa nacional, o espaço cibernético é composto de dispositivos computacionais, conectados em redes ou não, em que as informações digitais transitam e são processadas e/ou armazenadas (Ministério da Defesa 2014).

Em novembro de 2009, o Ministério da Defesa oficializou a atribuição da condução dos setores para cada uma das Forças. A distribuição foi: o Setor Espacial ficou a cargo da Força Aérea; o Setor Nuclear passou a ser conduzido pela Marinha do Brasil e o setor cibernético passou a ser gerido pelo Exército Brasileiro. A Diretriz Ministerial nº 0014/2009[7] – MD estabeleceu, ainda, que cada Força Singular elaborasse uma proposta de ações e diretrizes para cada setor (Brasil 2009). Deste modo, o Brasil incluiu o setor cibernético na Estratégia Nacional de Defesa, destacando-o como um dos setores de importância estratégica para a defesa do país (Santos 2021). Levando em consideração que se discutirão perspectivas da defesa cibernética a partir de uma ótica nacional, no âmbito do Ministério da Defesa, a definição constante da Doutrina Militar de Defesa Cibernética (MD31-M-07) estabelece defesa cibernética como sendo:

> "[...] um 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"(Ministério da Defesa 2014).

A Doutrina Militar de Defesa Cibernética, portanto, objetiva proporcionar uma unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD) e

As guerras resultam da estupidez e do egoísmo inerentes ao homem, as outras causas das guerras são secundárias e subordinadas a esses fatores.

7. Disponível em BRASIL. MD31-M-07: Defesa Cibernética. Brasília: Ministério da Defesa, 2013. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31$_M$07.*pdf* .*Acessoem* : 4*ago*.2024

contribuir para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético (Ministério da Defesa 2014). Isto posto, houve

> "[...] o estabelecimento do objetivo de criar um Sistema Militar para Defesa Cibernética, a introdução de defesa cibernética em exercícios das juntas militares e simulações de combate. Tal objetivo levou à criação do primeiro simulador de ataque cibernético no Brasil e à inserção de exercícios de defesa cibernética nas academias militares em todo o território nacional"(Lima, 2018 *apud* Santos 2021, p.27).

Desta maneira, o Simulador Nacional de Operações Cibernéticas (SIMOC) começou a ser operacionalizado no Centro de Instruções de Guerra Eletrônica (CIGE) em Brasília, com o objetivo de capacitar militares para a defesa do Brasil. Ademais, o Estado-Maior do Exército criou o Centro de Defesa Cibernética (CDCiber) em 2014 e estabeleceu as funções para os órgãos do setor cibernético. O CDCiber tem a missão de planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação dentro do Sistema Militar de Defesa Cibernética (SMDC). O objetivo é garantir o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra os interesses da Defesa Nacional (Santos 2021).

Assim sendo, o Sistema Militar de Defesa Cibernética (SMDC) foi construído em função de estabelecer as atribuições para os órgãos de estado e de governo vinculados à defesa nos diversos níveis de decisão. Em suma, estes níveis de decisão são:

> "a) Nível político – Segurança da Informação e Comunicações (SIC) 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; b) nível estratégico – Defesa Cibernética – a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF; e c) níveis operacional e tático – Guerra Cibernética – denominação restrita ao âmbito interno das FA"(BRASIL 2017, p.1-2).

Estas atribuições estão representadas na Figura 1 – enfatizando o papel de cada nível de decisão no processo.

Nesse sentido, destaca-se o Sistema de Guerra Cibernética do Exército (SGCEx) que trata de

> "[...] um conjunto de instalações, equipamentos, doutrinas, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de guerra cibernética, assegurando o seu uso efetivo pelo Exército Brasileiro, bem como impedindo ou dificultando a utilização do espaço cibernético pelo oponente. O SGCEx visa a proteção cibernética do Sistema de Comando e Controle do Exército, assegurando a capacidade de atuar em rede com segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da informação sob responsabilidade do Exército"(Kuhn 2022, p.22).

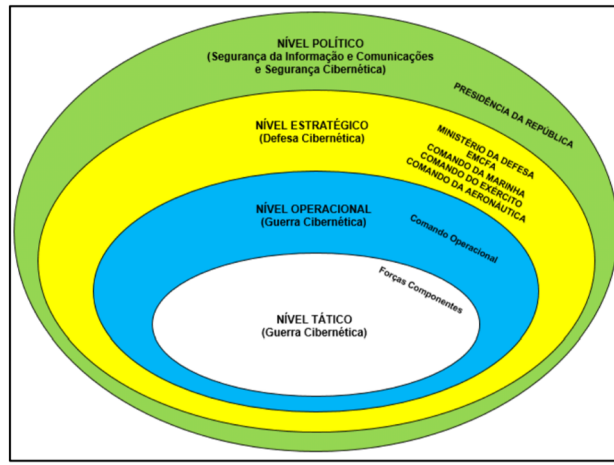

Figura 1. Níveis de Decisão

Fonte: BRASIL (2017, p.1-3).

Por conseguinte, a capacidade militar cibernética do Exército Brasileiro, desenvolvida no âmbito do SGCEx, é composta por três capacidades operativas: a proteção cibernética, o ataque cibernético e a exploração cibernética. A proteção visa neutralizar ataques e exploração cibernética contra os dispositivos computacionais nacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito e tem caráter permanente. O ataque visa interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente. Por fim, a exploração cibernética são buscas ou coletas nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados relevantes para as temáticas de defesa nacional (Marinho et al. 2022). Estas capacidades estão resumidas na Tabela 1.

A partir da compreensão da estratégia de Defesa Cibernética, é possível perceber que as principais limitações estão relacionadas à incapacidade ou à pouca capacidade de identificação de origem de ataques e atribuição de responsabilidades pelos ataques cibernéticos. Ademais, a eficácia restrita na defesa contra os ataques também limita as ações de defesa estratégica e expressa a vulnerabilidade dos sistemas computacionais. Também existe uma dificuldade no acompanhamento da evolução da tecnologia no campo cibernético, além da possibilidade de que, ao sofrer algum ataque, ainda sejam percebidas novas falhas que ainda não foram identificadas. No caso brasileiro, os desafios permeiam a segurança de dados de extrema confidencialidade que foram vazados em diferentes momentos da história.

Tabela 1. Capacidades do SGCEx.

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: BRASIL (2017, p.3-4).

> "O número de ataques cibernéticos tem crescido no Brasil desde 2001, tendo como alvos bancos, agências governamentais, organismos internacionais e partidos políticos. Devido à fragilidade na defesa deste espaço nacional, o país também tem sido alvo de espionagem de modo recorrente (...)"(Lima, 2018 *apud* Santos 2021, p.26).

Em 2011, o governo federal sofreu o seu maior ataque hacker já registrado até o momento, que foi reivindicado pelo grupo LulzSecBrazil[8]. O ataque impactou o funcionamento de diversos portais governamentais brasileiros, como o da Presidência da República, da Receita Federal e da Petrobras.

A Estratégia Nacional de Defesa foi incapaz de suprimir o ataque do grupo *Anonymous* às redes sociais da presidente Dilma Rousseff em 2013, ou até mesmo de ao menos identificar a espionagem realizada pela inteligência americana ao grampear os aparelhos de comunicação do Planalto - situação que foi conhecida apenas após o vazamento da relação de dados de espionagem no site da WikiLeaks.[9]

Desta forma, as limitações dizem respeito não somente à falta de produção tecnológica e produção expansiva de conhecimento científico na área dentro do país, mas também estão no cerne da infraestrutura, e até mesmo da falta de mão de obra totalmente qualificada para dar o suporte necessário na área de defesa cibernética dentro do território nacional.

A compreensão das estratégias brasileiras incide na percepção de como mesmo as

8. Disponível em G1. Ataque hacker foi o maior já sofrido por sites do governo na internet. G1 Tecnologia, 21 jun. 2011. Disponível em: https://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html. Acesso em: 4 ago. 2024.

9. Disponível em: WIKILEAKS. NSA Brazil. Disponível em: https://wikileaks.org/nsa-brazil/. Acesso em: 4 ago. 2024.

instituições ainda não se encontram plenamente preparadas para enfrentar o conflito no espaço cibernético. Apesar de uma "ágil" articulação a partir da organização das forças armadas para o cuidado deste espaço, vale levar em consideração que até antes disso não se tinha um grande movimento nacional consolidado em se preocupar com as questões do espaço cibernético.

4. Conclusão

O conflito no ciberespaço já é uma realidade. O que fazer a partir disso é uma das novas questões que se insere dentro da disciplina das Relações Internacionais, bem como um novo eixo de risco que preocupa não somente os Estados, mas também os setores privados e até mesmo a sociedade civil, que se percebe de forma mais vulnerável dentro desse processo.

Sendo uma questão que impacta todos os Estados no SI, percebe-se a relevância da discussão para a disciplina, ainda mais considerando que atravessa todas as camadas sociais e não se prende somente a uma divisão da conjuntura. Nesse caso, a conceituação de *cyberwar*, *cyberspace*, *cyberpower* e a discussão de uma estratégia para esse meio enriquecem e permitem avanços na área, primeiramente reconhecendo e percebendo as transformações que moldam a nova realidade global.

No caso do Brasil, foi possível averiguar que foram traçadas algumas estratégias para tentar compreender, explorar e até mesmo utilizar este espaço para as futuras estratégias. Nesse sentido, o Ministério da Defesa responsabilizou as Forças Armadas por cuidar do ciberespaço. Somente a partir deste momento, quando se explora e se iniciam as discussões desse meio, que se percebem as limitações nacionais no setor e os principais desafios para a área. Por isso, destaca-se a estratégia central das forças armadas no âmbito do SGCEx para o setor, deliberada em três eixos principais: a proteção cibernética, o ataque cibernético e a exploração cibernética. Ao estabelecer estes eixos como principais, é possível notar as limitações da estratégia – que estão principalmente ligadas à capacidade de identificação de origem dos ataques e o poder de resposta a eles dentro deste espaço.

Por fim, vale o questionamento: a nação brasileira, ao reconhecer essas limitações, já teria alcançado todas as proposituras objetivas na doutrina de defesa cibernética? Reconhecendo o cenário atual, é perceptível que não. Se faz necessário fomentar mais as discussões acerca das estratégias de defesa, e até mesmo apontar a necessidade de publicizar essa discussão para além da esfera militar, para assim poder dinamizar novas proposituras acerca do tema.

Recebido em: 19/01/2025.
Aprovado em: 06/10/2025.

Referências

Baxter, Pamela e Susan Jack. 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report* 13 (4): 544–559. https://doi.org/10.46743/2160-3715/2008.1573.

Bernardes, Amanda Rodrigues. 2022. (Im)possibilidades da guerra cibernética: análise do ato de guerra nas agressões cibernéticas. Dissertação (Mestrado), Escola de Comando e Estado-Maior do Exército. Acedido em 4 de agosto de 2024. https://bdex.eb.mil.br/jspui/bitstream/123456789/10367/1/MO%206544%20-%20AMANDA%20RODRIGUES%20BERNARDES.pdf.

Brasil. 2009. *Estratégia Nacional de Defesa: Decreto nº 6.703.* Decreto. Acedido em 26 de novembro de 2024. http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm.

BRASIL. 2017. *Manual de Campanha EB70-MC-10.232: Guerra Cibernética.* 1ª edição. Brasília: Exército Brasileiro. Acedido em 26 de novembro de 2024. https://bdex.eb.mil.br/jspui/bitstream/123456789/11912/1/EB70MC10232.pdf.

Galvão, Maria Cristiane Barbosa e Ivan Luiz Marques Ricarte. 2019. Revisão sistemática da literatura: conceituação, produção e publicação. *Logeion: Filosofia da Informação* 6 (1): 57–73. https://doi.org/10.21728/logeion.2019v6n1.p57-73.

Keohane, Robert O. e Joseph S. Nye. 2001. *Power and Interdependence: World Politics in Transition.* 3ª edição. Boston: Longman.

Kuhn, Leandro. 2022. A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha. Trabalho de Conclusão de Curso (Especialização em Ciências Militares), Escola de Comando e Estado-Maior do Exército. Acedido em 26 de novembro de 2024. https://bdex.eb.mil.br/jspui/bitstream/123456789/11872/1/MO%206699%20-%20Leandro%20KUHN.pdf.

Marinho, R. C., G. B. Pereira, H. de Q. Henriques e M. F. Neto. 2022. A defesa cibernética na proteção da propriedade intelectual dos produtos e sistemas de defesa do Exército Brasileiro. *Brazilian Journal of Development* 8 (1): 35–53. Acedido em 26 de novembro de 2024. https://doi.org/10.34117/bjdv8n1-003. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/42208.

Ministério da Defesa. 2014. *Doutrina Militar de Defesa Cibernética (MD31-M-08).* Brasília: Ministério da Defesa. https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf.

Nye, Joseph S. 2011. *The Future of Power.* 1ª edição. New York: PublicAffairs.

———. 2017. Soft power: the origins and political progress of a concept. *Palgrave Communications* 3:17008. https://doi.org/10.1057/palcomms.2017.8. https://doi.org/10.1057/palcomms.2017.8.

———. 2021. Soft power: the evolution of a concept. *Journal of Political Power,* https://doi.org/10.1080/2158379X.2021.1879572. https://doi.org/10.1080/2158379X.2021.1879572.

Pecequilo, Cristina Soreanu. 2012. *Introdução às Relações Internacionais: Temas, Atores e Visões.* 9ª edição. Petrópolis: Vozes.

Ruthfield, Scott. 1995. The Internet's History and Development: From Wartime Tool to Fish-Cam. *XRDS* 2 (1): 2–4. Acedido em 4 de agosto de 2024. https://doi.org/10.1145/332198.332202. https://doi.org/10.1145/332198.332202.

Saaida, Mohammed. 2024. Exploring the Dynamics of Complex Interdependence in International Relations. 1:1–7.

Santos, Marcel Deyvison Lima dos. 2021. O emprego da proteção cibernética para ampliar a segurança dos postos de comando da força terrestre componente. Trabalho de Conclusão de Curso (Especialização em Ciências Militares), Escola de Comando e Estado-Maior do Exército. Acedido em 4 de agosto de 2024. https://bdex.eb.mil.br/jspui/bitstream/123456789/10145/1/MO%206507%20-%20MARCEL%20Deyvison%20Lima%20dos%20Santos.pdf.

Sato, Eiiti. 2010. Cooperação internacional: uma componente essencial das relações internacionais. Acesso em: 13 jul. 2026, *Revista Eletrônica de Comunicação, Informação & Inovação em Saúde* 4 (1). https://doi.org/10.3395/reciis.v4i1.698. https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/698.

Sheldon, J. B. 2019. The Rise of Cyberpower. Em *Strategy in the Contemporary World,* 291–307. Oxford: Oxford University Press.

Silva, E. A. e F. M. Murakawa. 2023. Ciberguerra e cibersegurança: desafios para a segurança internacional na era digital. *Revista da Escola Superior de Guerra* (Rio de Janeiro) 38 (77): 185–209. Acedido em 4 de agosto de 2024. https://revista.esg.br/index.php/revistadaesg/article/download/1144/941/2235.

Visacro, Alessandro. 2009. *Guerra Irregular: Terrorismo, Guerrilha e Movimentos de Resistência ao Longo da História.* 1ª edição. São Paulo: Editora Contexto.

Waltz, Kenneth N. 2004. *O Homem, o Estado e a Guerra: uma análise teórica* [**inlang**português]. 331. São Paulo: Martins Fontes. ISBN: 85-336-1950-2.