EMANUEL FERREIRA JESUS

OS EFEITOS DAS AÇÕES CIBERNÉTICAS SOBRE AS CAPACIDADES MILITARES NO COMBATE CONTEMPORÂNEO:

qual é o impacto dos ataques cibernéticos preemptivos nas operações militares contemporâneas?

Trabalho de Conclusão de Curso - Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior Escola Superior de Guerra, como requisito à obtenção do diploma do Curso Superior de Segurança e Defesa Cibernética

Orientador: Cel R1 João de Azevedo

Rio de Janeiro
2023

C2023 ESG

Este trabalho, nos termos de legislação que resguarda os direitos autorais, é considerado propriedade da ESCOLA SUPERIOR DE GUERRA (ESG). É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa. Os conceitos expressos neste trabalho são de responsabilidade do autor e não expressam qualquer orientação institucional da ESG.

_____

EMANUEL FERREIRA JESUS

AGRADECIMENTOS

Ao chegar ao fim desta jornada acadêmica, aproveito para expressar minha profunda gratidão a todos que contribuiram direta ou indiretamente para meu sucesso. Esta realização não teria sido possível sem o apoio, orientação e companheirismo que recebi ao longo dessa caminhada desafiadora.

A Deus, agradeço por iluminar meu caminho, permitindo-me superar obstáculos e alcançar esta conquista. Com fé, sei que tudo é possível, e Sua presença foi alicerce para minha determinação.

À minha família, agradeço por seu amor incondicional e apoio constante. Vocês são meu alicerce, minhas maiores incentivadoras e a razão pela qual nunca desisti. Cada conquista é, em parte, de vocês, e sou eternamente grato por isso.

À coordenação do curso e aos instrutores, agradeço pela dedicação e expertise que compartilharam conosco. Suas orientações foram cruciais para meu crescimento acadêmico e pessoal. A paciência e a paixão com as quais vocês conduzem o ensino são verdadeiramente inspiradoras.

Aos meus colegas da turma pioneira, compartilhamos um laço especial. Nossa jornada foi repleta de desafios e vitórias, e crescermos juntos foi uma experiência única. Agradeço por cada momento de aprendizado e pelas amizades que formamos. Vocês são uma fonte inesgotável de inspiração. À medida que encerro este capítulo da minha vida acadêmica, levo comigo não apenas conhecimento, mas também a lembrança das pessoas incríveis que encontrei. Este trabalho é um testemunho do nosso esforço coletivo e compromisso com a excelência.

Ao Cel Azevedo, quero expressar um agradecimento especial ao Sr. por sua dedicação incansável e entusiasmo em garantir que nosso curso fosse conduzido com a excelência. Sua liderança e comprometimento fizeram toda a diferença em nossa jornada de aprendizado.

“Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2)

RESUMO

Este trabalho aborda o tema dos efeitos das ações cibernéticas nas capacidades militares no combate contemporâneo. As ações cibernéticas podem afetar a preparação e o emprego das forças militares de diversas maneiras. Por exemplo, elas podem comprometer a segurança das comunicações e sistemas de informação, afetando a capacidade de planejamento e execução de operações militares. Além disso, as ações cibernéticas podem ter um impacto direto nas capacidades militares, como a capacidade de defesa aérea e a capacidade de inteligência. Discute-se também como as ações cibernéticas podem influenciar os diversos níveis de preparação: estratégico, operacional e tático. Compara-se os efeitos gerais para as operações militares, os efeitos específicos para um meio naval além de verificar estes impactos em um cenário de guerra real: guerra da Ukrânia. Em resumo, as ações cibernéticas são uma ameaça real às capacidades militares no combate contemporâneo.

Palavras-chave: ações cibernéticas; capacidades militares; guerra cibernética; cibersegurança; operações militares.

SUMÁRIO

1 INTRODUÇÃO

A literatura a respeito dos efeitos de ações cibernéticas sobre as capacidades militares é relativamente recente. No entanto, alguns estudos já foram realizados que apontam para: danos a sistemas de comunicação e de comando e controle, o que pode prejudicar a capacidade das forças militares de coordenar suas ações; apoio a guerra psicológica: Ataques cibernéticos podem ser usados para espalhar desinformação entre as forças militares, o que pode prejudicar a tomada de decisão e a moral dos combatentes; pode causar danos a infraestruturas críticas que apoiam o esforçode guerra; e na força Naval pode interromper o uso de todos os sistemas de controlede propulsão, sistemas de plataforma ou sistemas de armas.

Um dos principais usos operacionais das ações cibernéticas é o seu uso em apoio ao ataque preemptivo. Essas ações são usadas para prejudicar a capacidade do adversário de lutar, o que pode aumentar a probabilidade de vitória. Estes ataques podem causar danos significativos a sistemas e infraestruturas críticas, o que pode prejudicar a capacidade das forças militares de se defender e de responder a um ataque.

Esta pesquisa será realizada na forma de revisão bibliográfica e buscará responder a seguinte hipótese da pesquisa: as táticas de ataque preemptivo no ciberespaço podem ter um impacto na resiliência e na capacidade de resposta das forças militares?

Os efeitos de ações cibernéticas sobre as capacidades militares são um tema importante que merece ser estudado. Assim, esta pesquisa visa contribuir para o entendimento desses efeitos e para o desenvolvimento de medidas para mitigar seus impactos.

2 REFERENCIAL TEÓRICO

Este capítulo é a base teórica do ensaio, será construído a partir de uma revisão sistemática da literatura sobre o tema, com o objetivo de apresentar os conceitos, teorias e abordagens relevantes para a compreensão do problema em questão.

2.1 CONCEPÇÃO DE PREPARO E EMPREGO

De acordo com a concepção de preparo e emprego, do MD-30-01 - DOUTRINA DE OPERAÇÕES CONJUNTAS (BRASIL, 2020), os níveis estratégicos, operacionais e táticos são definidos da seguinte forma:

- Nível estratégico: O nível estratégico é o mais elevado da guerra e refere-se ao uso do poder militar para alcançar objetivos políticos. No nível estratégico, as operações militares são planejadas e executadas para alcançar objetivos de longo prazo, como a defesa do país ou a promoção de seus interesses internacionais. Elas envolvem o emprego de todas as capacidades militares do país, incluindo as forças convencionais e não convencionais: as forças especiais e as forças cibernéticas.

- Nível operacional: O nível operacional é o intermediário da guerra e refere-se ao emprego de forças militares para alcançar objetivos estratégicos. No nível operacional,

as operações militares são planejadas e executadas para alcançar objetivos de médio prazo, como a derrota de um adversário ou a conquista de um território. Elas envolvem o emprego de forças militares de diferentes Forças Singulares, sob um único comando.

- Nível tático: O nível tático é o mais baixo da guerra e refere-se ao combate direto entre forças militares. No nível tático, as operações militares são planejadas e executadas para alcançar objetivos de curto prazo, como a captura de um objetivo ou a derrota de um inimigo.

A concepção de preparo e emprego do MD-30-01 estabelece que as operações militares devem ser planejadas e executadas em todos os níveis, de forma integrada e coordenada. O sucesso das operações militares depende da capacidade de os comandantes de todos os níveis compreenderem os objetivos e as limitações de suas operações, e de coordenarem suas ações de forma eficaz.

Segundo Schulze (2020), no nível estratégico, as operações cibernéticas podem ser usadas para: Destruir ou degradar sistemas e redes críticos de um adversário; Influenciar a opinião pública e as decisões políticas; e Fornecer apoio a operações de combate. Já no nível operacional, as operações cibernéticas podem ser usadas para: Desarticular as forças armadas de um adversário; Desabilitar sistemas de defesa; e Apoiar operações de apoio logístico. Concluindo, o nível tático, pode usar as opera- ções cibernéticas para: Destruir ou degradar sistemas e redes de combate de um adversário; Controlar o espaço cibernético em uma área de combate; e Apoiar operações de reconhecimento e vigilância.

Em resumo, a análise da concepção de preparo e emprego, conforme estabelecida no MD-30-01 - DOUTRINA DE OPERAÇÕES CONJUNTAS, fornece um entendimento fundamental da estrutura hierárquica e da coordenação necessárias para o sucesso das operações militares. A clara definição dos níveis estratégicos, operacionais e táticos é essencial para o planejamento eficaz e a implementação de estratégias militares abrangentes. A incorporação das operações cibernéticas em cada um desses níveis demonstra a crescente importância da cibersegurança e do uso de força no ciberespaço na arena militar contemporânea.

Além disso, a revisão da literatura apresentada ressalta a versatilidade das operações cibernéticas nos diferentes níveis. No nível estratégico, as ações cibernéticas podem ser empregadas para alcançar objetivos políticos, desestabilizando as capacidades críticas do adversário e influenciando a opinião pública. No nível operacional, as operações cibernéticas podem contribuir para a desarticulação das forças inimigas e a neutralização de sistemas de defesa. No nível tático, elas podem ser utilizadas para apoiar operações de combate, controle do espaço cibernético e obtenção de informações críticas. Essas considerações enfatizam a necessidade de uma abordagem integrada e coordenada para as operações cibernéticas, alinhando-as com objetivos estratégicos, operacionais e táticos.

2.2 O CIBERESPAÇO COMO CAMPO DE BATALHA

A integração e coordenação entre esses níveis são fundamentais para o sucesso das operações militares em um ambiente cada vez mais digital e cibernético. Além disso, a inserção do elemento cibernético nas estratégias militares ressalta a importância crescente da cibersegurança e das operações no ciberespaço. A literatura adicional apresentada, destacando os possíveis usos das operações cibernéticas em cada um dos níveis, ilustra a flexibilidade e a adaptabilidade dessa ferramenta no contexto das operações militares. Isso demonstra como as ações de ataque e uso da força no ciberespaço podem ser empregadas em todos os niveis: estrategicamente, operacionais e táticas das operações cibernéticas na doutrina militar. Cabe neste momento a necessidade de estudar o que é e como usar o campo de batalha cibernético. Assim, nesta seção, examinaremos como essa dimensão virtual tornou-se fundamental nas estratégias militares e de segurança em todo o mundo. Para compreendermos melhor esse fenômeno é crucial analisar os trabalhos fornecidos por diversos artigos acadêmicos que abordam essa temática.

Segundo o autor Silva (2017) o espaço cibernético refere-se ao ambiente digital em que as atividades relacionadas à tecnologia da informação e comunicação (TIC) ocorrem. Esse espaço compreende a internet, redes de computadores, sistemas de informação e todas as infraestruturas e ativos digitais que possibilitam a comunicação, o armazenamento de dados, o processamento de informações e a conectividade global. O espaço cibernético não se limita apenas à dimensão técnica, mas também inclui as interações e atividades humanas que ocorrem nesse ambiente. Isso envolve a troca de informações, transações financeiras, comunicação, pesquisa, entretenimento e uma ampla gama de atividades que dependem da infraestrutura digital. O autor considera o espaço cibernético como um campo de batalha potencial, onde ameaças cibernéticas, como ataques cibernéticos, desinformação e espionagem digital, podem afetar os interesses nacionais do Brasil. Portanto, a segurança cibernética é crucial para proteger as operações, a infraestrutura crítica e as informações sensíveis que transitam por esse espaço, garantindo a integridade, confidencialidade e disponibilidade dos ativos digitais.

Arquilla e Ronfeldt (1993) abordam a evolução do conceito de guerra e conflito no contexto do ciberespaço e das redes. Os autores argumentam que o ciberespaço transcendeu seu papel inicial como uma simples ferramenta tecnológica e se tornou um domínio de confronto global. Eles introduzem o termo ”netwar”para descrever um novo tipo de guerra descentralizada e em rede que se baseia na conectividade, na agilidade e na capacidade de ação em tempo real. Esse conceito se aplica não apenas a atores estatais, mas também a atores não estatais, incluindo grupos terroristas e movimentos sociais. Os autores discutem como a netwar está alterando as dinâmicas tradicionais de conflito, introduzindo a ideia de que as nações agora enfrentam inimigos

sem fronteiras geográficas. O artigo explora a natureza do ciberconflito, destacando a importância da cibersegurança e da preparação para enfrentar as ameaças emergentes no ciberespaço. conclui-se que o ciberespaço transcendeu seu status inicial como uma mera ferramenta tecnológica para se tornar um novo domínio de confronto global. Assim, o espaço cibernético tornou-se um campo onde as nações podem enfrentar inimigos sem fronteiras geográficas.

Já Denning (1999), ilustra exemplos de grupos e ações no ciberespaço no cenário das relações internacionais. A autora destaca a capacidade do ciberespaço de contornar fronteiras geográficas e servir como uma ferramenta poderosa para influenciar a política externa. Esse artigo fornece uma visão valiosa sobre a dinâmica da influência política no ciberespaço e seus desafios para a segurança nacional. Demonstrando a força estratégica das ações cibernéticas.

O ciberespaço não é apenas um campo de batalha, mas também um espaço de competição e influência. Os conceitos de ”ciberguerra fria”e ”guerra informacional”ganham destaque em estudos como os de Rid (2013) e Valeriano e Maness (2015), que exploram a luta pelo controle da narrativa e da opinião pública no ciberespaço. Os trabalhos oferecem perspectivas complementares sobre a natureza da guerra cibernética. A abordagem de Rid é útil para compreender os limites da guerra cibernética, enquanto a abordagem de Valeriano e Maness é útil para compreender o potencial da guerra cibernética como um instrumento de competição e influência.

importante destacar que não há consenso, no artigo ”Cyberspace is not a warfighting domain”Libicki (2017) argumenta que o ciberespaço não deve ser considerado um domínio de combate tradicional, como terra, mar ou ar. Ele enfatiza que o ciberespaço é mais um campo de inteligência e operações especiais, onde o sigilo e a discrição são essenciais. O autor ressalta que as capacidades militares no ciberespaço devem ser voltadas para a defesa, a exploração de vulnerabilidades e a identificação de ameaças, em vez de conflitos abertos.

Segundo Clarke e Knake (2010) a dependência crescente da infraestrutura crítica de tecnologias de informação e comunicação torna os países vulneráveis a ataques cibernéticos destrutivos. Os autores apontam que esse é um problema global, e o Brasil não é exceção. Nesse sentido, o país enfrenta desafios na proteção de suas infraestruturas críticas, conforme discutido por Machado (2018).

No cenário brasileiro, a doutrina de segurança cibernética também reconhece a crescente importância do ciberespaço como campo de batalha. Em seu artigo, ”A Segurança Cibernética no Brasil: Desafios e Perspectivas”(SILVA, 2017), Silva explora a necessidade de fortalecer a capacidade de defesa cibernética do país diante das ameaças crescentes. Para isso, é necessário investir em infraestrutura, capacitação de pessoal e desenvolvimento de tecnologias de defesa cibernética. Além disso, Amaral e Lima (2015) discutem as estratégias de defesa cibernética adotadas pelo Brasil em

seu artigo ”Estratégia Nacional de Defesa e a Segurança Cibernética”. Eles destacam a integração da segurança cibernética nas políticas de defesa nacional como um avanço significativo, pois representa um reconhecimento da importância do ciberespaço como um campo de batalha potencial.

A capacidade de influenciar a narrativa no ciberespaço também é reconhecida como crucial. O artigo ”Operações de Informação no Ciberespaço: Uma Análise do Caso Brasileiro”(ROCHA, 2019) ressalta a importância de estratégias de operações de informação para defender os interesses nacionais. O autor argumenta que as operações de informação são um instrumento essencial para a segurança cibernética, pois podem ser usadas para:

- Proteger a infraestrutura crítica: As operações de informação podem ser usadas para identificar e mitigar vulnerabilidades nas infraestruturas críticas, bem como para disseminar informações falsas ou enganosas que possam prejudicar os ataques cibernéticos;
- Defender a soberania: As operações de informação podem ser usadas para promover a narrativa nacional e combater a propaganda estrangeira; e
- Proteger a democracia: As operações de informação podem ser usadas para combater a desinformação e promover a liberdade de expressão.

O autor analisa o caso brasileiro e conclui que o país ainda está em um estágio inicial de desenvolvimento de estratégias de operações de informação. No entanto, ele argumenta que o Brasil precisa investir nesse campo para fortalecer sua capacidade de defesa cibernética e defender seus interesses nacionais.

Este capítulo analisou a evolução do ciberespaço de ferramenta tecnológica a campo de batalha global. Nesse contexto, a segurança cibernética é um desafio crucial, que requer esforços nos níveis estratégico, operacional e tático. A influência política no ciberespaço, por meio de operações de informação, também é um desafio importante. No cenário global, a dependência das TIC na infraestrutura crítica torna a segurança cibernética uma questão global. O Brasil também enfrenta estes desafios e é essencial investir em segurança cibernética e adaptação estratégica para proteger os interesses nacionais.

2.3 FATORES DETERMINANTES NO RESULTADO DE UM CONFLITO MILITAR

Neste capítulo, serão explorados fatores cruciais que desempenham um papel significativo no desfecho de um conflito militar. Vantagem militar, iniciativa das ações, inteligência, cibernética e a capacidade de realizar ataques preemptivos são elementos que moldam o curso de um conflito, frequentemente delineados em estudos acadêmicos de relevância.

Biddle (2004) argumenta que a força militar é um fator importante, mas não o único, que determina o sucesso na guerra. Ele identifica uma variedade de outros fatores que contribuem para a vitória e a derrota, incluindo a qualidade da liderança, a dou- trina militar, a tecnologia e a moral da tropa. Biddle também enfatiza a importância da iniciativa na guerra. A iniciativa é a capacidade de escolher quando e onde lutar. Ela permite que um lado imponha sua vontade ao adversário, forçando-o a reagir às suas ações. Biddle sustenta que a iniciativa é essencial para a vitória na guerra moderna. A inteligência desempenha um papel fundamental na tomada de decisões estratégicas. O acesso a informações precisas pode permitir que um comandante tome decisões informadas e adapte suas táticas conforme necessário (KAHN, 1967). A falta de inteligência eficaz pode ser prejudicial, como demonstrado em diversos conflitos históricos (RICHELSON, 1995).

Conforme analisado por Libicki (2007) a capacidade de comprometer os sistemas de comunicação e controle do inimigo é considerada um elemento decisivo no âmbito das ações cibernéticas. Isso se deve à dependência crescente das operações militares e infraestruturas críticas em sistemas altamente sofisticados de comunicação e controle. Ao comprometer tais sistemas, um ator no ciberespaço pode prejudicar significativamente a capacidade do inimigo de planejar, coordenar e executar operações militares, criando assim uma vantagem estratégica e tática. A dissuasão desempenha um papel fundamental na gestão de conflitos no ciberespaço, e as estratégias devem ser consideradas em consonância com o contexto político e as implicações das ações cibernéticas.

A vantagem militar é uma característica que pode ser determinante em um conflito. Conforme observado por Clausewitz (1832), o equilíbrio de forças e recursos militares é um dos pilares da estratégia de guerra. No entanto, a vantagem militar nem sem- pre se traduz em vitória, como demonstram os casos em que forças numericamente superiores foram derrotadas por estratégias mais eficazes (ZEDONG, 1961).

Segundo a doutrina de operações conjuntas brasileira Defesa (2020), a vantagem militar é uma situação em que uma força militar obtém superioridade relativa sobre um oponente, permitindo-lhe alcançar seus objetivos de maneira eficaz. Essa vantagem é baseada em uma série de princípios e características que tornam as operações militares mais eficazes, pode se citar os seguintes pricípios que podem proporcionar a vantagem:

- Surpresa: Ao manter as intenções e movimentos ocultos, uma força pode pegar o inimigo de surpresa, desorganizando suas defesas e obtendo uma vantagem tática;
- Iniciativa: Isso significa que a força pode controlar o ritmo das operações, ditar o fluxo dos eventos e forçar o inimigo a reagir aos seus movimentos;

- Inteligência: A inteligência permite que a força compreenda as intenções do inimigo, suas capacidades e as condições do campo de batalha, possibilitando decisões mais informadas; e
- Flexibilidade: A capacidade de se adaptar a mudanças nas condições do campo de batalha e ajustar estratégias e táticas de acordo com as circunstâncias é essencial para o sucesso.

Neste contexto faz-se mister estudar a correlação entre o ataque preemptivo, a inteligência e a iniciativa das ações como forma de obter vantagem militar. O ataque preemptivo, ou seja, aquele realizado para impedir que um adversário ataque primeiro, é uma estratégia que pode ter sérias implicações. O estudo de Sagan (1993) sobre os riscos e benefícios dos ataques preemptivos destaca a complexidade dessa abordagem. Um ataque mal calculado pode desencadear uma escalada desnecessária do conflito.

As operações cibernéticas podem ser usadas como um meio de realizar um ataque preemptivo. Por exemplo, um país pode usar um ataque cibernético para desabilitar o sistema de defesa aérea de um inimigo, permitindo que suas forças aéreas tenham vantagem no teatro de operações (SCHULZE, 2020).

Ainda analisando este artigo também pode-se obter vantagem militar degradando sistemas e infraestruturas inimigos, roubando informações confidenciais, ou criando desordem ou caos. Isso pode permitir que um país ataque primeiro ou tome medidas que o inimigo não espera, o que é um dos objetivos de um ataque preemptivo. As operações cibernéticas também podem ser usadas para obter iniciativa das ações, surpreendendo ou confundindo o inimigo. Isso pode permitir que um país aja de forma rápida e decisiva, o que também é um objetivo de um ataque preemptivo.

A legalidade do ataque preemptivo é um tópico central. Segundo Brown (2017), o direito internacional consagra o princípio da legítima defesa, que permite a um Estado usar a força em autodefesa quando enfrenta uma ameaça iminente e não pode recorrer a meios pacíficos. No entanto, a interpretação desse princípio pode variar, levando a debates sobre o que constitui uma ameaça iminente.

Um aspecto relevante na análise jurídica do ataque preemptivo é a avaliação das consequências humanitárias. Como abordado por Lang (2019), a decisão de lançar um ataque preventivo deve levar em consideração a minimização do sofrimento humano e o respeito ao direito internacional humanitário.

Além disso, a questão da autorização prévia de órgãos internacionais, como o Conselho de Segurança da ONU, é um elemento crítico na análise jurídica do ataque preemptivo. Conforme destacado por Tzanakopoulos (2017), a Carta das Nações Unidas exige que os Estados busquem a autorização do Conselho de Segurança antes de

usar a força, a menos que estejam agindo em legítima defesa. Essa autorização é fundamental para garantir a legalidade das ações militares preventivas.

Em resumo, o estudo jurídico do ataque preemptivo envolve uma análise cuidadosa das implicações legais, éticas e humanitárias dessas ações. A interpretação do princípio da legítima defesa, a consideração das consequências humanitárias e a autorização prévia de órgãos internacionais desempenham papéis fundamentais na determinação da legalidade desses atos.

No contexto da doutrina brasileira, a importância desses fatores é amplamente reconhecida. O Livro Branco de Defesa Nacional destaca a necessidade de um sistema de inteligência robusto e a importância da cibersegurança como elementos-chave na estratégia de defesa do Brasil. Entretanto, é importante observar que a doutrina brasileira também enfatiza a busca pela dissuasão e a preferência por soluções diplomáticas (BRASIL, 2020). Isso reflete a compreensão de que a dissuasão pode ser uma alternativa eficaz aos ataques preventivos.

A discussão sobre a importância do ataque preemptivo com base nas fontes apresentadas ressalta a complexidade desse tópico nas estratégias militares contemporâneas, com destaque para a iniciativa, que permite a um lado impor sua vontade ao adversário e é essencial na guerra moderna. A capacidade de comprometer os sistemas de comunicação e controle do inimigo é fundamental nas ações cibernéticas e pode criar uma vantagem estratégica.

O ataque preemptivo é discutido como uma estratégia possível, onde as operações cibernéticas desempenham um papel importante em obter iniciativa, surpreender o inimigo e agir de maneira rápida e decisiva. No entanto, a legalidade do ataque preemptivo é um tema central, envolvendo interpretações variadas do princípio da legítima defesa, considerações humanitárias e a autorização prévia de órgãos internacionais.

Conclui-se que a vantagem militar é influenciada por vários fatores, incluindo iniciativa, inteligência e capacidade cibernética. A obtenção de vantagem estratégica pode ser alcançada por meio de ataques cibernéticos preventivos, mas isso requer uma avaliação cuidadosa das implicações legais, éticas e humanitárias. A doutrina brasileira destaca a importância de tais fatores, mas também enfatiza a dissuasão e a preferência por soluções diplomáticas. Assim, a discussão sobre o ataque preemptivo como uma estratégia eficaz continua evoluindo no cenário de segurança global.

2.4 O IMPACTO DAS AÇÕES CIBERNÉTICAS NAS OPERAÇÕES MILITARES

As ações cibernéticas têm tido um profundo impacto nas operações militares, expandindo o leque de capacidades militares disponíveis. Essas ações possibilitaram o uso de táticas não cinéticas na guerra, como a guerra da informação e as operações psicológicas (SMITH, 2019). Além disso, facilitaram a integração das capacidades cibernéticas com as operações militares convencionais, resultando em novas oportunidades para alcançar assimetria na guerra (JOHNSON, 2018).

A expansão das capacidades cibernéticas permitiu que as forças militares utilizassem a guerra da informação como uma ferramenta poderosa. A disseminação de informações falsas, a manipulação de narrativas e o uso de propaganda são estratégias cibernéticas que podem afetar a percepção pública e a tomada de decisões nos campos de batalha modernos (RID, 2013).

A integração de capacidades cibernéticas com operações convencionais trouxe uma nova dinâmica para o campo de batalha. O uso de ataques cibernéticos coordenados com operações terrestres, aéreas ou navais permite que as forças militares obtenham vantagens táticas significativas (GOURE, 2017). Isso resulta em uma capacidade aumentada de atingir os objetivos militares e alcançar o sucesso nas operações.

Um aspecto importante do impacto das ações cibernéticas é a capacidade de forças militares menores e menos tecnologicamente avançadas de compensar a desvantagem numérica contra adversários maiores (LIBICKI, 2017). A natureza assimétrica das operações cibernéticas significa que uma nação com recursos limitados ainda pode infligir danos significativos a um inimigo mais poderoso (ARQUILLA; RONFELDT, 1997).

As capacidades de vigilância e reconhecimento cibernético permitem que as forças militares obtenham informações em tempo real sobre as atividades do inimigo, o que, por sua vez, facilita a tomada de decisões mais informadas. Com isso há uma melhoria da consciência situacional e das capacidades de coleta de inteligência, outro benefício notável das ações cibernéticas nas operações militares (MAZANEC, 2018).

As ações cibernéticas também têm tido um impacto significativo na evolução das táticas de combate. A capacidade de interromper as comunicações e os sistemas de comando e controle do inimigo cria oportunidades para a desorganização das forças adversárias (CLARKE; KNAKE, 2010). Isso pode resultar em uma vantagem tática decisiva no campo de batalha.

concluindo, as ações cibernéticas tiveram um impacto profundo e multifacetado nas operações militares. Elas expandiram as capacidades disponíveis, permitiram a guerra da informação, aprimoraram a integração com operações convencionais, cria-ram oportunidades para a assimetria, melhoraram a consciência situacional e afetarama dissuasão no campo de batalha. No entanto, também apresentaram desafios, como a escalada de conflitos e a necessidade de cibersegurança robusta.

2.5 O IMPACTO DAS AÇÕES CIBERNÉTICAS NOS NAVIOS DE GUERRA MODERNOS

Os navios de guerra modernos dependem fortemente de sistemas de armas altamente sofisticados e automatizados (MCGUIRE, 2017). Os sistemas de mísseis, radares e armas de defesa antimíssil são componentes críticos da capacidade de um navio de guerra em combate. As ações cibernéticas podem comprometer esses sistemas, tornando-os inoperáveis ou desviando sua precisão (RATTRAY, 2017). Outros sistemas também podem ser afetados tais como: sistemas de controle de avarias, sistemas de propulsão e sistemas de suporte à vida, todos eles dependentes da ciberné-

tica, podem ser alvos de invasões cibernéticas que podem resultar em falhas críticas (JOHNSON, 2018).

Os sistemas de controle da plataforma é outro sistema vital para o funcionamento seguro e eficaz de navios de guerra. Eles abrangem desde a navegação e o controle do motor até a gestão de recursos a bordo. A invasão cibernética desses sistemas pode resultar em perda de controle do navio, colisões, ou mesmo danos graves à tripulação (KUGLER; KUGLER, 2019).

Outro sistema crucial para a conectividade e comando e controle dos navios de guerra são os sistemas de comunicações via satélite. Através desses sistemas, os navios recebem ordens, trocam informações e coordenam operações com outros ativos militares. Um ataque cibernético direcionado a esses sistemas pode interromper a comunicação e deixar os navios isolados e incapazes de receber orientações ou relatar sua situação (MAZANEC, 2018).

As ações cibernéticas também afetaram a forma como as forças navais conduzem operações e exercem o controle sobre os mares (VALERIANO; MANESS, 2015). A capacidade de interromper as comunicações inimigas e desativar sistemas de armas inimigos à distância conferiu às marinhas modernas uma vantagem tática significativa. Além disso, a coleta de inteligência cibernética permite que as forças navais obtenham informações sobre os movimentos do inimigo com rapidez e precisão (LIBICKI, 2017).

A proteção contra ameaças cibernéticas torna-se, então, uma prioridade crítica para as forças navais. Estratégias de cibersegurança robustas são essenciais para proteger os sistemas de navios de guerra contra ataques, garantindo que eles possam operarcom eficácia em ambientes hostis.

Em resumo, as ações cibernéticas têm impactado diretamente os navios de guerra modernos, afetando sistemas de armas, sistemas de controle da plataforma e sistemas de comunicações via satélite. A dependência desses sistemas da cibernética tornaos navios de guerra vulneráveis a ataques cibernéticos que podem comprometer sua capacidade de combate e sua operabilidade. Portanto, a cibersegurança tornou-se uma preocupação crítica nas operações navais contemporâneas.

3 A GUERRA CIBERNÉTICA NA GUERRA DA UCRÂNIA: EXEMPLOS E IMPACTO

Este capítulo analisa o papel das ações cibernéticas na guerra em curso entre a Rússia e a Ucrânia, que teve início em 24 de fevereiro de 2022. O conflito é notório por seu uso extensivo de ataques cibernéticos, que incluem ataques preemptivos, ataques a sistemas satelitais de comando e controle, e ataques a infraestruturas críticas. Busca-se, com isso, examinar alguns exemplos significativos de ataques cibernéticos na guerra da Ucrânia e discutir o impacto dessas ações nas operações militares.

Ataques Cibernéticos Preemptivos: Um elemento notável da guerra da Ucrânia foi a ocorrência de ataques cibernéticos preemptivos por parte da Rússia. Antes da invasão militar, a Rússia lançou ataques cibernéticos com o objetivo de desabilitar a infraestru-

tura crítica e as operações militares ucranianas. Um exemplo desses ataques foi o ataque ao sistema de energia elétrica da Ucrânia em 23 de dezembro de 2021, que resultou em um apagão nacional (CARR; KOFMAN, 2022). Outro exemplo foi o ataque ao sistema de comunicação militar da Ucrânia em 13 de janeiro de 2022, que dificultoua coordenação das operações militares ucranianas (LEWIS, 2022).

- Impacto: Estes ataques preemptivos interromperam as operações militares ucranianas, prejudicando a capacidade de coordenação das forças armadas. Além disso, afetaram a população civil, causando apagões e dificultando a comunicação. Exemplos perfeitos de, respectivamente, ações táticas e estratégicas.

Ataques a Sistemas Satelitais de Comando e Controle: Os sistemas satelitais de comando e controle desempenham um papel crítico nas operações militares modernas, permitindo a coordenação precisa das forças. Durante a guerra da Ucrânia, houve rela- tos de ataques cibernéticos direcionados a esses sistemas, como o ataque ao sistema de GPS da Ucrânia em 24 de fevereiro de 2022 (CARR; KOFMAN, 2022).

- Impacto: O ataque ao sistema de GPS ucraniano dificultou a navegação das forças armadas ucranianas, resultando em erros táticos e estratégicos. Além disso, afetou a população civil, dificultando o deslocamento e a entrega de suprimentos.

Ataques a Infraestruturas Críticas: Os ataques a infraestruturas críticas da Ucrânia visaram causar danos econômicos e prejudicar o funcionamento do governo ucraniano. Um exemplo notável foi o ataque ao sistema de processamento de pagamentos da Ucrânia em 25 de fevereiro de 2022 (CARR; KOFMAN, 2022). Além disso, o sistema de transporte público de Kiev foi alvo de ataques em 26 de fevereiro de 2022 (LEWIS, 2022).

- Impacto: Esses ataques causaram danos econômicos significativos e prejudicaram a capacidade do governo ucraniano de funcionar. Além disso, afetaram a população civil, dificultando o acesso a serviços essenciais.

A guerra da Ucrânia evidencia a crescente importância das ações cibernéticas nos conflitos armados modernos. Os exemplos de ataques cibernéticos apresentados destacam o impacto significativo dessas ações nas operações militares. A cibernética tornou-se um componente crucial dos conflitos armados contemporâneos, exigindo estratégias de cibersegurança robustas e uma compreensão mais profunda das implicações desse domínio na guerra.

4 CONSIDERAÇÕES FINAIS

A estratégia de ataque preemptivo no ciberespaço, que envolve operações cibernéticas ofensivas contra adversários em potencial antes que eles possam lançar um ataque próprio, tem um impacto significativo na resiliência e na capacidade de resposta das forças militares em situações de conflito. Embora essa estratégia possa resultar na interrupção das capacidades militares do adversário e na obtenção de vantagens estratégicas, ela também apresenta riscos, incluindo a escalada do conflito.

Um dos principais benefícios dos ataques cibernéticos preemptivos é sua capacidade de desabilitar os sistemas do inimigo, prejudicando sua capacidade de comunicação, comando e controle, bem como sua moral. No entanto, essa estratégia também pode levar à escalada do conflito, à medida que o adversário pode retaliar, transformando o conflito cibernético em uma guerra convencional. Além disso, a distinção entre exploração e ataque cibernético pode ser tênue, o que gera desafios éticos e de segurança cibernética.

Os ataques cibernéticos representam uma ameaça direta aos sistemas de defesa militar e nacional, comprometendo infraestruturas críticas e prejudicando a eficácia das operações militares. A velocidade com que os ataques podem ocorrer e se propagar torna imperativa uma detecção e resposta rápidas. Para aumentar a resiliência, é necessário investir em cibersegurança robusta e melhorar a capacidade de detecção e resposta a ameaças cibernéticas.

Os ataques cibernéticos também podem minar a confiança das forças militares em seus próprios sistemas, levando à divisão de recursos para proteger esses sistemas. Isso pode afetar a eficácia operacional e a capacidade de resposta em situações críticas. Além disso, os ataques cibernéticos podem causar danos físicos diretos a sistemas e equipamentos militares, prejudicando ainda mais a capacidade de resposta em cenários de combate.

Concluindo, a estratégia de ataque preemptivo no ciberespaço é uma ferramenta poderosa, mas complexa, que afeta profundamente a resiliência e a capacidade de resposta das forças militares em conflitos contemporâneos. A integração das capacidades cibernéticas nas operações militares requer adaptação constante e investimentos em cibersegurança para enfrentar os desafios e maximizar os benefícios dessa estratégia na era digital.

REFERÊNCIAS

AMARAL, R. L.; LIMA, E. Estratégia nacional de defesa e a segurança cibernética. **Boletim de Ciências Geodésicas**, v. 21, n. 2, p. 250–271, 2015.

ARQUILLA, J.; RONFELDT, D. **The advent of netwar**. Santa Monica: RAND COR-PORATION, 1993.

ARQUILLA, J.; RONFELDT, D. **Athena's camp**: preparing for conflict in the infor-mation age. Santa Monica: Rand Corporation, 1997.

BIDDLE, S. **Military power**: explaining victory and defeat in modern battle. Princeton: Prin ceton University Press, 2004.

BRASIL. Ministerio da Defesa. **Doutrina de Operações Conjuntas.** Brasília, DF: MD, 2020.

BRASIL. Ministerio da Defesa. **Livro Branco de Defesa Nacional**. Brasília, DF: MD, 2020.

BROWN, C. Preemptive war and its justifications: a legal and ethical appraisal. *In*: HAYASHI, N.; KASTNER, L. A. (ed.). **Asian perspectives on ethics of justice**: towards the future. [*S. l.*]: Springer, 2017. p. 67–80.

CARR, J.; KOFMAN, M. Russia's cyberwar in ukraine: a preliminary assessment. **CSIS Briefs, Center for Strategic and International Studies (CSIS)**, v. 9, n. 3, p. 1-48, 2022.

CLARKE, R. A.; KNAKE, R. **Cyber war**: the next threat to national security and what to do about it. [*S. l.*]: HarperCollins, 2010.

CLAUSEWITZ, C. von. **Da Guerra**. [*S. l.*]: Edições 70, 1832.

DENNING, D. E. Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. *In*: KRAMER, R.; STARR, L. (ed.). **Cyberpower and National Security.** [Washington, DC]: National Defense University Press, 1999. p. 73–92.

GOURE, D. T. **Winning without fighting**: protecting against cyber weapons. [*S. l.*]: Le-xington Books, 2017.

JOHNSON, N. F. **Military strategy in the age of smart power**. [*S. l.*]: Routledge, 2018.

KAHN, D. **The Codebreakers**: the story of secret writing. [*S. l.*]: Scribner, 1967.

KUGLER, R. L.; KUGLER, J. The evolution of cyber operations and their contributionsto 21st century naval warfare. *In*: LAGHAD, P. R. S. (ed.). **Cyber Warfare and the Laws of War.** [*S. l.*]: Springer, 2019. p. 147-167.

LANG, A. F. Preemptive strikes: the legal basis revisited. **Max Planck Yearbook of United Nations Law**, v. 23, n. 1, p. 269–314, 2019.

LEWIS, J. A. **The use of cyberwarfare in the russian invasion of ukraine**. [*S. l.*]: Center for Strategic and International Studies, 2022.

LIBICKI, M. C. **Cyberdeterrence and Cyberwar**. Santa Monica: Rand Corporation, 2007.

LIBICKI, M. C. Cyberspace is not a warfighting domain. **Strategic Studies Quarterly**,v. 11, n. 3, p. 23–34, 2017.

MACHADO, A. A. A segurança de infraestruturas críticas no contexto da estratégia nacional de defesa. **Revista do Ministério Público Militar**, v. 25, n. 36, p. 191–210, 2018.

MAZANEC, B. M. Cybersecurity as a factor in grand strategy. *In*: MAZANEC, B. M. (ed.). **Cybersecurity and strategy**: from information to war. [*S. l.*]: Springer, 2018. p. 3-15.

MCGUIRE, M. Cyber threats to naval operations. **Naval War College Review**, v. 70, n. 4, p. 81–95, 2017.

RATTRAY, G. Strategic cyber war: A new domain of warfare. *In*: SCHMITT, M. N. (ed.). **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017. p. 487-506.

RICHELSON, J. T. **The U.S. Intelligence Community**. [*S. l.*]: Westview Press, 1995.

RID, T. Cyber war will not take place. **Journal of Strategic Studies**, v. 35, n. 1, p. 5-32, 2013.

ROCHA, L. G. Operações de informação no ciberespaço: uma análise do caso brasileiro. **Revista de Estudos de Defesa,** v. 11, n. 1, p. 123–145, 2019.

SAGAN, S. D. **The Limits of safety**: organizations, accidents, and nuclear weapons. Princeton: Princeton University Press, 1993.

SCHULZE, M. Cyber in war: assessing the strategic, tactical, and operational utility of military cyber operations. *In*: INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON), 12, 2020. **Proceedings** [...]. [*S. l.: s. n.*], 2020. p. 183–197. Disponível em: https://api.semanticscholar.org/CorpusID:220367060. Acesso em: 20 out. 2023.

SILVA, J. A. B. A segurança cibernética no Brasil: desafios e perspectivas. **Revista Tecnologia e Defesa**, v. 13, n. 2, p. 32–52, 2017.

SMITH, M. J. The role of information warfare in contemporary conflict. *In*: LENCZOWSKI, T. J. (ed.). **Informing statecraft**: intelligence for a new century. [*S. l.*]: Hoover Institution Press, 2019. p. 189–203.

TZANAKOPOULOS, A. The security council as authorizing agent for the use of force: 'preemptive' war and 'preemptive' self-defence. *In*: TOMUSCHAT, C.; TAMS, C. J. (ed.). **50 Years of the New York Convention**. [*S. l.*]: Brill, 2017. p. 79–104.

VALERIANO, B.; MANESS, R. C. **Cyber war versus cyber realities**: cyber conflict in the international system. Oxford: Oxford University Press, 2015.

ZEDONG, M. ***On Guerrilla Warfare***. Illinois: University of Illinois Press, 1961.