ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

LEANDER RIBEIRO ARCIPRETE, Maj Av

Paralisia Estratégica: os possíveis efeitos dos ataques cibernéticos como alternativa de neutralização adversária

Rio de Janeiro
2022

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

LEANDER RIBEIRO ARCIPRETE, Maj Av

Paralisia Estratégica: os possíveis efeitos dos ataques cibernéticos como alternativa de neutralização adversária

Trabalho de Conclusão de Curso apresentado, como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior.
Linha de Pesquisa: Poder Aeroespacial.
Orientador: Evandro Carlos Baranzelli

Rio de Janeiro
2022

RESUMO

O presente trabalho aborda a Paralisia Estratégica, enfatizando, neste contexto, os possíveis efeitos dos ataques cibernéticos como alternativa de neutralização adversária, tendo em vista que a guerra cibernética tem capacidades suficientes para realizar grande parte das tarefas estratégicas que antes eram realizadas por meio do poder aéreo, naval, espacial ou terrestre, uma vez que o poder cibernético passa a ocupar o lugar predominante para derrotar um inimigo. Nesse contexto, para atingir o objetivo proposto, o qual consiste em verificar os possíveis efeitos da Paralisia Estratégica por meio dos ataques cibernéticos de modo a compreender em que medida a concepção desse modelo de guerra pode ser fundamental para proporcionar uma importante estratégia de paralisar os pontos vitais de um país, recorreu-se a uma pesquisa cujo percurso metodológico utilizado foi conduzido por meio de uma pesquisa bibliográfica subsidiada por abordagem qualitativa, coletada a partir de livros, artigos e periódicos pertinentes ao assunto, a partir dos quais se fez possível apresentar respostas à problemática levantada. Diante da pesquisa realizada, compreende-se que o ciberespaço tornou-se um campo de guerra em que as vulnerabilidades do inimigo são exploradas sem a necessidade de força; consequentemente, os Estados devem ter uma estratégia que forneça uma resposta oportuna e precisa às ameaças que enfrentam.

Palavras-chave: Paralisia Estratégica; Guerras Cibernéticas; Neutralização Adversária; Guerras Híbridas.

ABSTRACT

The present work deals with Strategic Paralysis, emphasizing, in this context, the possible effects of cyber attacks as an alternative for opposing neutralization, given that cyber warfare has sufficient capabilities to perform most of the strategic tasks that were previously carried out through power. air, naval, space or land, once the cybernetic power comes to occupy the predominant place to defeat an enemy. In this context, to achieve the proposed objective, which is to verify the possible effects of Strategic Paralysis through cyber attacks in order to understand to what extent the conception of this model of war can be fundamental to provide an important strategy to paralyze the points vital aspects of a country, we resorted to a research whose methodological course used was conducted through a bibliographic research subsidized by a qualitative approach, collected from books, articles and periodicals relevant to the subject, from which it was possible to present answers to the problem raised. In view of the research carried out, it was possible to understand that cyberspace has become a field of war where the vulnerabilities of the enemy are exploited without the need for force, consequently, States must have a strategy that provides a timely and accurate response to the threats they face.
Keywords: *Strategic Paralysis; Cyber Wars; Opposing Neutralization; Hybrid Wars.*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O século XXI é caracterizado por um ritmo vertiginoso de mudanças, assim como pela crescente interconexão e complexidade dos cenários, sendo necessária uma adaptação dos sistemas para poder enfrentar a evolução da realidade. Em meio a esse cenário, os conflitos entre forças armadas e a ação das Forças Armadas não poderiam ficar de fora, levando à compreensão de que o repensar contínuo, a informação e o conhecimento são considerados como prioridade; sobretudo quando se depara com a necessidade de projetar uma solução para um problema que põe em perigo não apenas vidas humanas, mas o próprio futuro de uma nação.

Nesse contexto, compreende-se que as estratégias militares precisam se adaptar a esse avanço tecnológico, possibilitando a modernização do modo de se fazer guerra, alinhadas às estratégias do poder cibernético, a fim de que o alcance dos seus objetivos sejam atingidos e causando, dessa forma, o menor efeito colateral possível.

Por meio de ataques cibernéticos, os Estados podem afetar ativos de informação de seus adversários. Além disso, podem afetar suas infraestruturas que, porventura, estejam ligadas à internet sem a devida proteção, o que pode comprometer a segurança dos núcleos de informações de um país, afetando, com isso, toda a sociedade.

Portanto, considerando a relevância da temática suscitada, o presente trabalho apresenta como problema de pesquisa o seguinte questionamento: Quais os possíveis efeitos da Paralisia Estratégica por meio dos ataques cibernéticos? Frente à problemática levantada, parte-se da hipótese de que a Paralisia Estratégica, no que concerne ao espaço cibernético, por sua particularidade, tende a causar grandes efeitos ao país atingido, haja vista que sua ação contribui para a geração de capacidades que aumentam o poder de agir decisivamente no campo de batalha, tanto de forma ostensiva quanto preventiva, causando efeitos estratégicos que, muitas vezes, extrapolam a esfera militar e se projetam para outros elementos do Estado, como, por exemplo, a infraestrutura nacional.

Ademais, esse modelo de Paralisia Estratégica pode causar uma grande pane no sistema governamental, haja vista que, atualmente, é notória a vulnerabilidade de um Estado devido à sua dependência tecnológica. Isso contribui para a obtenção de vantagens estratégicas, tal como dificultar ao oponente o direcionamento do comando de suas Forças Militares, possibilitando, assim, paralisar estrategicamente o sistema do adversário, atingindo, desse modo, a liderança do Estado e neutralizando as suas forças de forma ágil e automática.

Com base nas prerrogativas suscitadas, o objetivo geral desta pesquisa consiste em

verificar os possíveis efeitos da Paralisia Estratégica por meio dos ataques cibernéticos de modo a compreender em que medida a concepção desse modelo de guerra pode ser fundamental para proporcionar uma importante estratégia de paralisar os pontos vitais de um país, a saber: liderança, infraestrutura, população e forças armadas.

A fim de que fosse possível alcançar o objetivo geral desta pesquisa, alguns objetivos específicos foram traçados, tais como: Descrever os aspectos doutrinários e conceituais da Paralisia Estratégica em suas particularidades; analisar o emprego da Paralisia Estratégica por meio dos ataques cibernéticos ante a possíveis situações de guerras; e caracterizar os ambientes operacionais em que é desenvolvida a Paralisia Estratégica em um contexto cibernético.

A temática levantada se justifica por compreender que a adoção da Paralisia Estratégica no cenário contemporâneo busca o domínio das comunicações para um perfeito controle e neutralização de suas ações operacionais. Acredita-se que, quando o sistema de comunicação é severamente afetado, seus líderes não conseguem gerenciar de forma precisa seus esforços de guerra, dificultando, assim, as ações do Estado.

Dessa forma, entende-se que os ataques cibernéticos, enquanto ações de Paralisia Estratégica, representam estratégias viáveis e passíveis de serem utilizadas na prevenção de possíveis guerras sangrentas, tais como as que impactaram drasticamente a sociedade em outros tempos, haja vista que esse novo modelo de ataque está destinado a aniquilar, em um menor espaço de tempo, a capacidade do país oponente de prosseguir na guerra. Isso significa que é possível neutralizar a ação de seus adversários por meio do seu sistema de comunicação, controle e inteligência, causando a perda do moral de combate, culminando no sentimento de derrota e espírito de rendição por parte do país atingido.

2 REFERÊNCIAL TEÓRICO

2.1 A GUERRA NA ERA DA INFORMAÇÃO

Nos últimos anos, o uso do poder aéreo foi imerso em cenários cada vez mais complexos, nos quais o confronto com as ameaças estatais deu lugar a conflitos irregulares e híbridos, pondo à prova os conceitos doutrinários das guerras tradicionais. Da mesma forma, o ritmo acelerado do desenvolvimento tecnológico tem gerado novas capacidades, tornando imprescindível uma revisão contínua dos preceitos existentes na busca de sua adaptação, evolução e validação para serem aplicados em cenários do presente e futuro (DOUHET; WARDEN, 2003).

Nessa perspectiva, Gonçalves (2018) considera que o planejamento e desenvolvimento de meios de informação e técnicas para guerra constituem, hoje, o centro das estratégias militares, haja vista que processos da segurança pública nessa direção apontam para uma "Guerra de Informação Estratégica", ou seja, uma nova face da guerra, alinhada ao pensamento militar.

A partir dessa concepção, compreende-se que a informação não pode ser pensada como um meio auxiliar de estratégia de guerra, mas deve ser considerada o centro de toda a política de guerra e base de ação militar por meio das redes de comunicação, de modo a introduzir mudanças significativas nas condições culturais, econômicas, políticas, sociais e militares.

2.2 PARALISIA ESTRATÉGICA

Desde a China antiga, com Sun Tzu, existe uma corrente de pensamento que procurou fazer uso mais eficiente dos meios de guerra, tentando derrotar o oponente sem a necessidade do consequente desgaste e aniquilação no campo de batalha (TZU, 2016). Com o advento dos meios aéreos, novos pensadores adotaram o conceito, reforçando a ideia de que, se o instrumento militar fosse aplicado nos alvos corretos, o oponente estaria enfraquecido, desorganizado e incapaz de continuar a luta, sendo esta considerada a estratégia mais lucrativa, chegando, portanto, à concepção de Paralisia Estratégica (MATOS; SOUZA; PEREZINO, 2015).

De acordo com Souza (2016), a Paralisia Estratégica consiste na paralisação de qualquer atividade, funcionamento ou processo, sendo especialmente focada no processo de tomada de decisão, a qual, no contexto militar, tem a possibilidade de neutralizar um governo em comandar suas forças militares pela destruição do próprio centro governamental e de todo o sistema de comunicações, controle e inteligência do país atacado, levando a um colapso no funcionamento do país. A esse respeito, Carvalho (2020) reitera que:

> A Estratégia da Paralisia é uma opção militar com dimensões físicas e morais que tem a intenção de incapacitar, em vez de destruir o inimigo. Ela busca o máximo efeito ou benefício político, com o mínimo esforço militar ou custo. Tem por objetivo uma decisão militar rápida, dirigida contra a capacidade física ou mental que tem o adversário de manter ou controlar o seu esforço de guerra, para diminuir sua vontade moral de resistir (FADOK, 1995 *apud* CARVALHO, 2020, p.13).

Nesse contexto, compreende-se que a Paralisia Estratégica, intermediada por uma guerra cibernética, pode atuar de várias formas, tais como: na propagação de vírus em redes financeiras, em ataques a sistemas de distribuição de energia elétrica, ou na interceptação dos

sistemas de comunicação móvel.

Para Marcelino (2021), dominar o espectro da informação é tão crítico para o inimigo quanto o espaço ou a ocupação da terra, e controlar as informações representa a obtenção de uma grande vantagem sobre as forças adversárias.

2.3 GUERRA CIBERNÉTICA E CONFLITOS CIBERNÉTICOS

A ciberguerra pode ser entendida como uma agressão promovida por um Estado no intuito de prejudicar seriamente as habilidades de outro para forçá-lo à aceitação de um objetivo próprio ou, simplesmente, roubar informações e destruir seus sistemas de comunicação, alterar suas bases de dados, ou seja, o que normalmente entende-se como guerra, mas com a diferença de que os meios utilizados não seriam violência física, mas um ataque de computador que varia de "infiltração de sistemas de computador inimigos para obter informações ao controle de projéteis por meio de computadores, passando pelo planejamento de operações, e gerenciamento de suprimentos etc." (COLE, 2000).

No entanto, para aqueles que consideram que guerra cibernética e guerra de rede são a mesma coisa, deve-se salientar que a guerra cibernética é o uso de todas as ferramentas eletrônicas e tecnológicas da informação para derrubar os sistemas eletrônicos e de comunicação do inimigo e manter o seu próprio sistema operacional (SANTOS, 2021).

De qualquer forma, se houvesse a necessidade de listar as características de uma guerra cibernética, elas seriam: complexidade, assimetria, objetivos limitados, curta duração, menos danos para soldados, maior espaço de combate, menor densidade de tropas, paridade, intensa luta pela superioridade da informação, aumento da integração, aumento das exigências impostas aos comandantes, novos aspectos de concentração de forças, reação rápida e tão devastadora quanto uma guerra convencional (THOMAS, 2001).

Mas, de todas as supracitadas características, talvez a mais importante seja a da assimetria, porque a guerra cibernética fornece as ferramentas necessárias para os menores poderem enfrentar, até vencerem e provarem ser superiores ao maior, com alguns riscos mínimos para eles, precisando apenas de um computador e alguns conhecimentos avançados, fundamentos do computador. Ademais, os objetivos deste tipo de guerra são:

1. Danificar um sistema ou entidade, a ponto de não poder mais funcionar ou ser restaurado a uma condição utilizável sem ser completamente reconstruído;

2. Interromper ou romper o fluxo de informações;

3. Destruir fisicamente as informações do adversário;

4. Reduzir a eficácia ou eficiência dos sistemas de comunicação do adversário e suas capacidades de coleta de informações;

5. Impedir que o adversário acesse e use sistemas e serviços críticos;

6. Enganar os oponentes;

7. Obter acesso aos sistemas inimigos e roubar suas informações;

8. Proteger seus sistemas e restaurar os sistemas comprometidos;

9. Responder rapidamente a ataques ou invasões do adversário.

Diante disso, é necessário compreender que, conforme Barros, Gomes e Freitas (2011) apresentam, existem três tipos de guerras cibernéticas:

1. Guerra de informações pessoais: área relacionada a questões e segurança bem como à privacidade dos dados e ao acesso às redes de informação.

2. Informações de nível corporativo/organizacional: área de espionagem clássica entre organizações em diferentes níveis (da empresa ao Estado) ou no mesmo nível.

3. Guerra de informações de escopo aberto/global: área relacionada às questões do ciberterrorismo em todos os níveis, tais como: ataques realizados a partir de computadores para centros de tecnologia; propaganda como forma de enviar mensagens e promover os danos causados por seus ataques; e/ou planejamentoe logística de ataques tradicionais, biológicos ou tecnológicos.

Na atual conjuntura, os guerreiros do ciberespaço são consultores e engenheiros equipados com arsenais informáticos alheios à imagem convencional das armas, e os encarregados por combater os vilões no cenário de guerra virtual, usando microfones e fones de ouvido nos laptops, sensores etc. Seus procedimentos são bastante semelhantes aos dos *hackers*, embora seus objetivos sejam, quase sempre, completamente diferentes (NETO, 2017).

De acordo com Neto (2017), a primeira coisa que qualquer *hacker* faz é visitar ou pesquisar alguns dos sites nos quais existem scripts para verificar o site que deseja violar, a fim de determinar qual deles é sua arquitetura tecnológica básica. Esses scripts consultam o servidor do site para determinar qual sistema operacional e tipo de software são usados. Posteriormente vem a parte mais difícil: encontrar "buracos" ou falhas na versão específica do software desse site, pois ele pode fornecer as "entradas" que permitem quebrar seu código. As informações sobre falhas de software imediatamente passam a ser de conhecimento público dentro da comunidade *hacker*. Obviamente, quando se trata de cibersoldados, as informações obtidas não são divulgadas. Assim, uma vez que um hacker encontra um buraco, penetrar no sistema é apenas uma questão de persistência, embora a grande maioria das tentativas termine em fracasso.

2.4 ESTADOS SE PREPARAM PARA GUERRA CIBERNÉTICA

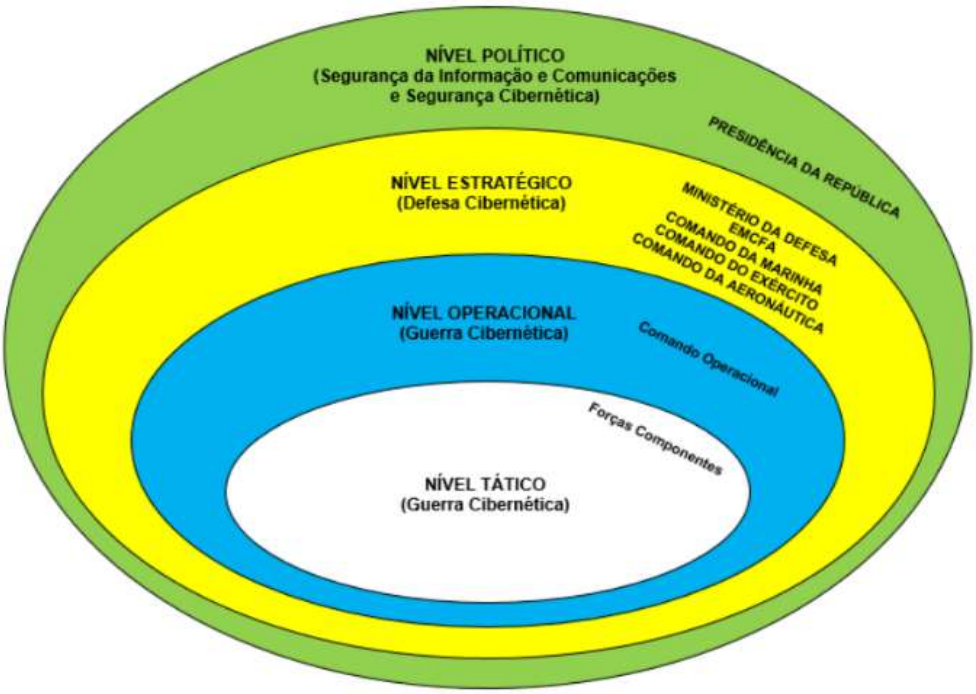
Em um mundo tão hiperconectado e hipercomputadorizado como o atual, qualquer impacto no coração das redes de informação e tecnologia pode gerar perdas milionárias para qualquer país ou instituição, sem falar nos fortes efeitos psicológicos que poderiam ser causados por um ataque com essas características (SANTOS, 2021).

Além disso, ainda de acordo com Santos (2021), as ameaças podem vir de qualquer lugar ou pessoa, sendo algo relativamente barato, difícil de contrabandear, difícil de associar etc. Nesse sentido, não se trata mais de *hackers* que, de forma esportiva, tratam de descobrir falhas em sistemas de segurança, ou de *crackers,* que, com uma mente niilista, parecem gostar de destruição, mas ações destinadas a paralisar capacidades militares ou serviços públicos de um governo inimigo (SANTOS, 2021).

Por isso, já existem muitos Estados, principalmente os mais desenvolvidos, que lançaram programas para encontrar e, se necessário, atacar as deficiências nos sistemas informáticos dos seus adversários, ao mesmo tempo em que aprovaram medidas para proteger seu ciberespaço e minimizar os efeitos e danos de ataques cibernéticos. Portanto, eles criaram escritórios do governo, controle, ou exércitos de cibersoldados.

No que concerne aos desdobramentos da política externa brasileira, segundo Pereira (2021), a Doutrina Militar de Defesa Cibernética estabelece seus fundamentos básicos a partir de competências distintas a cada setor do poder público, de modo que o Ministério da Defesa seja o setor responsável pela Defesa Cibernética, e a Presidência da República seja responsável pela Segurança Cibernética (BRASIL, 2014). Dessa forma, as ações realizadas no contexto cibernético serão estabelecidas a partir de quatro níveis: político, estratégico, operacional e tático, conforme mostrado na Figura 1:

Figura 1 — Níveis de ações no espaço cibernético



Fonte: Pereira (2021)

Conforme a ilustração mostra, o nível político, de responsabilidade da Presidência da República, compete à segurança da informação e comunicaçãoes e à segurança cibernética. O nível estratégico, a quem compete a Defesa Cibernética, possui em seu entorno o Ministério da Defesa, e os comandos da marinha, do exército e da aeronáutica. Os níveis operacional e tático, por sua vez, são os que atuam diretamente na guerra cibernética a partir do seu comando operacional e forças componentes, consecutivamente (PEREIRA, 2021).

2.5 ATAQUES CIBERNÉTICOS X GUERRA CIBERNÉTICA

Até o presente momento, não houve nenhum ataque que permita ser chamado de ciberguerra em si, uma vez que não foi registrado nenhum que tenha afetado instalações ou órgãos públicos, usinas nucleares, sistemas de transporte, infraestruturas nacionais etc., de algum país, causando danos e perdas incalculáveis.

Contudo, é verdade que ataques diários ocorrem em sistemas operacionais de diferentes órgãos ou instituições, mas, de acordo com Santos (2021), são mais sobre ações de *hackers*, que tendem normalmente interromper serviços não essenciais, causar algum dano aos sistemas operacionais de empresas, organizações etc., ou roubar algum tipo de informação ou segredo, mas sem gerar os efeitos atribuídos a qualquer tipo de guerra. Os exemplos a seguir apresentam

alguns dos milhares de ataques cibernéticos que foram produzidos nos últimos anos:

- *Década de 1990*

A Guerra do Golfo é tradicionalmente considerada o início da era da informação de guerra. Nela, aviões armados com munições de precisão atacaram a rede de telefonia, comunicações e energia elétrica em Bagdá, com especial crueldade contra os centros cientistas da computação da polícia secreta iraquiana (SILVA, 2020).

- *Anos 2000*

A cidade de Nova York foi lançada no caos com o resultado do maior apagão que passou na história dos Estados Unidos, o qual afetou quase toda a região nordeste do país, além do Canadá. Um apagão de trinta e quatro minutos no sul de Londres interrompeu a rede de metrô da cidade e o sistema ferroviário no sul da Inglaterra, afetando meio milhão de pessoas e a maioria dos serviços no centro da capital britânica. Ademais, 60% das estações do metrô tiveram que fechar, principalmente na zona sul da cidade. Além disso, apagaram-se mais de 270 semáforos e, embora essa avaria tenha sido corrigida após 34 minutos, houve um grande caos nas ruas afetadas (REUTERS, 2003).

É importante ressaltar que, conforme destacado em Palestra do Comando de Defesa Cibernética realizada em 2018, em meio às atividades articuladas pelo Ministério da Defesa com vistas a possíveis confrontos cibernéticos no ano de 2014, o referido Ministério implantou o Comando de Defesa Cibernética (ComDCiber), sendo este mais um instrumento integrante das Forças Armadas, bem como a Escola Nacional de Defesa Cibernética (ENaDCiber), voltada à capacitação dos oficiais das Forças Armadas a fim de que possam desenvolver suas capacidades de defesa no contexto cibernético de forma mais eficaz, conforme Figura 2.

Figura 2 — Organização do Exército Brasileiro no setor cibernético nacional

Fonte: Abdalla (2020)

No entanto, diante da crescente importância do setor cibernético nos mais variados cenários organizacionais, dentre os quais se enquadram as Forças Armadas, no ano de 2017, o Exército Brasileiro transformou o Projeto de Defesa Cibernética em Programa Estratégico do Exército, no intuito de favorecer o desenvolvimento estrutural e sua capacidade de ação frente a possíveis eventos de natureza cibernética, conforme mostrado na Figura 3.

Figura 3: Organizações Militares do Exército envolvidas no Projeto Estratégico de Defesa Cibernética

Fonte: Abdalla (2020)

Conforme evidenciado por Abdalla (2020), verifica-se que, para o desenvolvimento de atividades no domínio operacional cibernético, o Centro de Defesa Cibernética não se limitou

apenas a atividades operacionais no ciberespaço, mas viabilizou a necessidade de capacitar seus oficiais de modo que estejam preparados para atuar de forma eficiente, diante de possíveis ataques cibernéticos, ou mesmo quanto à exploração da rede adversária, com vistas a proteção e salvaguarda dos ativos de sua nação.

3 METODOLOGIA

Para o desenvolvimento deste trabalho, o percurso metodológico utilizado foi conduzido por meio de estudo bibliográfico e documental, a partir de uma abordagem qualitativa, descritiva e não experimental, subsidiada pela Taxonomia de Bloom (FERRAZ; BELHOT, 2010).

Os dados foram coletados por meio da busca nas bases de dados do Google Acadêmico e periódicos da CAPES, a partir das palavras-chave: Paralisia Estratégica, guerras cibernéticas e guerras híbridas, as quais serviram como embasamento para o desenvolvimento deste trabalho.

Como critérios de inclusão, foram utilizados artigos com texto disponível na íntegra, em português, inglês e espanhol, publicados nos últimos 10 (dez) anos, que tratassem claramente da Paralisia Estratégica, enfatizando os possíveis efeitos dos ataques cibernéticos como alternativa de neutralização adversária. Foram excluídos os artigos incompletos, não gratuitos, com restrição de acesso e os que não atenderam aos critérios de inclusão delineados.

Para a coleta de dados, no primeiro momento foi realizado um levantamento bibliográfico referente à Paralisia Estratégica em suas particularidades, bem como sobre os possíveis efeitos dos ataques cibernéticos como alternativa de neutralização adversária. E, no segundo momento, foram levados em consideração os objetivos específicos do estudo.

Para a análise dos dados coletados, esta pesquisa utilizou a técnica da análise de conteúdo. Seguiram-se três etapas: a pré-análise, quando foi realizada a organização e leitura do material; a exploração do material, e, na terceira etapa, o tratamento dos resultados, interpretação e categorização dos conteúdos.

Finalmente, foram respeitados os princípios éticos, mantendo a fidedignidade das ideias e conceitos expressos pelos autores, inclusive as referências, conforme as obras analisadas, respeitando a NBR 6023 da Associação Brasileira de Normas Técnicas.

4 RESULTADOS E DISCUSSÃO

4.1 CARACTERÍSTICAS BÉLICAS DO CIBERESPAÇO

A antiga ciência militar conceitua o campo de batalha como o espaço geográfico onde ocorrem as batalhas, por isso era de suma importância escolhê-lo e usá-lo com sabedoria. Isso foi praticado em todos os conflitos durante os séculos XVII, XVIII e XIX, nos quais a guerra posicional era vista como o meio para a vitória. No entanto, os avanços tecnológicos trouxeram novas arenas em que as batalhas são travadas.

Embora devido ao desenvolvimento tecnológico alcançado até meados do século XX, o campo onde as batalhas foram travadas fosse entendido apenas como o espaço geográfico/material dentro ou fora da atmosfera terrestre, agora fala-se de um ciberespaço que não é tocado, mas é sentido. Consequentemente, o campo de batalha cibernético pode ser interpretado como o espaço virtual no qual ocorrem um ou mais combates entre dois oponentes (NYE JUNIOR, 2012).

Ao longo do tempo, o ciberespaço cresceu em importância dentro das estratégias de segurança nacional dos Estados que dependem cada vez mais da interação com a rede para suas atividades, não apenas comerciais, acadêmicas, financeiras, mas também de defesa e ataque. Por isso, o toque final à discussão internacional sobre a conceituação bélica do ciberespaço foi dado pelo ex-secretário de Defesa dos Estados Unidos, William J. Lynn III (2010, p.3), que definiu o ciberespaço como o "quinto domínio da guerra".

Com isso, as diferenças foram derrubadas, aceitou-se que há uma competição acirrada entre os Estados neste campo bélico desde o final do século XX e os Estados tecnologicamente dependentes focados em fortalecer seus meios de segurança cibernética. Da mesma forma, para aqueles Estados que não haviam considerado a fragilidade dos sistemas digitais de comando e controle de suas instalações vitais, essa declaração significou o início de um plano para desenvolver uma estratégia de defesa e obtenção de vantagens nesse cenário de guerra virtual (CLARKE; KNAKE, 2015).

Da mesma forma, com base nas declarações de Lynn, a sociedade internacional assumiu a tarefa de estabelecer uma regulamentação para as atividades que são realizadas tanto no ciberespaço quanto na Internet e que podem dar origem a conflitos cibernéticos.

A história da guerra indica que a influência dos desenvolvimentos tecnológicos aplicados às armas gerou grandes mudanças nas estratégias e táticas de guerra. A chegada dos computadores como centros de controle e sua posterior interligação por meio da rede é um

fenômeno que atrai a cada dia a atenção dos exércitos para atingir seus objetivos minimizando os riscos. De fato, a popularidade da rede de redes e a dependência que esta ferramenta de comunicação criou tornaram-se o meio ideal para testar a eficácia das armas digitais.

4.2 CARACTERIZAÇÃO DE ARMA CIBERNÉTICA

Existe atualmente um debate sobre o que se entende por uma arma cibernética; especialmente porque os poderes da China e da Rússia, por exemplo, não chegaram a um consenso sobre essa questão (RID; MCBURNEY, 2012). No mesmo teor de ideias, Tomas Rid e Peter McBurney (2012) compreendem que é difícil definir armas cibernéticas porque constituem uma nova forma de causar danos. No entanto, como uma arma é qualquer coisa que seja usada para causar danos (RID; MCBURNEY, 2012), e foram documentados casos em que ataques virtuais foram realizados usando a informação e o espectro eletromagnético como instrumento e meio de guerra, respectivamente, pode-se falar de armas cibernéticas.

Vale lembrar que as armas digitais são projetadas para causar danos materiais e físicos através do espectro eletromagnético e da internet, independentemente de o dano paralisar uma cidade, uma vila, uma organização ou a vida de um indivíduo. Para Peter Lorents e Rain Ottis (2010), armas cibernéticas podem ser compreendidas como uma tecnologia de informação baseada em sistemas da mesma ordem (software, hardware e meios de comunicação) que foram projetadas para prejudicar e danificar a estrutura e a operação de algum outro sistema. Sendo assim, essa amplitude da definição permite o estabelecimento de várias classificações para armas tecnológicas que ameaçam a segurança cibernética dos Estados.

É pertinente esclarecer que não há consenso sobre a melhor forma de definir uma arma cibernética. Portanto, quando adaptado para expressar o que poderia ser definido como uma arma cibernética, caracteriza-se como instrumento, meio ou máquina destinada a atacar ou defender-se em qualquer área (material ou virtual) do conflito (ROSA, 2015). Definição que também permitiria usar a classificação tradicional entre armas convencionais e armas de destruição em massa fornecida pelo Escritório das Nações Unidas para Assuntos de Desarmamento, em janeiro de 2022, para enquadrar os instrumentos de ciberataque e ciberdefesa como arma convencional; todavia, vale lembrar que, frente aos avanços tecnológicos e consequentemente do impacto dos ciberataques, os instrumentos tecnológicos utilizados em ciberataques pode resultar em impactos de destruição em massa (UNODA, 2022). Sua habilidade e velocidade de transformação de uma arma não letal para uma arma

letal é precisamente o que atrai os estudiosos da segurança nacional (CLARKE; KNAKE, 2015).

As armas cibernéticas podem ser classificadas de acordo com seu escopo, método de implantação e finalidade. Entre os mais importantes estão: vírus, *worms*, programas maliciosos, bombas lógicas, *botnets*, *spyware*, *backdoors* e cavalos de Troia. Abaixo foi incuída uma breve descrição de algumas das armas cibernéticas mencionadas, com base na informação apresentada pela empresa de cibersegurança Panda Security (online - data desconhecida).

Vírus: programas de várias características que são introduzidas nos computadores através de e-mail, USB, internet etc. Eles se caracterizam por se reproduzir infectando outros arquivos ou programas e realizando ações irritantes ou prejudiciais para o usuário. Seu nome se deve à sua enorme semelhança com vírus humanos. Eles podem ser chamados de microprogramas.

***Worms*:** semelhantes aos vírus, porque são autorreplicantes e prejudiciais, mas se diferem por não precisarem de outros arquivos para serem reproduzidos. Eles se reproduzem sem danificar outro arquivo, mas muito rapidamente, o que colapsa as redes. Eles geralmente são espalhados por e-mail.

Programas maliciosos (*malware*): envolvem tanto a perda de dados quanto a perda de produtividade. Os programas incluídos incluem: discador, piada, risco de segurança, ferramenta de *hack*, vulnerabilidade, *spyware*, *oax* e *spam*.

***Trojans*:** diferem dos vírus porque não se reproduzem infectando outros arquivos, nem se espalham fazendo uma cópia de si mesmos. Eles emulam os astutos gregos da mitologia e chegam ao computador como um programa aparentemente inofensivo, porém, quando executado, aparece sua segunda arma, o *Trojan*. Eles podem ser extremamente perigosos, realizando ações como capturar textos digitados pelo teclado ou registrar senhas.

***Backdoor*:** um programa que entra no computador de forma encoberta, aparentando ser inofensivo. Uma vez executado, ele estabelece uma "porta dos fundos" por meio da qual o computador pode ser controlado. Além disso, ele permite realizar ações que comprometam as informações ou atrapalhem o trabalho do usuário. Pode dar acesso a todas as informações, excluir arquivos, destruir informações, encaminhar dados confidenciais para uma estação externa ou abrir portas de comunicação (PANDA SECURITY, data desconhecida).

A essas armas devem ser adicionadas as armas cibernéticas que têm a capacidade de aprender com o ambiente e são modificadas de acordo com as condições em que são desenvolvidas; as chamadas "armas de aprendizagem" (armas que aprendem). É importante esclarecer que sua consideração como armas cibernéticas é resultado do fato de que tais

programas ou códigos maliciosos em determinados contextos podem sabotar e danificar tanto sujeitos quanto objetos. Portanto, uma vez que conseguem atacar a segurança cibernética de instituições e indivíduos e até mesmo causar sua destruição ou morte, tornam-se um instrumento de guerra muito útil no ciberespaço (NYE JUNIOR, 2012).

Nesse sentido, como temos visto neste trabalho, a diversidade de maneiras de obter o controle da infraestrutura crítica de uma nação torna as armas cibernéticas o meio ideal de quebrar a vontade do inimigo sem lutar. Isso seria alcançado se um Estado não tomasse as medidas políticas, econômicas, sociais e militares para garantir a segurança cibernética. Dessa forma, como abordado por Geers (2011), não antecipando que um Estado pode entrar em uma paralisia ao perder o controle de suas usinas nucleares, seus sistemas de controle de tráfego aéreo, das corretoras e do sistema financeiro, do patrimônio estratégico e secreto à informação dos planos nacionais tornam-se uma vulnerabilidade que pode ser explorada por potenciais inimigos com grande facilidade e grande impacto no poder de resposta.

4.3 PRINCIPAIS MEIOS PARA REALIZAR OS ATAQUES CIBERNÉTICOS

As armas cibernéticas são utilizadas para realizar diversos ataques cibernéticos, os quais são entendidos como: atos deliberados lançados por meio do ciberespaço para manipular, destruir, negar, degradar ou destruir computadores ou suas redes, e/ou as informações neles encontradas, que geram danos no ciberespaço ou no mundo material de modo a comprometer a segurança nacional de um Estado (SHAKARIAN, 2013). Por isso, os ciberataques tornaram-se uma prioridade para os sistemas de defesa dos Estados.

Os ataques cibernéticos em todo o mundo são realizados usando uma variedade de táticas e armas cibernéticas. De acordo com o *Internet Security Threat Report*, entre as principais ameaças à segurança de Estados, organizações e indivíduos estão: ciberespionagem, infecções por vírus, roubo de informações, ataques contra a segurança das indústrias, interceptação de comunicações com *backdoors* e ataques de reconhecimento (BROADCOM, 2014).

Os ataques cibernéticos visam a espionagem, danos financeiros e manipulação de infraestrutura nacional crítica. Seu impacto é suficiente para influenciar o curso dos conflitos entre governos, entre cidadãos e entre si (ROSA, 2015). Consequentemente, os ataques podem ser classificados de acordo com os atores dos ataques, como patrocinados pelos Estados ou realizados por atores da sociedade civil, coletiva ou individualmente.

Nesse contexto, os meios utilizados como instrumentos de ataque cibernético visam paralisar a vida de uma nação conectada à rede. Isso significa que, por meio da introdução de vírus informáticos, as informações que circulam pelas redes estabelecidas em todo o mundo podem ser anuladas total ou parcialmente.

De acordo com o documento apresentado pela ONU (2013 *apud* LIN, 2012), existem ciberataques que vão desde a desfiguração de sites, passando por negação de serviços até o roubo de informações e infiltração de redes de computadores e servidores. Por isso, Lin (2012, p.64) alerta que: "Os ataques cibernéticos têm o objetivo de impedir que usuários acessem serviços ou interrompam máquinas controladas por computadores, enquanto a exploração cibernética é feita para penetrar nos computadores para obter informações".

Ademais, é claro que os ataques cibernéticos visam buscar ou destruir informações, controlar máquinas e negar acesso a serviços, o que facilmente desestabiliza as atividades de uma nação dependente da rede. Os ataques cibernéticos têm como objetivo, entre muitas outras coisas: primeiro, explorar o poder e o alcance da internet; segundo, explorar sua vulnerabilidade; terceiro, os invasores cibernéticos se beneficiam do anonimato; e quarto, mesmo Estados-nação podem ser considerados como alvos (KEIZER, 2009).

Assim, dentre as características que tornam os ataques cibernéticos um meio eficaz de ataque à segurança dos Estados, encontram-se as seguintes:

a) Barato - os meios de ataque podem ser adquiridos online, a baixo custo ou até gratuitamente;

b) Simples - um invasor com habilidades básicas de tecnologia da informação pode realizar o ataque;

c) Eficaz - mesmo os menores ataques podem causar grandes danos.

4.3.1 AMEAÇAS DIGITAIS CONTRA A SEGURANÇA NACIONAL DOS ESTADOS

A natureza das ameaças é determinada por suas motivações e intenções. Por isso, segundo o *Global Internet Security Threat Report,* publicado em abril de 2009, ciberespionagem, ciberoperações militares, ciberterrorismo e cibercrime podem ser citados como as principais ameaças à segurança dos Estados (CLARKE; KNAKE, 2015).

Essa classificação de ameaças resume-se a basicamente outros dois tipos de ameaças, a espionagem cibernética e as operações cibernéticas militares: uma com dupla utilização entre os Estados e grupos terroristas (ciberterrorismo), e outra que poderia ser colocadacomo exclusivamente de autoria total de grupos criminosos (cibercrime). Essa tendência de ameaça continuou ao longo da segunda década do século XXI; por exemplo, o *Internet Security Threat*

Report volta a referir a ciberespionagem como uma das principais ameaças à segurança da Internet, o que confirma que este flagelo é um dos inimigos a ser vencido pelas forças de segurança (BROADCOM, 2014).

Sem medo de errar e como resultado da análise da tendência de conflitos no século XXI, o ciberespaço estará presente em qualquer guerra (mesmo antes do início do combate); uma vez que é usado como meio de lançamento de armas cibernéticas militares, mas, em tempos de paz e durante o conflito, pode ser usado para espionagem cibernética, que se torna uma tática para obter informações estratégicas do inimigo (NYE JUNIOR, 2012). Por isso, os Estados devem reagir com ações que garantam a segurança cibernética com uma estratégia de guerra cibernética.

4.4 CIBERGUERRA ENQUANTO CONCEITO INACABADO

A estruturação de conceitos sólidos e universais para os diferentes fenômenos que ameaçam a segurança internacional é uma obrigação de todos os atores do sistema internacional. No entanto, a chegada de novos conceitos que são, por uma razão ou outra, popularizados traz consigo um uso que não segue regras e gera mais confusão do que certeza. É o caso do termo "ciberguerra", que designa vagamente algum tipo de ataque ou retaliação, invasão ilegal de uma rede de computadores ou ato de espionagem cibernética. O anterior pode ser parte de uma estratégia ou conflito político/militar para derrubar a cibersegurança de um Estado, reduzindo as capacidades de defesa e ataque de um ator internacional no ciberespaço, ao mesmo tempo em que se realiza um ataque direto com forças materiais.

Isso fez com que a guerra cibernética fosse considerada guerra de informação, guerra de rede ou guerra digital e confundida com guerra eletrônica (SHAKARIAN, 2013). Ademais, fez com que o ciberespaço se tornasse o calcanhar de Aquiles dos sistemas cibernéticos, especialmente quando as Forças Armadas, bem como os governos e as economias que protegem dependem cada vez mais das tecnologias da informação. Um exemplo disso é o que Orton (2009) indicou sobre a Força Aérea dos EUA: "Em 2010, a Força Aérea dos Estados Unidos adquirirá mais aeronaves não tripuladas do que tripuladas pela primeira vez" (ORTON, 2009, p.71).

4.4.1 CARACTERÍSTICAS DA GUERRA CIBERNÉTICA

Para explicar o fenômeno da ciberguerra, seria necessário retornar às causas e motivações da guerra apresentadas por Stephen Van Evera (1999) em seu livro "Causas da

Guerra: poder e raízes do conflito". As causas, segundo Van Evera, podem ser classificadas em cinco grupos principais de hipóteses: a guerra é mais provável quando há controle de recursos; quando o poder dos estados flutua repentinamente; a conquista é fácil; quando a vantagem está com o primeiro lado; e, finalmente, quando os Estados são vítimas de um falso otimismo. Todas essas causas são movidas por duas motivações principais: a busca pelo próprio poder e o medo do poder dos outros.

A diferença entre motivações e causas está no fato de que as motivações fazem parte da natureza humana, ou seja, são passionais e nada racionais; enquanto as causas são elementos racionais que se encontram no preâmbulo da guerra e levam a ela. No entanto, ambos têm o objetivo final de manter ou aumentar o controle e a influência sobre os outros. Isso nos mostra o que Thomas Hobbes disse sobre o poder: "existe como inclinação geral de toda a humanidade um desejo perpétuo e incansável de poder e mais poder que só cessa com a morte" (HOBBES, 1651, p. 01).

Essa busca incansável pelo poder é um fator-chave para o surgimento de conflitos entre Estados, que usariam todos os meios e áreas de guerra à sua disposição para quebrar a vontade de luta de seu oponente, incluindo a guerra cibernética. Para compreender esse último preceito, é necessário partir do conceito estabelecido para a guerra do ponto de vista de Karl Von Clausewitz (2015) que, em sua obra-prima *Da Guerra*, define a guerra como:

> A guerra nada mais é do que um duelo em maior escala. Se quiséssemos conceber os inúmeros duelos residuais que o compõem como uma unidade, poderíamos representá-lo para nós mesmos como dois lutadores, cada um tentando impor sua vontade ao outro por meio da força física [...] (CLAUSEWITZ, 2015, p.1).

A citação de Karl Von Clausewitz estabelece claramente que existem dois adversários, com força ou capacidade suficientes para enfrentar o outro (muito embora nem sempre essas forças ou capacidades sejam simétricas às forças oponentes), cujo objetivo é impor sua própria vontade, usando todos os meios disponíveis para o efeito. Na verdade, ele nunca menciona que daria exclusivamente por meio das Forças Armadas.

Com base no exposto, podemos afirmar que os líderes de opinião e doutrina são os países com maior desenvolvimento no campo da cibersegurança, pois determinam e constroem os conceitos a serem utilizados pelo resto do mundo. Assim, estudar esses Estados ou formadores de opinião nos permite estabelecer parâmetros de comparação e crítica. Por isso, é pertinente ressaltar o que é definido como guerra cibernética, de acordo com o Departamento de Estado dos EUA (CARTWRIGHT, 2010):

> Cyber Warefare (CW) ou Guerra cibernética (CG): Um conflito armado conduzido no todo ou em parte por meios cibernéticos. Operações militares conduzidas para negar a uma força oposta o uso efetivo de sistemas e armas do ciberespaço em um

> conflito. Isso inclui ações de ciberataque, ciberdefesa e ciberhabilitação (CARTWRIGHT, 2010, p.7. Tradução nossa).

Na mesma linha, segundo Jeffrey Carr, o conceito de guerra cibernética que foi moldado pelo Departamento de Defesa dos EUA é: "A Guerra Cibernética é a arte e a ciência de lutar sem lutar; de derrotar um oponente sem derramar seu sangue..." (CARR, 2011, p. 2). Pode-se perceber, então, que tal definição retoma as ideias apresentadas por Sun Tzu (2016) em sua obra *A Arte da Guerra*, quando se refere aos atos estratégicos de um Estado em tempos de guerra.

Em contraste, o autor Jeffrey Carr, em seu livro *Inside Cyber Warfare*: *Mapping the Cyber Underworld*, indica que os militares classificam erroneamente atos internacionais de conflito cibernético como guerra cibernética. Nas palavras do autor:

> [...] atos internacionais de conflito cibernético (comumente referido erroneamente como guerra cibernética) estão intrinsecamente entrelaçados com crimes cibernéticos, segurança cibernética, terrorismo cibernético e espionagem cibernética (CARR, 2011, p. 13).

Dessa forma, compreende-se que a guerra cibernética refere-se ao uso de capacidades baseadas na rede de um Estado para interromper, negar, degradar, manipular ou destruir informações residentes em computadores e redes de computadores, ou os próprios computadores e os redes de outro Estado. Entretanto, vale ressaltar que os objetivos da guerra cibernética são: informação em redes de computadores, computadores, sistemas acessórios e, por fim, toda a infraestrutura de informação e comunicação do inimigo (CARR, 2011).

Definições em que ciberataques, redes de computadores, sistemas de controle e comunicação têm os Estados como atores, fazendo parte de um conflito armado no qual pode ou não haver derramamento de sangue podem ser encontradas como elementos comuns. Ao refletir sobre o fato de as considerações serem diferentes e/ou não existir uma definição internacional única, pode-se concluir o seguinte:

a) A guerra cibernética confunde-se com atos ilícitos de vários tipos realizados por agentes não estatais;

b) Atos que violem a cibersegurança podem ser usados como cobertura perfeita para os atos de guerra de um Estado;

c) A guerra cibernética é o conjunto de atos praticados exclusivamente pelas forças de um Estado para dominar ou prejudicar um terceiro.

Assim, compreende-se que o impacto alcançado pelos ataques cibernéticos, bem como os autores de tais atos, determinam se um ataque à segurança cibernética é um ato de guerra cibernética. No entanto, a condição de anonimato dos atacantes é a principal barreira para identificar com certeza quais são os atos de guerra cibernética e fazer uso dos exércitos cibernéticos para a segurança cibernética.

Atualmente, há uma linha muito tênue entre a guerra cibernética e as atividades de crimes cibernéticos, o que permite que atores do sistema internacional que ameaçam a segurança cibernética de terceiros fiquem impunes ou sejam classificados erroneamente. Esse foi o caso de três ciberataques sofridos por Estados como Estônia, Rússia e Irã durante as primeiras décadas do século XXI.

Ademais, deve-se ressaltar que, segundo Geers (2011), os ataques cibernéticos que preocupam os Estados são aqueles que vêm de outros Estados, grupos ciberterroristas e hacktivistas; já que são eles que ameaçam a segurança nacional, as instituições e o poder do Estado. No entanto, a confluência do cibercrime com a ação do Estado deu origem a uma mistura perigosa que pode ser usada para atacar outro Estado por meio de mercenários cibernéticos (GEERS, 2011).

Em suma, a guerra cibernética é muito atraente para nações pequenas, pois poucos meios são necessários para criar uma bomba digital. Essa condição permite falar sobre guerra cibernética assimétrica, como descrito por Geers (2011, p.42) em: “Como a guerra cibernética é uma guerra não convencional e assimétrica, nações fracas em poder militar convencional também provavelmente investirão nela como forma de compensar desvantagens convencionais”.

Com base na citação de Geers (2011), entende-se que, como a guerra cibernética é uma guerra assimétrica, e portanto não depende necessariamente de ter equivalência quanto a um arcenal militar e/ou financeiro para entrar em guerras com outros países mais fortes nesse sentido, as nações com poder militar convencional provavelmente investirão nela como forma de equilibrar as desvantagens convencionais de armas convencionais. Trata-se de uma forma de fazer guerra que não exige grande capacidade tecnológica, mas de indivíduos engenhosos e experientes que explorem as fraquezas da infraestrutura digital em benefício de sua nação.

5 CONCLUSÃO

Diante do exposto neste artigo, pode-se constatar que o século XXI evidencia a presença latente de um poder tecnológico obtido pelo domínio da infraestrutura de comunicações digitais e dos computadores, a partir dos quais se vê nascer uma nova forma de controlar as massas por meio do domínio do ambiente virtual no qual se desenrola o quotidiano desse século. Assim, frente à pesquisa realizada, pode-se compreender que o ciberespaço é considerado o quinto domínio da guerra e, portanto, requer o desenvolvimento de táticas e estratégias que, por um lado, maximizem os efeitos das armas cibernéticas, e, por outro, garanta a segurança cibernética

nacional. Isso porque é no ciberespaço que se forma o ciberpoder, entendido como ataque e exploração da rede de computadores para, efetivamente, desativar o poder militar de um Estado adversário de forma não sangrenta.

Dessa forma, dada a relevância do uso da Paralisia Estratégica como alternativa de neutralização adversária, pode-se compreender que os perigos decorrentes do ciberespaço motivam que os ataques de retaliação sejam realizados apenas quando os pilares da segurança nacional estiverem em risco. Sendo assim, isso leva à necessidade de reconsideração dos conceitos de segurança internacional vigentes na atual conjuntura.

Nesse sentido, pode-se concluir com êxito que o problema levantado nesta pesquisa foi atendido ao se constatar, com base na teoria analisada, que, em uma era em que os sistemas estão cada vez mais conectados em rede, os ataques cibernéticos vêm despontando com um potencial considerável, haja vista que suas ações de paralisia podem desestruturar sistemas de forma instantânea, prejudicando os procedimentos e tomadas de decisão precisas e oportunas de uma nação. Tais ocorrências são resultado da limitação de possíveis ações de contra-ataques, sendo esses os principais efeitos da Paralisia Estratégica por meio dos ataques cibernéticos.

De outra forma, entende-se que, ao identificar as estratégias de ataque de uma nação rival, é possível adotar contramedidas que possam ser tomadas no intuito de reduzir, ou pelo menos eliminar, os seus efeitos. No entanto, é pertinente ressaltar que, devido às características flexíveis tanto das armas cibernéticas quanto do espaço cibernético, por enquanto não há tecnologia que garanta a segurança cibernética dos sistemas. A isso se deve acrescentar que as armas cibernéticas representam uma séria ameaça cibernética que põe em perigo a segurança cibernética nacional em todos os campos de atividade social que estão conectados à rede.

Assim sendo, cumpre-se o objetivo proposto por este estudo ao constatar-se que a guerra cibernética tem capacidades suficientes para realizar grande parte das tarefas estratégicas que antes eram realizadas por meio do poder aéreo, naval, espacial ou terrestre, uma vez que o poder cibernético passa a ocupar o lugar predominante para derrotar um inimigo. Isso porque entende-se que, nesta guerra do século XXI, absolutamente tudo pode se tornar alvo de ataques cibernéticos; seja nos sistemas de administração pública, nos sistemas bancários, nas Forças Armadas, dentre outros.

Por fim, destaca-se o fato de que, até então, não existe um sistema de alerta precoce contra ataques cibernéticos com armas cibernéticas. Consequentemente, a cibersegurança é um trabalho constante de preparação e reação aos eventos. Pela primeira vez na história, tal como evidenciado no decorrer desta pesquisa, as armas cibernéticas permitem que pequenos Estados com pequenos orçamentos de defesa causem danos graves a um inimigo poderoso. Logo, cabe

aos Estados se prepararem para os imprevistos e desconectarem-se, se necessário, de modo a buscar meios alternativos para o comando e o controle dos diferentes instrumentos de guerras cibernéticas.

A presente pesquisa não esgota, de forma alguma, o tema aqui estudado. Sendo assim, como sugestão para pesquisas futuras, tendo em vista a análise dos efeitos da Paralisia Estratégica por meio de ataques cibernéticos, acredita-se ser de grande relevância a busca de novas informações relacionadas a possíveis alternativas de defesas frente aos ataques cibernéticos.

REFERÊNCIAS

ABDALLA, Joffre Ferreira. **Domínio do espaço cibernértico por um país**: uma análise da presença do exército brasileiro no domínio cibernético. Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, 2020. Diponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/8305/1/2_AC_Final_OUT20_Cap%20Abdalla.pdf Acesso em: 06 jul. 2022.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS Whitney Lacerda de**. Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: https://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf Acesso em: 06 jul. 2022.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas**. Doutrina Militar de Defesa Cibernética. Brasília, 2014.

BROADCOM. **Relatório sobre ameaças à segurança na Internet**. 2014.Sysmantec. [Edição digital]. Disponível em: https://www.broadcom.com/site-search?q=Internet-Security-Threat-Report%202014. Acesso em: 15 maio 2022.

CARR**,** Jeffrey. **Inside Cyber Warfare**: Mapping the Cyber Underworld. O'Reilly Media; 2nd ed. [e-book] Sebastopol, California, EE.UU. 2011.

CARTWRIGHT, James E. **Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates.** Washington, DC. 2010. Retrieved in: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf. Acessed in: 10 may 2022.

CARVALHO, Guilherme Almeida Matos de. **A teoria de warden aplicada na guerra cibernética:** a aderência do ataque do Stuxnet à Estratégia da Paralisia e à Teoria dos Cinco Anéis. Curso de Estado-Maior para Oficiais Superiores (Dissertação) 51fl. Escola de Guerra Naval, Rio de janeiro, 2020. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CEMOS_076_MONO_CC_CA_GUILHERME%20CARVALHO.pdf. Acesso em: 21 fev. 2022.

COLLE, Raymond. Internet: un cuerpo enfermo y un campo de batalla. **Revista Latina de Comunicación Social**, 2000. Disponible en: http://www.ull.es/publicaciones/latina/aa2-000qjn/91colle.htm. Acesso en: 20 jun. 2022.

CLARKE, Richard A.; KNAKE Robert K. **Guerra Cibernética**: A próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015. 242 p.

CLAUSEWITZ, Karl Von. **Da guerra**. A Esfera dos Livros. 2015. Disponível em: https://www.esferalibros.com/noticias/von-clausewitz-maestro-de-la-guerra/ Acesso em: 15 maio 2022.

DOUHET, Giulio; WARDEN, John. Aspectos Evolutivos da Teoria do Poder Aéreo. **Nação e Defesa**, n.106, 2a série. Outono-Inverno, 2003.

FERRAZ, A. P. M; BELHOT, R. V. Taxonomia de Bloom: revisão teórica e apresentação das adequações do instrumento para definição de objetivos instrucionais. **Gest. Prod**., v. 17, n. 2, p. 421-431, 2010. Disponível em: https://webcache.googleusercontent.com/search?q=cache:T7IeKkeQ8JcJ:https://www.scielo.br/j/gp/a/bRkFgcJqbGCDp3HjQqFdqBm/%3Fformat%3Dpdf%26lang%3Dpt+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 15 maio 2022.

GEERS, Kenneth. Sun Tzu and cyber war. **Cooperative Cyber Defence Centre of Excellence***,* 2011. [Digital Edition]. Retrieved in: https://ccdcoe.org/uploads/2018/10/Geers2011_SunTzuandCyberWar.pdf. Accessed in: 17 may 2022.

GONÇALVES, Ricardo Penedo. **A primeira Guerra Cibernética**:os ataques cibernéticos contra a Estônia, em 2007, à luz da teoria dos cinco anéis do Coronel John Warden. Escola de Guerra Naval. Rio de Janeiro, 2018. Disponível em: https://webcache.googleusercontent.com/search?q=cache:FFR6tx1-g-wJ:https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CEMOS%2520023%2520MONO%2520CC%2520RICARDO%2520PENEDO.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br Acesso em: 17 maio, 2022.

HOBBES, Thomas. **The Leviathan**: Selections on the State of Nature, State of War and formation of the State, 1651. Retrieved in: http://courses.washington.edu/hsteu302/Hobbes%20selections%20(edited).htm. Accessed in: 20 may 2022.

KEISER, Gregg. Russian 'cyber militia' knocks Kyrgyzstan offline. **Computerworld**. News. Security. Published in: jan. 28, 2009. Retrieved in: https://www.computerworld.com/article/2769407/russian--cyber-militia--knocks-kyrgyzstan-offline.html. Accessed in: 15 may 2022.

LIN, Herbert. A virtual necessity: Some modest steps toward greater cybersecurity. **Bulletin of the Atomic Scientists**, v. 68, n.5, p.75-87, 2012. Retrieved in: https://journals.sagepub.com/doi/full/10.1177/0096340212459039. Accessed in: 20 may 2022.

LORENTS, Peter; OTTIS, Rain. **Knowledge Based Framework For Cyber Weapons And Conflict**. Conference on Cyber Conflict. Proceedings, 2010. Retrieved in: https://ccdcoe.org/uploads/2018/10/Lorents-et-al-Knowledge-Based-Framework-for-Cyber-Weapons-and-Conflict.pdf. Accessed in: 15 may 2022.

LYNN III. William J. Defending a New Domain. The Pentagon's Cyberstrategy. **Foreign Affairs**, 2010. Retrieved in: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Accessed in: 20 may 2022.

MARCELINO, Henriques Manuel. **Segurança cibernética e ciberdefesa em moçambique**: fundamentos, características e desafios. (Tese) Universidade Federal do Rio Grande do Sul. Faculdade de Ciências Econômicas. Programa de Pós-Graduação em Estudos Estratégicos Internacionais. Maputo, 2021. 229 p. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/222091/001126905.pdf?sequence=1&isAllowed=y. Acesso em: 30 jan.2022.

MATOS, Sergio Ricardo Reis; SOUZA, Marcelo Bastos de; PEREZINO, Paulo Eduardo de Mello. Os conflitos contemporâneos e a teoria de sun tzu: novas abordagens, antigos postulados. **Revista InterAção**, v. 9, n. 9, jul/dez 2015. Disponível em: https://periodicos.ufsm.br/interacao/article/download/17084/pdf . Acesso em: 30 jan. 2022.

NYE JUNIOR, Joseph S. **O Futuro do Poder**. São Paulo: Benvirá, 2012. 334 p.

NETO, Ricardo Borges Gama. Guerra cibernética / guerra eletrônica: conceitos, desafios e espaços de interação. **Revista Política Hoje**, v.26, n. 1, p. 201-217, 2017. Disponível em: file:///C:/Users/POSITIVO/Downloads/9180-34022-1-PB.pdf. Acesso em: 07 jul. 2022.

ORTON, Megan. Air Force remains committed to unmanned aircraft systems. **Air Force**. 2009. Retrieved in: https://www.af.mil/News/Article-Display/Article/121391/air-force-remains-committed-to-unmanned-aircraft-systems/. Accessed in: 15 may 2022.

PEREIRA, Séfora de Carvalho. **A Doutrina Militar de Defesa Cibernética e seus desdobramentos na política externa brasileira**. Núcleo de Pesquisa em Relações Internacionais. 2021. Disponível em: https://nupri.prp.usp.br/blog/a-doutrina-militar-de-defesa-cibernetica-e-seus-desdobramentos-na-politica-externa-brasileira/. Acesso em: 08 jul. 2022.

PANDA SECURITY. Virus. **Pandasecurity.com** [Online] [date unkown] Retrieved in: https://www.pandasecurity.com/en/security-info/virus/. Accessed in: 16 may 2022.

RID, Tomas; MCBURNEY, Peter. Cyber-Weapons. **The RUSI Journal**, n.157, v.1, p. 6-13, 2012. Retrieved in: https://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354. Accessed in: 15 may 2022.

ROSA, Carlos Eduardo Valle. **Poder aéreo**: guia de estudos. 1a ed. Rio de Janeiro: UNIFA, 2015.

REUTERS. Mykel Nicolaou. Apagão para parte de Londres por 40 minutos em plena hora do rush. **Folha de São Paulo**. São Paulo, sexta-feira, 29 ago. 2003.Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2908200303.htm. Acesso em: 07 jul. 2022.

SHAKARIAN, Paulo. **Introduction to Ciber-Warfare**. Manhattam: Elsevier, 2013. E-book.

SANTOS, Ilana Danielle Soares. **Conflitos cibernéticos**: a ascensão do ciberespaço segundo a produção científica de Relações Internacionais indexada na Web of Science. 2021. 172 f., il. Dissertação (Mestrado em Relações Internacionais) Universidade de Brasília, Brasília, 2021. Diponível em: https://repositorio.unb.br/handle/10482/41940 Acesso em: 07 jul. 2022.

SILVA, Daniel Neves. **Guerra do Golfo**. Brasil Escola. 2020. Disponível em: https://brasilescola.uol.com.br/historiag/guerra-golfo.htm. Acesso em: 07 jul. 2022.

SOUZA, Marcio Braga de. **A aderência da estratégia da paralisia sob a ótica do pensamento clássico**. Trabalho de conclusão do Curso de Estado Maior para Oficiais Superiores - Escola de Guerra Naval. Rio de Janeiro, 2016, 50p.

TZU, Sun. **A Arte da Guerra**. Trad. Cândida de Sampaio Bastos. 1a ed. São Paulo: Editora Cultura, 2016.

THOMAS, Timothy L. Las estrategias electrónicas de China. **Military Review***,* p. 72-79, jul-ago, 2001.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. Conventional Arms [online]. **United Nations**. Office for Disarmament Affairs [n.d]. Retrieved in: https://www.un.org/disarmament/conventional-arms/ Accessed: em: 15 jun. 2022.

VAN EVERA, Stephen. **Causes of War**: Power and the Roots of Conflict. Cornell University Press, 1999. Retrieved in: https://www.jstor.org/stable/10.7591/j.ctt24hg70. Accessed: 20 may 2022.