ESCOLA DE GUERRA NAVAL

CC(FN) RODRIGO CERQUEIRA GOMES

A GUERRA CIBERNÉTICA ENTRE RÚSSIA E UCRÂNIA, À LUZ DAS TEORIAS DE CLAUSEWITZ, PARTICULARMENTE ENTRE 2014 E 2022.

Rio de Janeiro

2024

CC(FN) RODRIGO CERQUEIRA GOMES

A GUERRA CIBERNÉTICA ENTRE RÚSSIA E UCRÂNIA, À LUZ DAS TEORIAS DE CLAUSEWITZ, PARTICULARMENTE ENTRE 2014 E 2022.

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF(RM1) Fabiano Rebello Cantarino

Rio de Janeiro

Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Documento assinado digitalmente
gov.br
RODRIGO CERQUEIRA GOMES
Data: 13/11/2024 17:59:44-0300
Verifique em https://validar.iti.gov.br

DEDICATÓRIA

Dedico este projeto ao meu orientador, meus instrutores e professores cujos ensinamentos e apoio foram cruciais para meu desenvolvimento.

Também gostaria de dedicar o trabalho aos meus colegas de turma, por seu companheirismo e troca de conhecimento, que enriqueceram minha experiência acadêmica.

Por fim, à minha família, por seu amor, apoio incondicional e incentivo constante, que me deram forças para seguir adiante.

AGRADECIMENTO

Com gratidão, agradeço a todos que contribuíram para a realização deste trabalho acadêmico.

Primeiramente, a Deus, por me conceder a sabedoria necessária para enfrentar os desafios e construir este conhecimento.

À minha família, que suportou minha ausência mesmo estando presente, e especialmente aos meus pais, que sempre apoiaram meu sucesso e conquistas.

Agradeço também aos meus colegas da turma Dodsworth, por sua colaboração e apoio constantes durante esta jornada.

Finalmente, expresso minha gratidão ao Corpo de Fuzileiros Navais e à Escola de Guerra Naval, pela confiança e apoio indispensável ao meu crescimento profissional e intelectual.

“Mesmo nas noites mais escuras, ainda há uma estrela brilhando. O desafio é encontrar essa luz e segui-la.”

Elie Wiesel

RESUMO

O objeto de pesquisa deste trabalho é investigar para melhor compreender se as teorias de Clausewitz continuam a ser relevantes no contexto da guerra moderna, particularmente na guerra cibernética. Apesar dos avanços tecnológicos que moldam os conflitos contemporâneos, os princípios fundamentais de Clausewitz permanecem inalterados. A “névoa da guerra” persiste na era da informação, exacerbada pelo excesso de dados que complicam a tomada de decisões. A identificação do “centro de gravidade”, pontos centrais de poder e movimento, é vital na estratégia militar moderna, tanto em termos de alvos tangíveis quanto intangíveis, como a opinião pública e a estabilidade política. A fricção é encontrada na complexidade e incerteza das operações, por meios da dificuldade de identificação da origem e extensão dos ataques. A proteção de infraestruturas críticas, como energia e comunicações, é crucial para a segurança de um Estado, refletindo a relevância contínua dos conceitos de Clausewitz. Eventos como BlackEnergy e NotPetya ilustram como esses princípios permanecem aplicáveis na era da informação. A integração de estratégias convencionais e cibernéticas sublinha a importância de Clausewitz na análise estratégica moderna. Portanto, as teorias de Clausewitz, longe de serem obsoletas, adaptaram-se e continuam fundamentais para a análise e a estratégia militar contemporânea. Elas não apenas preservam sua relevância, mas também ganham em profundidade com a incorporação de novas tecnologias e com a necessidade de uma abordagem estratégica completa, abrangendo tanto componentes tradicionais quanto cibernéticos. Dessa forma, a aplicabilidade duradoura das teorias de Clausewitz fortalece sua importância para o entendimento e a execução de operações militares no cenário atual de guerra cibernética.

Palavras-chave: Guerra Cibernética; Clausewitz; Névoa da Guerra; Fricção; Centro de Gravidade e Infraestruturas Críticas.

ABSTRACT

The Cyber Warfare between Russia and Ukraine, in light of Clausewitz's theories, particularly between 2014 and 2022

The research objective of this work is to investigate how Clausewitz's theories remain relevant in the context of modern warfare, particularly in cyber warfare. Despite the technological advances that shape contemporary conflicts, Clausewitz's fundamental principles remain unchanged. The "fog of war" persists in the information age, exacerbated by the overload of data that complicates decision-making. The identification of the "center of gravity," central points of power and movement, is vital in modern military strategy, encompassing both tangible and intangible targets, such as public opinion and political stability. Friction is encountered in the complexity and uncertainty of operations, including the difficulty of identifying the origin and extent of attacks. The protection of critical infrastructures, such as energy and communications, is crucial for the security of a state, reflecting the ongoing relevance of Clausewitz's concepts. Events like BlackEnergy and NotPetya demonstrate how these principles remain applicable in the information age. The integration of conventional and cyber strategies underscores the importance of Clausewitz in modern strategic analysis. Therefore, Clausewitz's theories, far from being obsolete, have adapted and remain essential to contemporary military analysis and strategy. They not only retain their relevance but also gain depth through the incorporation of new technologies and the need for a comprehensive strategic approach that encompasses both traditional and cyber components. In this way, the enduring applicability of Clausewitz's theories reinforces their importance for understanding and conducting military operations in the current context of cyber warfare.

Keywords: Cyber War; Clausewitz; Fog of War; Friction; Center of Gravity; Critical Infrastructures.

SUMÁRIO

1 INTRODUÇÃO

A partir da segunda metade do século anterior, a sociedade foi impactada pela evolução tecnológica associada à Tecnologia da Informação (TI), expondo pessoas, organizações e Estados mais vulneráveis a um novo tipo de ameaça: a cibernética (Túlio, 2016).

O ambiente atual dos conflitos modernos foi profundamente influenciado pela presença de civis e da mídia nas áreas de operações, por unidades de combate mais letais, pela utilização de veículos aéreos não tripulados controlados remotamente ou operados de forma autônoma e pela capacidade de conduzir operações no espaço cibernético (Túlio, 2016).

Neste cenário, quanto mais avançado tecnologicamente um Estado, maior sua vulnerabilidade à ameaça cibernética. A anexação da Crimeia pela Rússia em 2014 é um exemplo marcante de como a guerra cibernética foi integrada com operações militares tradicionais para alcançar objetivos geopolíticos específicos. Este evento salientou o papel do ciberespaço como uma frente operacional crucial, tanto para a coleta de inteligência quanto para a execução de operações que afetam diretamente a infraestrutura e a comunicação.

A Rússia empregou táticas cibernéticas, especialmente o *spear phishing*[1], para obter documentos e informações vitais da Ucrânia. Essas informações foram cruciais para compreender os planos econômicos e militares da Ucrânia, permitindo à Rússia antecipar e neutralizar movimentos ucranianos antes mesmo de serem implementados. Adicionalmente, houve um aumento significativo da propaganda pró-russa na internet, visando moldar a percepção pública e a narrativa sobre o conflito (Bateman, 2022).

Simultaneamente, operações cinéticas foram meticulosamente coordenadas com as ações no ciberespaço. Soldados russos, vestidos de civis, assumiram o controle de infraestruturas críticas, como torres de transmissão, estações de rádio e televisão na Crimeia, substituindo canais de comunicação ucranianos por russos. Isso alterou a informação disponível para a população local e desestabilizou a moral ucraniana (Mueller, 2023).

---

[1] Ataque direcionado a indivíduos específicos ou organizações, utilizando informações pessoais ou profissionais para enganar e obter dados sensíveis (Laboratório de Tecnologia da Informação, Centro de Recursos de Segurança de Informática)

Esse paradoxo destaca a característica mais marcante proporcionada pelas ações cibernéticas, que transcendem fronteiras físicas e geopolíticas. Seus atores podem ser estatais ou não e seus ataques podem resultar em significativos danos financeiros, paralisação de infraestruturas críticas, neutralização de sistemas militares e, indiretamente, até mesmo a perda de vidas (Túlio, 2016).

No âmbito militar, o tema é abordado de forma específica. Estados têm desenvolvido estratégias com suas Forças Armadas com o propósito de expandir suas capacidades operacionais e lidar com ameaças cibernéticas. Com isso, eleva-se o investimento em pessoal, tecnologia, processos e conhecimento para não apenas se defender de ataques cibernéticos, mas também para utilizar as técnicas e metodologias como parte integrante de sua capacidade operacional.

Atualmente, o emprego associado entre operações cibernética e operações convencionais está remodelando as estratégias militares, destacando sua crescente importância no panorama dos conflitos modernos. Essa interação entre as operações cibernéticas e as convencionais aprimora a eficácia das últimas, possibilitando uma abordagem mais coordenada e estratégica na condução dos conflitos.

Adicionalmente, as operações cibernéticas exigem menos recursos físicos e humanos em comparação com operações militares tradicionais reduzindo o risco de baixas e danos materiais.

Outro ponto relevante das operações cibernéticas é seu alcance global, pois podem ser conduzidas de praticamente qualquer lugar, afetando alvos em qualquer parte do mundo, ampliando o alcance estratégico de um país, sem a necessidade de utilização das forças no terreno.

Contudo, duas características relativamente novas das operações cibernéticas se destacam no contexto das estratégias militares tradicionais. A primeira é o alto grau de anonimato que os ataques cibernéticos proporcionam, o que dificulta a atribuição precisa da origem da ofensiva. Esse anonimato permite que os Estados utilizem táticas cibernéticas dentro de uma estratégia de “guerra nas sombras”, evitando as consequências políticas e diplomáticas que acompanhariam um ataque militar aberto. A segunda característica é a capacidade da guerra cibernética de afetar infraestruturas críticas, como redes elétricas, sistemas hídricos e de comunicação. Comprometer esses sistemas pode desestabilizar significativamente a segurança nacional, impactar a economia e afetar a saúde da

população do país atacado, ampliando assim o espectro de influência e controle em um conflito moderno.

Essas duas perspectivas podem ser comparadas, respectivamente, à “névoa da guerra” e ao “centro de gravidade” descritos por Clausewitz. A “névoa da guerra” refere-se à confusão e incerteza que predominam no campo de batalha, paralelo ao anonimato dos ataques cibernéticos que obscurece a identificação da origem das ofensivas. Já o “centro de gravidade”, que Clausewitz define como o ponto mais importante que sustenta toda a estrutura de força do adversário, se assemelha à capacidade da guerra cibernética de atingir e paralisar infraestruturas críticas, atacando assim o coração das capacidades de um Estado.

1.1 A INTEGRAÇÃO DA GUERRA CIBERNÉTICA NAS OPERAÇÕES MILITARES.

A importância da guerra cibernética nas operações militares modernas é indiscutível. Ela desempenha um papel crítico não só fornecendo suporte direto ao combate, mas também ampliando os efeitos das operações convencionais. As operações cibernéticas podem preceder e intensificar ações cinéticas no Teatro de Operações, configurando o ambiente de batalha de maneira que aumenta substancialmente as chances de sucesso em conflitos. Assim, a capacidade de executar uma guerra cibernética eficaz tornou-se um componente fundamental da doutrina militar moderna, refletindo o cenário de guerra híbrida que caracteriza o século XXI.

Em agosto de 2008, a Rússia interveio no conflito entre Geórgia e Ossétia do Sul, a favor desta última, declarando guerra contra a Geórgia. Sem grande surpresa, o exército russo expulsou rapidamente as forças georgianas da Ossétia do Sul, no dia seguinte.

Antes mesmo que os confrontos físicos começassem, o governo da Geórgia já sofria com ataques de *Distributed Denial of Service*[2] (DDoS) contra meios de

[2] Tipo de ataque cibernético em que vários dispositivos, frequentemente infectados por malware, que são usados para sobrecarregar um sistema-alvo com um volume excessivo de solicitações. Esse tráfego massivo dificulta ou impede que o sistema responda a usuários legítimos, resultando em uma negação de serviço. Ataques DDoS são comumente direcionados a sites, servidores ou redes, causando interrupções temporárias ou até mesmo a indisponibilidade completa dos serviços afetados. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Glossary of key information security terms*. Disponível em: https://csrc.nist.gov/glossary. Acesso em: 13 nov. 2024.

comunicação e *websites* governamentais que atingiram principalmente o servidor web do site presidencial. Os georgianos enfrentaram dificuldades para acessar sites internacionais de notícias como CNN e BBC, além de estarem impedidos de enviar e-mails para o exterior. À medida que o confronto terrestre intensificava-se, também aumentava a intensidade e a sofisticação dos ataques cibernéticos.

A Geórgia foi forçada a deslocar seus *websites* governamentais para servidores em outros países. Em um esforço para se proteger, tentou bloquear todo o tráfego de internet vindo da Rússia, mas os atacantes russos adaptaram suas estratégias, fazendo os ataques parecerem originários da China, Canadá, Turquia e Estônia. Por outro lado, o setor bancário georgiano optou por desligar seus servidores como medida preventiva, julgando que a perda temporária de acesso ao sistema bancário online era preferível ao risco de roubo de dados críticos ou danos internos.

Segundo Sarah P. White, da Modern War Institute, West Point, a Guerra da Geórgia é amplamente reconhecida como um dos primeiros exemplos claros onde a guerra cibernética foi utilizada de forma integrada com operações militares tradicionais. Este conflito ilustra um ponto de inflexão na condução da guerra, evidenciando a interdependência entre ações cinéticas (físicas) e não cinéticas (cibernéticas) no Teatro de Operações.

A anexação da Crimeia pela Rússia em 2014 é um exemplo marcante de como a guerra cibernética foi integrada com operações militares tradicionais para alcançar objetivos geopolíticos específicos. Este evento destacou o papel do ciberespaço como uma frente operacional crucial, tanto para a coleta de inteligência quanto para a execução de operações que afetam diretamente a infraestrutura e a comunicação (Mueller, 2023).

Segundo Jon Bateman, em seu artigo *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications* publicado pela Carnegie Endowment for International Peace, as operações cibernéticas da Rússia desempenharam um papel crucial no apoio às operações de informação e propaganda, buscando minar o apoio à Ucrânia e influenciar a percepção global do conflito. Além disso, o Centro de Estudos Estratégicos e Internacionais (CSIS) destaca que essas operações cibernéticas foram usadas para espionagem e coleta de inteligência, o que ajudou a Rússia a se preparar para suas ações militares (CSIS, 2022).

Simultaneamente, operações cinéticas foram meticulosamente coordenadas com as ações no ciberespaço. As forças russas isolaram a Crimeia do restante do território ucraniano, cortando comunicações terrestres, diminuindo a capacidade de comando e controle da Ucrânia sobre a península (Mueller, 2023).

Como resultado, a população da Crimeia ficou praticamente isolada, mantendo comunicação apenas com os russos. Este isolamento contribuiu para facilitar a anexação da região pela Rússia, demonstrando como a guerra cibernética pode complementar e potencializar operações militares convencionais, redefinindo o cenário de conflitos modernos (Mueller, 2023).

Desde a anexação da Crimeia em 2014 até o início da invasão da Ucrânia continental pela Rússia em 2022, a relação entre esses dois países foi caracterizada por uma série de eventos significativos no ciberespaço. Estes eventos demonstraram que o impacto do avanço tecnológico não está restrito a vida em sociedade, mas também evidenciaram a evolução das capacidades cibernéticas de ambos os atores. Essa dinâmica reforçou a realidade de uma arena digital em constante expansão, onde confrontos tecnológicos desempenham um papel cada vez mais central nas relações internacionais.

1.2 PROBLEMA A SER PESQUISADO, HIPÓTESE E DELIMITAÇÃO TEMPORAL

Os fatos até aqui apresentados despertaram o interesse em aprofundar nossa pesquisa sobre a importância crescente do “quinto domínio”, o ciberespaço, nos conflitos contemporâneos. Este trabalho focará na integração das novas capacidades cibernéticas dos Estados com as estratégias de guerra convencionais, explorando como elas estão transformando a dinâmica e os resultados dos conflitos modernos.

Diante disso, surge o seguinte problema: a teoria de Carl von Clausewitz está ultrapassada no contexto das operações militares contemporâneas, considerando as mudanças decorrentes dos avanços tecnológicos? Nossa hipótese inicial é que as teorias de Clausewitz continuam relevantes e aplicáveis, mesmo em contextos de crescente emprego da guerra cibernética.

Assim, este trabalho se dedica a explorar detalhadamente a guerra cibernética entre Rússia e Ucrânia sob a perspectiva das teorias de Clausewitz,

particularmente no período de 2014 a 2022[3], investigando se as estratégias e táticas adotadas durante o conflito corroboram ou contrapõem os conceitos tradicionais de guerra propostos pelo teórico prussiano.

Para que ao final possamos chegar a uma solução do problema proposto, este trabalho será dividido da seguinte maneira:

O primeiro capítulo será composto por uma breve Introdução.

O Capítulo 2 abordará algumas das teorias de Clausewitz aplicadas às guerras modernas, com o objetivo de identificar sua evolução ao longo do tempo. Conceitos como a natureza da guerra e suas ações recíprocas, a névoa da guerra inerente às dinâmicas dos conflitos contemporâneos, e a evolução do centro de gravidade, que agora inclui infraestruturas críticas e o ciberespaço, serão discutidos. Nesse contexto, a fricção adquire uma nova conotação com a introdução de tecnologias cibernéticas.

O Capítulo 3 apresenta uma breve evolução da guerra cibernética desde o fim da Guerra Fria até os dias atuais. A abordagem será restrita aos atores Rússia e Ucrânia, com o objetivo de orientar o leitor sobre a evolução tecnológica desses países e explicar suas diferentes posturas em relação às ações cibernéticas.

No Capítulo 4, serão analisados alguns acontecimentos cibernéticos ocorridos entre a Rússia e a Ucrânia, de forma a permitir ao leitor identificar as teorias de Clausewitz e confirmar sua aplicação nos conflitos modernos.

Por último, a Conclusão do trabalho apresentará uma possível solução para o problema proposto, com base nos dados apresentados até o momento. A parte final não pretende esgotar o assunto, destacando que o conflito escolhido ainda está em andamento enquanto o autor escreve. Portanto, é provável que novos eventos surjam até o término do conflito, proporcionando uma compreensão mais aprofundada e relevante das teorias de Clausewitz na análise dos conflitos modernos.

[3]Considerando que o conflito continua em andamento, nossa análise será limitada aos eventos ocorridos até o ano de 2022 buscando entender como os princípios de Clausewitz são evidenciados em um contexto marcado por conflitos digitais e tecnológicos.

2 DAS TEORIAS DE CLAUSEWITZ ÀS GUERRAS CONTEMPORÂNEAS

Neste capítulo, exploraremos algumas das ideias fundamentais de Carl Von Clausewitz, sem pretender abordar sua obra de maneira completa. O objetivo não é esgotar todos os aspectos da teoria do filósofo militar, nem atualizar totalmente sua obra, mas utilizar seus conceitos como base para uma comparação com os elementos característicos das guerras modernas e futuras. Focaremos em selecionar e discutir as características mais marcantes de suas teorias, especialmente aquelas que se mostram relevantes e pertinentes ao analisar os cenários de conflito contemporâneo e emergente.

2.1 A GUERRA, AÇÕES RECÍPROCAS E SEUS EXTREMOS.

A complexidade da obra de Clausewitz é reconhecida, e muitos dos seus conceitos são incrivelmente relevantes para a compreensão da guerra moderna. (Clausewitz, 1979). Neste contexto, o autor desse trabalho destaca como essas teorias clássicas continuam aplicáveis e influentes, demonstrando que, longe de estarem ultrapassadas, elas oferecem *insights* valiosos para entender a natureza dos conflitos atuais (Mahnken, 2010).

Inicialmente, consideraremos a definição de Clausewitz: “A guerra é, pois, um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade” (Clausewitz, 1979).

A partir desta definição, analisaremos de forma individualizada as ações recíprocas e suas condições extremas e, para aprimorar a compreensão, realizaremos uma análise integrada entre esses conceitos (Clausewitz, 1979). Contudo, devido à natureza mutável da guerra e sua habilidade para se ajustar ao tempo, é vital analisar as teorias de Clausewitz tanto em seus elementos isolados quanto em sua estrutura conjunta (Clausewitz, 1979).

Apesar das consideráveis mudanças associadas ao desenvolvimento tecnológico que definem e moldam os conflitos bélicos contemporâneos, a intenção de destruir o inimigo não foi minimizada ou abrandada por esse progresso. (Clausewitz, 1979). Percebe-se que, através dos tempos, persiste a noção de que a guerra é intrinsecamente um ato de violência e que não existem limites para como essa violência pode se manifestar (Clausewitz, 1979). Cada lado do conflito impõe

essa verdade ao outro, resultando em uma ação recíproca que, em teoria, deve se estender até os extremos. É assim que nos confrontamos com a primeira ação recíproca e os extremos iniciais (Clausewitz, 1979).

Na segunda ação recíproca e seu extremo, as partes beligerantes de uma guerra sempre almejam impor suas próprias vontades ao adversário (Clausewitz, 1979). Isso caracteriza a guerra como uma ação entre forças ativas que buscam prevalecer suas vontades contra o oponente com o propósito de que ele se renda por ser obrigado a assumir uma posição desfavorável (Clausewitz, 1979).

Analisando a terceira ação recíproca e seu respectivo extremo, a vitória sobre o adversário é resultado do emprego de um esforço proporcional à sua resistência (Clausewitz, 1979). Esse esforço é o produto de dois fatores: a extensão de meios de que dispõe o adversário e a firmeza de sua vontade (Clausewitz, 1979). Neste contexto, a abordagem de Clausewitz visa dimensionar esses dois fatores de maneira quantitativa e qualitativa, respectivamente.

Atualmente, o fator denominado “extensão de meios de que dispõe o adversário” não se traduz necessariamente em quantidade numérica mas, ao combinar com o que Clausewitz chamou de “firmeza de vontade”, surge uma associação onde o primeiro se transformou em amplitude tecnológica dos meios e o segundo, na capacidade e vontade de empregar essa tecnologia em combate contra seus adversários.

Ao analisar em conjunto as ações recíprocas descritas e considerando um contexto em que elas são empregadas simultaneamente em um ambiente conflituoso atual, é plausível considerar, na teoria, que o oponente será conduzido a uma situação desvantajosa (Clausewitz, 1979). Essa situação desvantajosa não pode ser temporária, pois o adversário esperaria até que a situação lhe fosse favorável novamente. O objetivo é, portanto, que a situação incômoda seja duradoura e que cada ação executada pelo adversário contribua significativamente para o conduzi-lo, cada vez mais, para essa posição de desvantagem, agravando sua situação (Clausewitz, 1979). É essencial buscar colocá-lo em situações ou condições difíceis para que ele se sinta constantemente ameaçado forçando o adversário a executar a nossa vontade (Clausewitz, 1979).

A guerra nunca irrompe de maneira súbita, e sua evolução não é obra de um instante. A guerra nunca se baseia em um ato isolado, nem consiste em um único e instantâneo golpe de força (Clausewitz, 1979). Uma guerra é, em sua essência, o

reflexo dos resultados obtidos por meio de uma série de ações sucessivas que exploram as situações favoráveis oriundas de ações anteriores. Ou seja, a guerra se vale de ações complementares e simultâneas, no tempo e no espaço, e nos fornece uma ampla noção de que uma ação deve ser orientada conforme os resultados obtidos (Clausewitz, 1979).

Ainda, há de se considerar que “a reunião perfeita de todas as forças num mesmo momento é contrária à natureza da guerra” (Clausewitz, 1979). Mas isso não constitui um motivo para diminuir a intensidade dos esforços direcionados a obter vantagem no ataque. Verifica-se, portanto, uma tendência natural de realizar um faseamento de uma guerra, que se traduz superficialmente, como a ação tomada, observação dos resultados obtidos e ação subsequente (Clausewitz, 1979).

2.2 NÉVOA DA GUERRA: INCERTEZA DAS DINÂMICAS DA GUERRA MODERNA

Um conceito que continua a ser fundamental para entender a teoria e prática da guerra é a ideia de “névoa da guerra” que, segundo Clausewitz, é explicada da seguinte forma:

> A guerra é o domínio da incerteza. Três quartos dos fatores em que se baseiam os combates na guerra estão envoltos numa névoa de maior ou menor incerteza. É necessário um discernimento sensível e perspicaz e uma exímia inteligência para descobrir a verdade.(Clausewitz, 1979).

Na era da informação, a “névoa da guerra” não desapareceu, mas intensificou-se devido à introdução de novas tecnologias como drones, satélites, sistemas de inteligência artificial e a capacidade cibernética, que proporcionam uma grande quantidade de dados disponíveis e transformam o campo de batalha moderno (Liles, 2012). A sobrecarga de informações geradas pelas inovações tecnológicas molda a incerteza no campo de conflito, onde a dificuldade é discernir informações precisas e úteis em meio a um mar de dados potencialmente enganosos ou irrelevantes. Além de introduzir novas camadas de incerteza, o desenvolvimento tecnológico se tornou uma grande arma (Proença Jr, 2011) quando empregado com o propósito de afetar infraestruturas críticas[4] sem efetivamente o

[4]As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico

desencadeamento de um confronto físico direto, desafiando as normas tradicionais de engajamento.

No ambiente de guerra contemporâneo, a necessidade de tomar decisões rápidas com informações incompletas é uma realidade constante, impulsionada pela velocidade vertiginosa das operações modernas. Este cenário exige o gerenciamento das incertezas e o desenvolvimento de estratégias adaptativas para lidar com a imprevisibilidade do combate (Teixeira; Júnior; Lopes; Freitas, 2017).

O conceito de Clausewitz sobre a “névoa da guerra” continua sendo muito relevante no ambiente de guerra contemporânea. As tecnologias avançadas e a natureza rápida dos conflitos modernos intensificam a necessidade de desenvolver estratégias adaptativas para lidar com a imprevisibilidade do combate (Peron, 2016).

2.3 A EVOLUÇÃO DO CENTRO DE GRAVIDADE NOS CONFLITOS MODERNOS

Clausewitz definiu Centro de Gravidade como o ponto central de todo o poder e movimento, do qual tudo depende (Clausewitz, 1979). Atualmente, considerando o cenário internacional dominado por inovações tecnológicas, identificar e neutralizar o Centro de Gravidade oponente pode envolver operações que vão além do campo de batalha convencional (Clausewitz, 1979). Os atuais conflitos são frequentemente abordados segundo o conceito de Guerra Híbrida[5] (Brasil, 2016).

Assim, o sucesso das operações militares no século XXI depende não apenas da capacidade de mobilizar e concentrar forças, mas também de identificar e atacar os centros nevrálgicos do inimigo (Clausewitz, 1979). Estes centros podem ser tangíveis, como instalações urbanas estratégicas, centros de comando e controle, e infraestruturas logísticas, ou intangíveis, como a opinião pública, a estabilidade política, e os sistemas de comunicação e informação. A estratégia contemporânea,

---

sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente (Decreto nº 10.569, de 9 de dezembro de 2020 – Planalto).

[5] Conceito cada vez mais adotado para descrever os novos conflitos do século XXI, muitas vezes chamados de “conflitos do futuro”. Esses conflitos combinam, no tempo e no espaço, ações de combate convencional com operações de natureza irregular, guerra cibernética e operações de informação, entre outras. Envolvem tanto atores estatais quanto não-estatais, operando em ambientes reais e informacionais, incluindo redes sociais. A natureza da Guerra Híbrida destaca as características complexas dos conflitos contemporâneos, tornando as missões das Forças Armadas muito mais complexas, dinâmicas e sofisticadas (Brasil, 2016).

portanto, deve ser capaz de discernir esses centros, reconhecendo que a destruição ou desestabilização dos mesmos pode paralisar a capacidade operacional do adversário mais efetivamente do que a destruição de suas forças convencionais.

> A condição fundamental, entretanto, não consiste meramente na maior concentração de forças possível. Elas devem ser dispostas também de modo a permitir que possam combater em circunstâncias suficientemente favoráveis. [...] É, portanto, um grande ato de discernimento estratégico distinguir estes centros de gravidade das forças do inimigo e identificar as suas esferas de eficácia (Clausewitz, 1979).

A potencialização do conceito de Centro de Gravidade no ambiente contemporâneo reforça a necessidade de uma estratégia militar sustentada em uma rápida adaptação às mudanças no campo de batalha e na eficácia na utilização de todos os recursos disponíveis para identificar o Centro de Gravidade do adversário (Clausewitz, 1979). Essa nova abordagem da estratégia militar implica a utilização coordenada e simultânea de ações cinéticas e não-cinéticas para exercer uma influência mais efetiva e abrangente sobre o conflito (Clausewitz, 1979).

Portanto, o conceito de Centro de Gravidade tornou-se mais abrangente devido às inovações tecnológicas e complexidades dos conflitos modernos (Limell, 2015). A identificação precisa dos centros de gravidade em uma guerra contemporânea e a aplicação de forças de maneira cirúrgica e estratégica contra esses pontos podem determinar o sucesso ou o fracasso de operações militares (Clausewitz, 1979).

2.4 UMA NOVA CONCEPÇÃO DE FRICÇÃO

Carl von Clausewitz descreve a fricção como a força que transforma a guerra em uma realidade mais complexa, difícil e desgastante do que sua definição teórica. É o único conceito que contém características que distinguem a guerra real da guerra no papel (Clausewitz, 1979).

Ainda, segundo Clausewitz, a máquina militar é composta por componentes, cada um dos quais contém o seu potencial de fricção" (Clausewitz, 1979).

Transportando as considerações de Clausewitz para os dias de hoje, o conceito de fricção pode ser relacionado ao contexto das guerras modernas de várias maneiras, principalmente considerando fatores que dificultam a tomada de decisão como a complexidade, incerteza e imprevisibilidade das operações militares.

Atualmente, as forças armadas dependem fortemente de sistemas avançados de comando, controle, comunicações, computadores, inteligência, vigilância e reconhecimento (C4ISR). Dentro desse contexto, é justo afirmar que esses sistemas são os componentes das guerras modernas e, embora possam aumentar a eficácia, eles também introduzem novas formas de fricção, como falhas técnicas, ataques cibernéticos, dificuldades de integração entre diferentes tecnologias e a necessidade de treinamento especializado.

A incerteza inerente ao campo de batalha, também chamada de Névoa da Guerra*,* onde informações incompletas ou contraditórias são comuns, materializa uma fonte significativa de fricção. Além disso, as campanhas de desinformação podem desmoralizar tropas, confundir o público e enganar os líderes militares sobre a situação no campo de batalha.

Assim, a alta intensidade de fricção, junto a novas modalidades causadas pela evolução tecnológica, destacam a natureza complexa e imprevisível da guerra. Isso aumenta as incertezas no campo de batalha, causando surpresas e dificuldades nas operações.

A fricção na guerra moderna assume uma característica fundamental nos conflitos armados. Compreender e gerenciar essa fricção é essencial para o sucesso das operações militares de hoje. Adaptar-se rapidamente, integrar sistemas complexos e manter o moral das tropas são fatores decisivos para superar as inevitáveis fricções da guerra.

2.5 A IMPORTÂNCIA DAS INFRAESTRUTURAS CRÍTICAS.

Embora Carl von Clausewitz não tenha usado especificamente o termo “infraestrutura crítica” em sua obra, ele apresenta conceitos fundamentais para a compreensão do termo dentro do contexto das guerras modernas. A interpretação atual do termo abrange setores importantes como: energia, água e saneamento, transporte, comunicações, saúde e financeiro. Em tempos de guerra, a proteção e o ataque a essas infraestruturas críticas podem ter um impacto significativo nas capacidades militares e civis de um país. A abordagem de Clausewitz para a proteção de fortificações, depósito de suprimentos e cidades pode ser aplicada à proteção do que chamamos atualmente de infraestruturas críticas, destacando a

importância de garantir que essas instalações estejam bem defendidas e possam operar de forma resiliente em face de ataques.

> “A perda de uma fortificação enfraquece a defesa do inimigo, principalmente quando ela constituir uma parte essencial desta defesa. A sua ocupação proporciona vários benefícios ao atacante. Ele pode utilizá-la como um armazém ou depósito, para proteger a região e os seus alojamentos, e assim por diante” (Clausewitz, 1979).

Ainda, de acordo com o teórico militar, "[…] as cidades grandes e prósperas, principalmente as comerciais, são as fontes naturais de suprimentos de um exército, que será diretamente afetado, portanto, pela sua posse ou pela sua perda." (Clausewitz, 1979). Trazendo a descrição anterior para o contexto atual, os modernos conglomerados urbanos, de onde emanam significativos poderes econômicos, políticos e comerciais, também afetam diretamente a postura de um Estado em uma guerra. Dessa forma, a proteção dessas importantes cidades pode ser vista como uma analogia à proteção de infraestruturas críticas.

Estes pontos destacam a complexidade e a criticidade das infraestruturas críticas no contexto das operações militares modernas. A proteção dessas infraestruturas é fundamental para a segurança do Estado, exigindo uma abordagem integrada e coordenada entre diversos atores e setores.

3 A EVOLUÇÃO DA GUERRA CIBERNÉTICA

Este capítulo tem como propósito traçar a evolução da guerra cibernética, desde suas origens no desenvolvimento da tecnologia da informação e das comunicações até seu emprego no conflito entre Rússia e Ucrânia. O capítulo mostra como esses avanços tecnológicos, combinados com eventos históricos como a Guerra Fria e o surgimento de *malware*[6], moldaram o cenário das operações cibernéticas. Além disso, discute a importância estratégica crescente dessas operações no contexto do conflito entre Rússia e Ucrânia, destacando a complexidade e sofisticação crescente da guerra cibernética como uma dimensão essencial das estratégias militares modernas.

A origem e a evolução das operações de guerra cibernética estão intrinsecamente ligadas ao desenvolvimento da tecnologia da informação e das comunicações, especialmente a partir da segunda metade do século XX. Este campo complexo e dinâmico tem raízes profundas que remontam a vários marcos históricos e tecnológicos (Edelman, 2024).

Nas décadas de 1960 e 1970, a criação dos primeiros computadores e redes de comunicação, como a ARPANET[7] (precursora da Internet), trouxe consigo as primeiras preocupações com a segurança da informação. Esses avanços iniciais destacaram o potencial para a realização de ataques cibernéticos à medida que a interconectividade aumentava (Egloff, 2022).

Durante a Guerra Fria (1947-1991), a competição tecnológica entre os Estados Unidos e a ex-União Soviética impulsionou o desenvolvimento de técnicas de espionagem e sabotagem cibernética. Ambas as superpotências exploraram o uso de tecnologias de informação para interceptar e manipular comunicações eletrônicas, reconhecendo a importância estratégica dessas capacidades. Nesse contexto, a vitória nesse confronto bipolar seria o resultado de uma antecipação tecnológica estadunidense (Brzezinski,1989). A percepção de Brzezinski (1989) sobre o fim da União das Repúblicas Socialistas Soviéticas (URSS) vai ao encontro

[6] *Software* ou *firmware* destinado a executar um processo não autorizado que terá impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação (https://csrc.nist.gov/glossary/term/malware).

[7] Advanced Research Projects Agency Network, foi a primeira rede operacional de comutação de pacotes. Desenvolvida pela Agência de Projetos de Pesquisa Avançada de Defesa dos Estados Unidos, a ARPANET tinha como objetivo facilitar a comunicação entre instituições de pesquisa e compartilhar recursos computacionais caros e escassos. (https://www.britannica.com/topic/ARPANET).

com uma transformação significante nas relações internacionais: a revolução da informação

Na década de 1980, a emergência de vírus de computador e outras formas de *malware* evidenciou o potencial destrutivo de ataques cibernéticos. Isso evidenciou as vulnerabilidades dos sistemas de computação e despertou uma maior conscientização sobre a necessidade de segurança cibernética (Alam, 2022).

Nos anos 1990, conflitos como a Guerra do Golfo Pérsico (1990-1991) e as Guerras Iugoslavas[8] (1991-1999) marcaram os primeiros usos de ataques cibernéticos em operações militares. A manipulação de comunicações e redes de computadores inimigas começou a ser explorada, ainda que de forma incipiente (Rovner, 2021).

O início dos anos 2000 viu a formalização das operações cibernéticas com a criação de unidades militares especializadas. Em 2009, por exemplo, o Departamento de Defesa dos EUA estabeleceu o Comando Cibernético dos Estados Unidos (USCYBERCOM) para coordenar e conduzir operações cibernéticas, destacando a crescente importância dessa dimensão de guerra (USCYBERCOM, 2018).

3.1 A ASCENSÃO DA GUERRA CIBERNÉTICA NO SÉCULO XXI.

Ataques como o *Stuxnet*[9] em 2010, que visou instalações nucleares iranianas, demonstraram o poder devastador de operações cibernéticas bem-sucedidas (Alvarez, 2015). Atribuído aos Estados Unidos e a Israel, marcou um ponto de inflexão ao evidenciar que ataques cibernéticos poderiam causar danos físicos significativos a infraestruturas críticas (Zetter, 2014).

Ao longo da década de 2010, as operações de guerra cibernética tornaram-se cada vez mais sofisticadas e internacionalizadas. Países de todo o mundo desenvolveram capacidades ofensivas e defensivas no ciberespaço materializando o emprego estratégico das operações cibernéticas para atingir objetivos políticos e

[8] Guerra da Eslovênia (1991), Guerra da Croácia (1991-1995), Guerra da Bósnia (1992-1995) e Guerra do Kosovo (1998-1999) (Baker, 2015).

[9] Malware descoberto em 2010, projetado para atacar sistemas industriais, especificamente as centrífugas do programa nuclear iraniano. É reconhecido como a primeira arma cibernética que causou danos físicos a infraestruturas críticas. Desenvolvido possivelmente por Estados Unidos e Israel, Stuxnet se infiltrou nas redes industriais, alterando o funcionamento das centrífugas e danificando-as enquanto reportava operações normais aos sistemas de monitoramento. (Clarke, Knake, 2015).

econômicos. Atualmente, o emprego dos meios cibernéticos, combinados aos meios convencionais de força materializam um binômio decisivo empregado na condução de um conflito (Langner, 2011).

Considerando todo o processo de evolução e a importância atual, pode-se definir guerra cibernética como o emprego ofensivo e defensivo de informações e sistemas de informação para comprometer a capacidade de comando e controle (C2) do adversário (Sheldon, 2013). Isso inclui ações como exploração, negação, corrupção, degradação ou destruição de dados e sistemas de informação, visando proteger as infraestruturas críticas e garantir a segurança nacional no ambiente cibernético. Devido à sua importância, alguns teóricos contemporâneos afirmam que as ações cibernéticas desempenham o papel de uma poderosa arma estratégica, com efeitos de dissuasão comparáveis aos das armas nucleares (Krepinevich, 2012).

Diante do processo histórico, da definição, do campo de atuação e das múltiplas possibilidades de emprego, a evolução das armas tecnológicas evidencia claramente sua importância crucial no cenário bélico atual.

Entretanto, mesmo que a guerra cibernética possibilite alcançar a vitória militar com menor uso efetivo de força, reduzindo o emprego de energia cinética nos conflitos, ela ainda não possui a capacidade de influenciar decisivamente no resultado de um conflito.

3.2 O EMPREGO DA GUERRA CIBERNÉTICA ENTRE RÚSSIA E UCRÂNIA.

No cenário contemporâneo, a guerra cibernética surge como uma ferramenta pertencente a um outro domínio, o ciberespaço[10], mas só produz resultados consideráveis quando somada ou potencializada por meios de emprego militar convencional (Teixeira Júnior; Lopes; Freitas, 2017).

Percebe-se assim uma conexão entre ciberespaço e uso da força concretizando a concepção de “armas combinadas” que, segundo House (2008), define-se como uma ideia básica na qual diferentes armas e sistemas de armas

[10] Constitui um dos cinco domínios operacionais e permeia os demais: o terrestre, o marítimo, o aéreo e o espacial. Esse domínio pode alavancar as capacidades de todos os outros, e a combinação dos meios e a convergência de esforços tornam-se indispensáveis para que seja obtido o máximo rendimento das forças disponíveis (EB70-MC-10.232, Manual de Campanha de Guerra Cibernética, 1ª Edição, 2017).

devem ser usados em conjunto para elevar a eficácia em combate de cada uma. Assim, a combinação entre a tecnologia cibernética e o uso de força convencional possibilita e aumenta a probabilidade de conquista dos objetivos militares.

É imperativo a existência de uma estratégia comum que combine armas convencionais e cibernéticas, não apenas no sentido ofensivo, mas também no preventivo, confirmando assim a natureza subsidiária do domínio cibernético em relação aos demais (Libicki, 2012).

Nesse contexto, a Rússia destaca-se como um ator capaz de combinar o emprego da guerra cibernética com armas convencionais. Esse fato é resultado de sua presumida experiência que teve origem após a Guerra Fria, com o processo de transformação militar liderada pelos EUA (Sloan, 2012).

Por outro lado, conforme Temnycky (2021), a Ucrânia tornou-se alvo constante de ataques cibernéticos, especialmente após o aumento das tensões com a Rússia em 2014. Esses ataques visavam infraestruturas críticas e incluíam campanhas de desinformação, sublinhando o uso do ciberespaço como extensão dos conflitos tradicionais. Em resposta, a Ucrânia fortaleceu sua defesa cibernética.

Percebe-se, portanto, que os fatos descritos acima refletem uma postura híbrida com ações de ataques e defesas cibernéticos, ilustrando a complexidade do confronto contínuo entre Rússia e Ucrânia no ciberespaço. Principalmente a partir de 2014, a Rússia tem coordenado ataques cibernéticos simultâneos a operações militares convencionais, enquanto a Ucrânia tem fortalecido suas capacidades defensivas, demonstrando como a guerra cibernética complementa e intensifica os conflitos contemporâneos entre os dois países.

4 ANÁLISE DAS AÇÕES CIBERNÉTICAS ENTRE RÚSSIA E UCRÂNIA (2014-2022), À LUZ DE CLAUSEWITZ

Este capítulo examina algumas das principais ações cibernéticas executadas no âmbito do conflito entre Rússia e Ucrânia, de 2014 a 2022, à luz das perspectivas teóricas de Clausewitz sobre Névoa da Guerra, Centro de Gravidade, Fricção e Infraestruturas Críticas, destacando as estratégias, táticas e impactos dessas ações.

Inicialmente, é importante ressaltar que o conflito ainda está em andamento e que este trabalho aborda alguns fatos ocorridos na moldura temporal de análise, comprovados e divulgados até o presente momento. Devido à continuidade do conflito, futuras revelações poderão evidenciar ações mais relevantes que possam suplantar os exemplos aqui citados. Apenas o tempo poderá revelar se ocorreram outras ações mais significativas no contexto do referido conflito.

Entretanto, mesmo considerando que o conflito entre Rússia e Ucrânia, ainda não terminou, a moldura temporal de 2014 a 2022 permite analisar as ações cibernéticas de ambos os países. Nesse contexto, observamos comportamentos distintos entre os atores envolvidos. A Rússia, com uma capacidade cibernética mais avançada e consolidada, manteve a iniciativa em ações ofensivas no domínio cibernético. Em contraste, a Ucrânia adotou uma postura defensiva e reativa devido à sua desvantagem tecnológica, apesar da ajuda recebida de países ocidentais, especialmente dos aliados da OTAN.

A crise na Ucrânia começou em 2013 com protestos em massa que levaram à deposição do presidente pró-Rússia Viktor Yanukovych. Em 2014, a Rússia anexou a Crimeia[11], o que desencadeou um conflito armado no leste da Ucrânia. Paralelamente ao conflito militar, a guerra cibernética emergiu entre Rússia e Ucrânia como uma ferramenta crucial para ambas as partes e parte fundamental do conflito mais amplo entre os dois países (Lewis, 2022).

[11] A Crise da Crimeia de 2014 ocorreu entre 23 de fevereiro e 28 de março, resultando na anexação da Crimeia pela Rússia. O conflito começou após a destituição do presidente ucraniano Viktor Yanukovych, levando a protestos e tensões entre as populações pró-russas e pró-ucranianas na região. Manifestações de russos étnicos exigiam maior autonomia ou integração com a Rússia, e tropas russas, disfarçadas como “forças de autodefesa locais”, ocuparam pontos estratégicos na península. A operação foi predominantemente terrestre, com a presença de tropas russas ocupando edifícios governamentais e instalações estratégicas. Por outro lado, a marinha russa demonstrou força em Sebastopol, um porto naval importante. Este evento alterou a dinâmica geopolítica na região do Mar Negro e teve repercussões duradouras nas relações internacionais e na segurança europeia. (Saluschev, 2014)

Entre 2014 e 2022, a Rússia implementou uma vasta campanha de desinformação e propaganda contra a Ucrânia, utilizando meios cibernéticos para disseminar informações falsas, manipular a opinião pública e criar divisões internas. Essa estratégia fazia parte de um conflito híbrido[12] mais amplo, combinando operações militares convencionais com técnicas cibernéticas e de guerra psicológica (Mueller, 2023).

Ataques cibernéticos foram utilizados para derrubar sites governamentais e de notícias ucranianas, substituindo seu conteúdo por propaganda pró-Rússia ou desinformação (Mueller, 2023).

A prática utilizada pela Rússia contra a Ucrânia exemplifica uma abordagem moderna e sofisticada de guerra cibernética, que vai além do campo de batalha tradicional. A resposta eficaz a tais ameaças requer não apenas defesas cibernéticas robustas, mas também uma forte resiliência informacional e cooperação internacional para combater a propagação de desinformação (Osadchuk, 2023).

Examinaremos alguns dos principais ataques realizados como o BlackEnergy de 2015, o NotPetya de 2017 e o ataque Setor de Defesa Ucraniano em 2018 sob a ótica dos conceitos de Clausewitz, proporcionando uma compreensão mais profunda dos impactos e desafios das operações cibernéticas nos conflitos modernos.

4.1 O ATAQUE DE BLACKENERGY[13] EM 2015: UM MARCO NA GUERRA CIBERNÉTICA

Em dezembro de 2015, um ataque coordenado lançado por hackers russos contra a rede elétrica ucraniana utilizou um *malware* denominado BlackEnergy, deixando centenas de milhares de pessoas sem eletricidade por várias horas, nas regiões de Ivano-Frankivsk e Kyiv. O governo ucraniano identificou a Rússia como a responsável pelo ataque. Este evento não apenas ganhou destaque global por

[12] Emprego não convencional de diversas capacidades, táticas e meios, buscando alcançar efeitos sinérgicos nas dimensões físicas e psicológicas do conflito (Barbosa, 2020).

[13] Malware altamente modular que permite adicionar ou remover funcionalidades conforme necessário. Serve como ferramentas para espionagem, sabotagem e ataques de negação de serviço. Além disso, pode destruir dados, dificultando a recuperação dos sistemas afetados. Destaca-se pelo uso de e-mails com anexos maliciosos ou links para sites comprometidos (*pishing*), ataques direcionados a indivíduos específicos com informações personalizadas (spear *phishing*) e acesso não autorizado a sistemas críticos explorando vulnerabilidades conhecidas. (Kaspersky, 2024). Disponível em: https://www.kaspersky.com.br/resource-center/threats/types-of-malware. Acesso em: 27 jun. 2024).

atacar a infraestrutura crítica, mas também demonstrou as capacidades cibernéticas da Rússia, tornando-se um exemplo significativo de guerra cibernética entre Estados (Sanger, 2018).

O ataque direcionado a infraestruturas críticas afetou três empresas de distribuição de energia na Ucrânia ao acessar os sistemas de controle das subestações elétricas, permitindo que desligassem remotamente várias subestações. Os atacantes não só desligaram as subestações, mas também corromperam os dispositivos usados para controlar a rede elétrica, dificultando a recuperação. Além disso, apagaram dados críticos nos sistemas de controle, tornando o processo de recuperação mais complexo. As interrupções no fornecimento de energia duraram aproximadamente seis horas, dependendo da região e da capacidade das equipes de resposta em restaurar o serviço (Sanger, 2018).

David E. Sanger (2018) afirma que, além do impacto social pela interrupção do serviço elétrico, o ataque causou perturbações significativas nas operações diárias, incluindo o fechamento temporário de negócios e serviços essenciais. O impacto econômico incluiu custos significativos de recuperação e reforço das medidas de segurança.

De acordo com o relatório do *Electricity Information Sharing and Analysis Center* (E-ISAC, 2016), o ataque destacou as vulnerabilidades nas infraestruturas críticas ucranianas e levou a um aumento na conscientização sobre a importância da cibersegurança, resultando em esforços coordenados entre governos e empresas para melhorar as defesas cibernéticas e a resiliência das infraestruturas críticas.

Após o ataque, houve um esforço concentrado para atualizar os sistemas de segurança e implementar melhores práticas de cibersegurança. Isso incluiu a atualização de software, a implementação de sistemas de detecção de intrusão mais robustos e a realização de treinamentos de conscientização de segurança para os funcionários (E-ISAC, 2016).

Os ataques cibernéticos de 2015, amplamente considerados como uma ação orquestrada por *hackers* vinculados ao governo russo (Greenberg, 2019), proporcionaram vantagens e desvantagens para Rússia e Ucrânia respectivamente, se considerarmos o contexto pós anexação da Crimeia.

Como consequências negativas do BlackEnergy para a Ucrânia, Romano Osadchuk (2023) destaca o enfraquecimento da economia por meio das

perturbações econômicas significativas que afetaram empresas e cidadãos; e a permanência de um clima de insegurança e medo na sociedade pelo fato do ataque atingir diretamente a confiança pública no governo e nas suas capacidades de defesa ucraniana.

De acordo com David E. Sanger (2018), para a Rússia, o ataque serviu como uma demonstração clara de sua capacidade cibernética, enviando uma mensagem geopolítica não só à Ucrânia, mas também ao mundo, sobre o poder de suas operações cibernéticas. Assim, ao mostrar sua capacidade de causar danos significativos, a Rússia pode ter buscado dissuadir outros países de tomar ações contra seus interesses.

Como visto no capítulo anterior, uma ação cibernética realizada isoladamente não possui a capacidade de influenciar decisivamente no resultado de um conflito. Assim sendo, desestabilizar a infraestrutura crítica ucraniana pode ter sido uma medida para ganhar vantagem em conflitos militares ou negociações políticas como afirma Romano Osadchuk (2023). Na época, em 2015, a Rússia estava envolvida no conflito na região de Donbas e na anexação da Crimeia ocorrida no ano anterior, e tal ataque poderia ter sido uma forma de pressionar o governo ucraniano.

Neste diapasão, o ataque permitiu ainda à Rússia promover uma narrativa de que o governo ucraniano é incapaz de proteger seu próprio povo, influenciando a opinião pública dentro da Ucrânia. Ataques dessa natureza podem exacerbar divisões internas dentro da Ucrânia, entre diferentes grupos políticos ou regiões, enfraquecendo ainda mais a coesão nacional (Mueller, 2023)(Osadchuk, 2023).

Analisando o ocorrido sob a perspectiva do campo da inteligência, os ataques podem ter sido usados para coletar informações sobre a infraestrutura de energia da Ucrânia e suas defesas cibernéticas. Assim, ao observar as respostas da Ucrânia e da comunidade internacional frente ao ataque, a Rússia pode modelar sua estratégia cibernética para operações futuras (Mueller, 2023).

Relacionando os ataques do BlackEnergy ao conceito de fricção de Clausewitz, nota-se que essa fricção se manifesta nas dificuldades enfrentadas pelas equipes de resposta em implementar sua própria estratégia, ou seja, mitigar os danos e restaurar os sistemas comprometidos. Neste contexto, é importante destacar que o conceito comum de fricção precisa ser reinterpretado à luz das ações de guerra cibernéticas pois esse conceito não se manifesta através de ações cinéticas, mas sim através de ações não cinéticas.

Outros conceitos observados no caso em questão são os de infraestruturas críticas e de Centro de Gravidade. Segundo David E. Sanger (2018), os ataques foram dirigidos especificamente contra a infraestrutura crítica de energia da Ucrânia, destacando a vulnerabilidade de sistemas essenciais a ciberataques. A referida infraestrutura de energia da Ucrânia pode também ser considerada como um centro de gravidade, por ser crucial para o país, ou ao menos para as cidades atingidas, uma vez que outras estruturas essenciais de funcionamento foram atingidas em consequência do ataque. Considerando os conceitos de Clausewitz citados, os *hackers* russos almejavam alcançar vantagens como desestabilizar a economia ucraniana, causar pânico na população, enfraquecer a capacidade daquele país de manter a confiança pública além de promover uma forte pressão nas negociações políticas relacionadas à disputa da Crimeia iniciada em 2014 (Osadchuk, 2023).

Ainda dentro da análise comparativa do caso com os conceitos do teórico militar prussiano, o conceito de névoa de guerra se aplica particularmente à incerteza e confusão geradas aos ucranianos pelos ataques cibernéticos. Dados como a identificação da origem, a compreensão do alcance total do comprometimento e a dificuldade de uma resposta eficaz foram aspectos proporcionados pela complexidade do ambiente cibernético.

Portanto, conclui-se que o ataque de BlackEnergy foi um evento marcante na história da guerra cibernética. Ele demonstrou a capacidade dos atacantes de causar danos físicos significativos através de meios cibernéticos e ressaltou a necessidade urgente de proteger infraestruturas críticas contra tais ameaças. A experiência da Ucrânia destaca a importância de uma preparação e de uma resposta coordenada para enfrentar as ameaças cibernéticas modernas, protegendo assim a segurança nacional e a estabilidade econômica. A Rússia, ao realizar ataques cibernéticos contra a Ucrânia, pode ter se beneficiado de várias maneiras, desde desestabilizar a Ucrânia economicamente até demonstrar seu poder cibernético e ganhar vantagem estratégica, conforme exposto por Romano Osadchuk (2023). Esses benefícios potencialmente aumentam a influência da Rússia na região e destacam a importância da cibersegurança em um cenário geopolítico cada vez mais digitalizado.

O caso BlackEnergy, ao ser analisado através dos conceitos de Clausewitz, revela a natureza complexa dos conflitos cibernéticos. A fricção, o ataque aos centros de gravidade, a vulnerabilidade das infraestruturas críticas e a névoa da

guerra são todos elementos que demonstram como a teoria militar clássica pode ser aplicada para entender melhor os desafios e dinâmicas das ameaças cibernéticas contemporâneas.

Por fim, é justo considerar que o evento BlackEnergy, direcionado contra a infraestrutura de rede elétrica e responsável por danos significativos a sistemas essenciais de funcionamento da sociedade ucraniana, afetando segurança, economia e bem-estar da população, exemplifica como ciberataques direcionados a infraestruturas críticas podem ser usados como uma ferramenta estratégica em conflitos entre Estados-nação, com impactos significativos na segurança, economia e estabilidade social. Destaca-se também as vulnerabilidades das infraestruturas críticas ucranianas, exigindo esforços para melhorar a cibersegurança. Isso reflete a importância estratégica dessas infraestruturas e a necessidade de protegê-las contra ameaças cibernéticas.

4.2 NOTPETYA EM 2017: DESESTABILIZAÇÃO E GUERRA CIBERNÉTICA CONTRA A UCRÂNIA

O NotPetya surgiu em junho de 2017 e foi um ataque destrutivo considerado inicialmente com o propósito de obter resgates financeiros mas, ao ser analisado criteriosamente, seu verdadeiro objetivo de causar danos aos sistemas ucranianos foi revelado. Disfarçado como um *ransomware*[14], ele criptografava dados em sistemas infectados e pedia um resgate em Bitcoin para fornecer a chave de descriptografia. No entanto, mesmo quando o pagamento era feito, os dados raramente eram recuperados, sugerindo que o verdadeiro propósito era a destruição de dados (Greenberg, 2019).

O NotPetya utilizou para sua propagação, uma atualização comprometida do software de contabilidade amplamente utilizada por empresas na Ucrânia para fins de conformidade fiscal. Ao comprometer a atualização deste software, os atacantes conseguiram distribuir o *malware* rapidamente dentro da rede das empresas que usavam o *software*. Além disso, o NotPetya explorou vulnerabilidades do Windows,

[14] *Ransomware* é um tipo de *malware* que criptografa os dados das vítimas, tornando-os inacessíveis, e exige um pagamento de resgate, geralmente em criptomoedas, para fornecer a chave de descriptografia. A infecção pode ocorrer através de e-mails de *phishing*, links maliciosos ou vulnerabilidades de rede, espalhando-se rapidamente para outros dispositivos na rede.

que permitiu a sua rápida disseminação através de redes internas e, eventualmente, globalmente (Greenberg, 2019).

Embora o ataque tivesse como alvos iniciais empresas e instituições ucranianas, ele rapidamente se espalhou para várias partes do mundo, afetando empresas globais de diversos setores. Entre as vítimas estavam gigantes como a Maersk, empresa de transporte marítimo, a Merck, empresa farmacêutica, e a FedEx, empresa de logística. O ataque causou interrupções significativas nas operações dessas empresas, resultando em perdas financeiras estimadas em bilhões de dólares. Várias investigações e análises de especialistas em segurança cibernética, incluindo o governo dos EUA, atribuíram o ataque ao grupo de hackers conhecido como *Sandworm*[15] (Greenberg, 2019).

Clausewitz argumenta que a guerra é uma extensão da política, utilizada para alcançar objetivos políticos que não podem ser obtidos por outros meios. O ataque NotPetya pode ser visto como um exemplo de guerra cibernética utilizada como ferramenta política uma vez que foi direcionado principalmente contra a Ucrânia, um país com o qual a Rússia tem tensões políticas significativas (Sanger, 2018). A disseminação global do ataque também pode ser interpretada como um sinal de força e capacidade cibernética da Rússia, projetando poder, diminuindo a capacidade de resistência ucraniana e instigando temor em nível internacional.

O NotPetya também trouxe à luz um outro conceito do teórico militar prussiano o qual argumenta que a força deve ser usada de forma eficiente e proporcional para alcançar objetivos estratégicos. De acordo com David E. Sanger (2018), o NotPetya utilizou um método de propagação altamente eficaz e específico ao comprometer uma atualização de um software utilizado, demonstrando um uso estratégico da força cibernética para maximizar o impacto com recursos relativamente limitados.

Outro conceito de Clausewitz plausível de ser considerado neste ataque é o de Centro de Gravidade que se traduz como fonte de poder de um adversário, que, se atacada, pode desestabilizar e derrotar o inimigo. No contexto do NotPetya, o "centro de gravidade" poderia ser interpretado como as capacidades econômicas da Ucrânia. Andy Greenberg (2019) argumenta que, ao atacar o software amplamente

[15]Considerado vinculado estreitamente ao governo russo, o Sandworm tem um histórico de conduzir ataques cibernéticos sofisticados e destrutivos, muitas vezes com motivações geopolíticas. A atribuição ao Sandworm sugere que o ataque fazia parte de uma estratégia mais ampla de desestabilização e de guerra cibernética contra a Ucrânia. (Greenberg, 2019)

utilizado em setores essenciais da economia ucraniana, os hackers visaram um ponto crítico que, ao ser comprometido, desestabilizou significativamente as operações financeiras e comerciais do país.

Ainda, há uma estreita relação com o NotPetya e o conceito clausewitziano de “névoa da guerra”. Neste caso, a incerteza sobre a origem, natureza e propósito do ataque dificultaram a resposta inicial das vítimas e das equipes de segurança cibernética, prolongando o impacto do ataque e exacerbando os danos causados.

Outra consideração a ser observada no caso NotPetya, é referente ao conceito de “fricção da guerra” de Clausewitz. O referido conceito pode ser observado nas dificuldades enfrentadas pelas instituições afetadas para restaurar seus sistemas e operações. De acordo com Greenberg (2020), o ataque interrompeu cadeias de suprimentos, operações de negócios e comunicações globais. Cabe neste momento uma ressalva quanto ao conceito de “fricção da guerra” o qual, em ações de guerra cibernética não se traduz efetivamente em ações cinéticas mas em ações não cinéticas.

A análise do NotPetya através dos conceitos de Clausewitz revela a profundidade e a complexidade estratégica da guerra cibernética. Assim como as guerras convencionais analisadas por Clausewitz, os ataques cibernéticos como o NotPetya são influenciados por objetivos políticos, estratégias de desestabilização e a exploração de vulnerabilidades críticas, podendo ser considerada como uma continuação da política por meios digitais.

Por fim, de acordo com Greenberg (2020) o NotPetya destacou a vulnerabilidade das infraestruturas digitais globais a ataques cibernéticos destrutivos e a capacidade de tais ataques de causar danos econômicos substanciais. Ele também sublinhou a importância da segurança cibernética robusta e da cooperação internacional na identificação e resposta às ameaças cibernéticas.

4.3 *PHISHING* COMO ARMA DE GUERRA EM 2018: O CASO DO SETOR DE DEFESA UCRANIANO

Em 2018, o setor de defesa da Ucrânia foi alvo de uma série de campanhas, de *phishing*[16] atribuídas ao grupo de hackers russos conhecido como Fancy Bear,

[16]Técnica de ataque cibernético em que os criminosos se passam por entidades confiáveis para enganar indivíduos e induzi-los a divulgar informações sensíveis, como senhas, números de cartão

com o objetivo de roubar informações sensíveis, incluindo planos de operações militares, comunicações internas e dados pessoais de oficiais de defesa, comprometer as comunicações e operações das forças armadas e desestabilizar e enfraquecer a capacidade de defesa do país. O evento foi considerado uma campanha pois caracterizou-se por ações descentralizadas com o objetivo de atingir alvos específicos em um determinado período de tempo. Acredita-se que a referida campanha tenha iniciado em 2017 com ápice ofensivo em 2018 (Bateman, 2022).

Tendo como alvos prioritários oficiais militares de alto escalão, funcionários do Ministério da Defesa ucraniano, empresas de defesa e contratantes envolvidos em projetos sensíveis e unidades de inteligência militar, os *hackers* enviaram e-mails que pareciam ser de fontes confiáveis, com anexos infectados que instalavam *malware* no sistema dos computadores dos alvos. Os e-mails de *phishing* também incluíam links para sites falsos que imitavam portais de login de organizações de defesa, induzindo as vítimas a inserir suas credenciais. Os hackers personalizaram e-mails com informações específicas sobre os alvos, aumentando a probabilidade de sucesso dos ataques. Engenharia social também foi usada para coletar informações sobre os alvos, permitindo que os e-mails parecessem ainda mais legítimos e difíceis de detectar (Bateman, 2022).

Segundo Joe Bateman (2022), as consequências para a Ucrânia foram devastadoras no âmbito da Defesa Nacional com o comprometimento de informações sensíveis sobre operações e exercícios militares além do roubo e vazamento de dados pessoais de oficiais de defesa, aumentando o risco de ameaças físicas e cibernéticas adicionais. Destaca-se também como resultado um colapso nas comunicações e operações militares, obrigando as forças armadas a alterar muitos protocolos de segurança. Assim, a capacidade da Ucrânia de defender suas fronteiras e conduzir operações militares foi consideravelmente enfraquecida, expondo e aumentando a vulnerabilidade às ações hostis (Bateman, 2022).

Após identificado o sucesso da campanha, as autoridades ucranianas, contando com o apoio e colaboração de parceiros internacionais, lançaram investigações para identificar e mitigar o impacto dos ataques. Oficiais e funcionários foram alertados sobre as técnicas de *phishing* e receberam treinamento para

---

de crédito ou outros dados pessoais. Esse tipo de ataque é frequentemente realizado por meio de e-mails, mensagens instantâneas ou *websites* falsos que imitam fontes legítimas.

reconhecer e evitar e-mails suspeitos. A Ucrânia recebeu assistência técnica e estratégica de parceiros internacionais, incluindo a OTAN e a União Europeia, para melhorar suas defesas cibernéticas. Além disso, aumentou o compartilhamento de informações sobre ameaças cibernéticas entre a Ucrânia e seus aliados, fortalecendo a resiliência coletiva contra ataques cibernéticos (Clarke; Knake, 2019).

Ao analisar a campanha de *phishing* de 2018, as ações desencadeadas e seus respectivos resultados, observa-se uma estreita relação com alguns axiomas de Clausewitz. A fricção, que em guerra cibernética recebe uma forma diferente da convencional, materializou-se com o comprometimento das comunicações e roubo de informações sensíveis ucranianas. Isso exigiu que as forças armadas desviassem recursos e atenção para mitigar os danos e fortalecer suas defesas cibernéticas. Importante destacar que, de acordo com o argumento de Clarke e Knake (2019),a necessidade de identificar e responder a cada ataque de *phishing* exige uma complexidade adicional no campo da qualificação de pessoal para reconhecer ameaças e implementar novas medidas de segurança.

Outro conceito de Clausewitz observado no caso em análise é o de centro de gravidade que, segundo Clausewitz, é a fonte de força ou poder de um adversário, cujo ataque ou neutralização pode desestabilizar e derrotar o inimigo.

Nesse caso, o setor de defesa ucraniano pode ser considerado um centro de gravidade, pois sua eficácia é crucial para a segurança e estabilidade do país. Bateman (2022) e Mueller (2023) argumentam que, ao direcionar ataques cibernéticos contra o setor de defesa, os *hackers* russos visavam enfraquecer a capacidade militar da Ucrânia, minando sua defesa nacional. O roubo de dados críticos sobre operações militares e planos estratégicos atacou o centro de gravidade, comprometendo a capacidade de resposta da Ucrânia e fornecendo uma vantagem estratégica aos russos.

Ainda sob um enfoque de conceitos teóricos de Clausewitz, os sistemas de TI e comunicação do setor de defesa podem ser considerados infraestruturas críticas. Comprometer esses sistemas através de *phishing* pode paralisar a capacidade de resposta militar e criar vulnerabilidades significativas. Nesse contexto, a dependência de tecnologias de comunicação e informação torna esses sistemas alvos atraentes para ataques cibernéticos, destacando a necessidade de proteger infraestruturas críticas contra tais ameaças (Bateman, 2022).

Podemos considerar ainda que a campanha de *phishing* criou uma “névoa da guerra” com origem na dimensão cibernética, onde as forças de defesa ucranianas enfrentaram incertezas sobre a extensão dos compromissos, a origem dos ataques e a veracidade das informações comprometidas. Assim, a necessidade de reagir rapidamente a ataques cibernéticos, identificar fontes confiáveis de informação e mitigar danos foram elementos de um ambiente complexo e desafiador para a tomada de decisão.

Outro aspecto clausewitziano que podemos abordar nessa análise comparativa, é o de fricção. Cada e-mail de *phishing* bem-sucedido, cada sistema comprometido e cada necessidade de reforço de segurança adicionaram fricção ao ambiente operacional das forças de defesa ucranianas. A fricção causada pela campanha de *phishing* se manifestou em interrupções nas comunicações, necessidade de reparos e atualizações de sistemas, e desvio de recursos para a cibersegurança, afetando negativamente a eficácia operacional.

Portanto, a campanha de *phishing* contra o setor de defesa ucraniano entre 2017 e 2018 destacou a sofisticação e persistência dos ataques cibernéticos patrocinados pelo Estado (Mueller, 2023). A resposta da Ucrânia combinou medidas imediatas, fortalecimento das defesas cibernéticas e cooperação internacional, enfatizando a necessidade de uma abordagem criteriosa para enfrentar ameaças complexas (Bateman, 2022).

Por fim, a associação entre a campanha de *phishing* e os conceitos de fricção, centro de gravidade, infraestruturas críticas e névoa da guerra de Clausewitz revela os desafios contemporâneos no domínio cibernético. Essa análise destaca a importância de uma estratégia resiliente de defesa cibernética em tempos de conflitos modernos, onde a proteção contra ameaças digitais se torna crucial para a segurança nacional e a estabilidade das infraestruturas críticas.

5 CONSIDERAÇÕES FINAIS

Diante dos fatos analisados e apesar da complexidade da obra de Clausewitz ser amplamente reconhecida, é justo afirmar que muitos de seus conceitos ainda permanecem relevantes para a compreensão da guerra moderna.

Apesar das mudanças tecnológicas que moldam os conflitos atuais, a intenção de destruir o inimigo permanece constante. Segundo Clausewitz, a guerra é vista como uma ação entre forças que buscam impor suas vontades ao adversário, resultando em uma ação recíproca que tende a se estender aos extremos. Esta dinâmica se desenvolve em três fases a saber: a primeira é a imposição de violência até os extremos, a segunda é a tentativa de forçar o adversário a assumir uma posição desfavorável, e a terceira relaciona a vitória ao esforço medido pela “extensão de meios” e a “firmeza de vontade”. É nesta última fase que o quinto domínio estabelece relações com as expressões “extensão de meios” e “firmeza de vontade”. A “extensão de meios” pode ser relacionada à amplitude tecnológica disponível, enquanto a “firmeza de vontade” refere-se à capacidade de utilizar essa tecnologia de forma eficaz em combate

Nesse contexto, a combinação dessas ações recíprocas em um ambiente conflituoso tem o propósito de colocar o adversário em uma situação desvantajosa duradoura, onde cada ação agrava sua posição.

Clausewitz também destaca que a guerra não surge de maneira súbita, mas evolui através de uma série de ações sucessivas que aproveitam situações favoráveis oriundas de ações anteriores. A guerra, portanto, é uma série de ações complementares e sucessivas, onde a observação dos resultados obtidos orienta ações subsequentes. Ainda, Clausewitz observa que a reunião perfeita de todas as forças em um único momento é impraticável, implicando um faseamento natural da guerra.

Outro conceito abordado foi o de “névoa da guerra”. A incerteza que permeia a guerra, exige discernimento e inteligência na busca de informações relevantes para o decisor. Na era da informação, embora a “névoa da guerra” pareça ter se dissipado, o excesso de informações disponíveis coloca os tomadores de decisão em uma posição difícil, pois precisam filtrar e selecionar os dados realmente importantes no campo de batalha. As novas tecnologias, como drones, satélites, inteligência artificial e capacidades cibernéticas, intensificam esse desafio ao gerar

uma sobrecarga de dados, dificultando a distinção entre informações precisas e dados enganosos ou irrelevantes.

É justo afirmar que o desenvolvimento tecnológico introduziu novas camadas de incerteza e transformou o conceito de “névoa da guerra”. A falta de informações precisas deu lugar a uma superabundância de dados, que precisam ser processados e analisados para fornecer precisão nas operações de combate. Assim, o conceito de “névoa da guerra” de Clausewitz permanece altamente relevante, intensificado pelas tecnologias avançadas e pela natureza dinâmica dos conflitos modernos.

Por outro lado, o conceito de Centro de Gravidade foi definido por Clausewitz como o ponto central de todo poder e movimento, do qual tudo depende. No cenário contemporâneo, dominado por inovações tecnológicas, identificar e neutralizar o Centro de Gravidade do oponente pode ir além do campo de batalha convencional. O sucesso das operações militares no século XXI depende tanto da mobilização de forças quanto da identificação e ataque aos centros nevrálgicos do inimigo, que podem ser tangíveis, como instalações estratégicas, ou intangíveis, como a opinião pública e a estabilidade política.

A estratégia militar contemporânea deve identificar e focar nesses centros de gravidade, reconhecendo que sua neutralização pode comprometer a capacidade operacional do adversário de forma mais eficaz do que a destruição de forças convencionais.

A potencialização do conceito de centro de gravidade no ambiente contemporâneo exige a adoções de uma estratégia militar que utilize todos os recursos disponíveis para identificar e atacar esses centros de forma eficiente. Assim, essa abordagem envolve a coordenação de ações cinéticas e não cinéticas no conflito.

Portanto, o conceito de Centro de Gravidade tornou-se mais abrangente devido às inovações tecnológicas e à complexidade dos conflitos modernos. A identificação precisa desses centros e a aplicação estratégica de forças contra eles podem determinar o sucesso ou o fracasso das operações militares.

O conceito de “fricção” de Carl von Clausewitz, refere-se às dificuldades e complicações inevitáveis que surgem durante a execução de operações militares. Clausewitz descreve a fricção como o que diferencia a guerra real da guerra teórica ou idealizada sendo, portanto, uma metáfora para os diversos fatores que

complicam e atrasam as operações, exigindo resiliência, adaptabilidade e habilidade para superá-la e alcançar os objetivos.

No contexto da guerra cibernética, a fricção resulta da complexidade, incerteza e imprevisibilidade das operações cibernéticas, manifestando-se em dificuldades para identificar a origem e a extensão dos ataques, bem como a magnitude dos danos provocados, além de dificuldades na coordenação das respostas a esses ataques.

Embora Carl von Clausewitz não tenha usado especificamente o termo “infraestrutura crítica” em sua obra, ele destacou a importância de proteger fortificações, depósitos de suprimentos e cidades por entender serem fundamentais para o funcionamento do estado. Atualmente, as infraestruturas críticas incluem setores como energia, água e saneamento, transporte, comunicações, saúde e financeiro. Proteger e atacar essas infraestruturas durante guerras pode ter um impacto significativo nas capacidades militares e civis de um país.

Nesse contexto, os conglomerados urbanos modernos, com seu poder econômico, político e comercial, desempenham um papel crucial na postura de um Estado em guerra. Pode-se, então, fazer uma analogia entre a proteção dessas cidades à proteção das infraestruturas críticas citadas por Clausewitz.

Dentro do escopo do trabalho, a guerra cibernética é uma ferramenta do ciberespaço que produz resultados significativos quando combinada com meios militares convencionais.

Uma estratégia que combine armas convencionais e cibernéticas é fundamental, tanto ofensivamente quanto preventivamente, destacando a natureza subsidiária do domínio cibernético. A Rússia se destaca por sua capacidade de integrar guerra cibernética com armas convencionais, resultado de sua experiência pós-Guerra Fria.

Por outro lado, a Ucrânia, alvo frequente de ataques cibernéticos desde 2014, especialmente por parte da Rússia, reforçou sua defesa cibernética em resposta. Esses ataques visaram infraestruturas críticas e incluíram campanhas de desinformação, demonstrando o uso do ciberespaço como extensão dos conflitos tradicionais.

De uma forma geral, de 2014 até 2022, a Rússia coordenou ataques cibernéticos simultâneos a operações militares convencionais, enquanto a Ucrânia

fortaleceu suas capacidades defensivas. Isso ilustra a complexidade do confronto contínuo entre os dois países no ciberespaço.

Em dezembro de 2015, hackers russos lançaram um ataque contra a rede elétrica ucraniana usando o *malware* BlackEnergy, deixando milhares de pessoas sem eletricidade. O governo ucraniano identificou a Rússia como responsável pelo ataque, que ganhou destaque global e demonstrou as capacidades cibernéticas russas.

Além do impacto social pela interrupção do serviço elétrico, o ataque causou perturbações significativas nas operações diárias, incluindo o fechamento temporário de negócios e serviços essenciais. O ataque destacou as vulnerabilidades nas infraestruturas críticas ucranianas e levou a um aumento na conscientização global sobre a importância da cibersegurança, resultando em esforços coordenados para melhorar as defesas cibernéticas e a resiliência das infraestruturas críticas. Após o ataque, houve um esforço concentrado da Ucrânia com a finalidade de atualizar os sistemas de segurança e implementar melhores práticas de cibersegurança.

Os ataques cibernéticos de 2015, orquestrados por *hackers* vinculados ao governo russo, proporcionaram vantagens e desvantagens para Rússia e Ucrânia respectivamente.

As consequências negativas para a Ucrânia incluíram o enfraquecimento da economia e a criação de um clima de insegurança e medo na sociedade. Para a Rússia, o ataque serviu como uma demonstração clara de sua capacidade cibernética, enviando uma mensagem geopolítica não só à Ucrânia, mas também ao mundo. Ao desestabilizar a infraestrutura crítica ucraniana, a Rússia poderia ter buscado ganhar vantagem em conflitos militares ou negociações políticas, especialmente no contexto do conflito da anexação da Crimeia em 2014.

O ataque também permitiu à Rússia promover a narrativa de que o governo ucraniano é incapaz de proteger seu próprio povo, exacerbando divisões internas dentro da Ucrânia e enfraquecendo a coesão nacional. Além disso, os ataques podem ter sido usados para coletar inteligência sobre a infraestrutura de energia da Ucrânia e suas defesas cibernéticas, permitindo aprimoramentos para futuras ações.

Os conceitos de Clausewitz aplicados ao caso incluem a fricção, manifestada nas dificuldades técnicas e operacionais enfrentadas pelas equipes de resposta; infraestruturas críticas; e o centro de gravidade, se considerarmos o sistema de energia sendo crucial para o funcionamento país. Identificamos também

o conceito de névoa da guerra de Clausewitz devido as incertezas durante o ataques.

BlackEnergy foi um evento marcante na história da guerra cibernética, destacando a necessidade de proteger infraestruturas críticas contra ameaças cibernéticas e a importância da cibersegurança em um cenário geopolítico cada vez mais digitalizado.

Outro evento que merece destaque foi o NotPetya em junho de 2017 que surgiu inicialmente como um ataque considerado para obter resgates financeiros mas, descobriu-se que seu verdadeiro objetivo era causar danos aos sistemas ucranianos.

O NotPetya se propagou através de uma atualização comprometida de um software amplamente utilizado na Ucrânia e explorou vulnerabilidades do Windows, permitindo sua rápida disseminação por redes internas e globais. Embora tivesse como objetivo empresas e instituições ucranianas, ele rapidamente se espalhou para várias partes do mundo resultando em interrupções significativas de operações e perdas financeiras estimadas em bilhões de dólares.

Analisando NotPetya sob a ótica de Clausewitz, podemos associar o ataque cibernético russo ao uso da força de forma eficiente e proporcional para alcançar objetivos estratégicos, maximizando o impacto com recursos limitados.

Outro conceito de Clausewitz aplicável ao ataque é o de Centro de Gravidade, que pode ser interpretado como as capacidades econômicas da Ucrânia. Ao atacar um *software* crucial para a economia ucraniana, os *hackers* desestabilizaram significativamente as operações financeiras e comerciais do país.

A confusão inicial sobre a natureza do ataque e sua posterior revelação como um ataque destrutivo, relaciona-se ao conceito de “névoa da guerra” de, dificultando a identificação da origem bem como a extensão dos danos.

Da mesma forma, o conceito de fricção é observado nas dificuldades enfrentadas pelas empresas para restaurar seus sistemas e operações. O ataque causou um grande comprometimento operacional, interrompendo cadeias de suprimentos e comunicações globais.

A análise do NotPetya através dos conceitos de Clausewitz revela a amplitude estratégica da guerra cibernética. O ataque destacou a vulnerabilidade das infraestruturas digitais globais e a necessidade de segurança cibernética robusta e cooperação internacional na resposta a tais ameaças.

Em 2018, o setor de defesa da Ucrânia foi alvo de uma campanha de *phishing* atribuídas ao grupo de *hackers* russos conhecido como Fancy Bear. O objetivo era roubar informações sensíveis, incluindo planos de operações militares, além de comprometer as comunicações e operações das forças armadas, desestabilizando e enfraquecendo a capacidade de defesa do país.

Os principais alvos incluíam oficiais militares de alto escalão e funcionários do Ministério da Defesa ucraniano, além de unidades de inteligência militar. Através de e-mails de *phishing*, os *hackers* imitavam portais de login de organizações de defesa, levando as vítimas a inserir suas credenciais.

As consequências para a Defesa Nacional da Ucrânia foram devastadoras, com o comprometimento de informações sobre operações e exercícios militares, elevando o risco de novas ameaças. As forças armadas foram obrigadas a modificar muitos protocolos de segurança com o propósito de evitar o enfraquecimento da capacidade de defender as fronteiras e conduzir operações militares.

A Ucrânia, através de apoio internacional conseguiu identificar e mitigar os impactos dos ataques. Oficiais e funcionários foram alertados sobre as técnicas de *phishing* e receberam treinamento para reconhecer e evitar e-mails suspeitos. A Ucrânia também recebeu assistência técnica e estratégica de parceiros internacionais, como a OTAN e a União Europeia, para fortalecer suas defesas cibernéticas.

Analisando a campanha de *phishing* de 2018, observa-se uma estreita relação com alguns conceitos de Clausewitz. A fricção, nesse caso, materializou-se pela dificuldade de compreender o alcance do ataque exigindo que as forças armadas fortalecessem suas defesas cibernéticas. Por outro lado, a fricção causada pelas interrupções nas comunicações, necessidade de reparos e atualizações de sistemas afetaram a eficácia operacional das forças de defesa ucranianas.

Outro conceito clausewitziano observado é o de centro de gravidade associado, no caso em questão, ao setor de defesa ucraniano. Atacar por meio de ações cibernéticas este setor visava enfraquecer a capacidade militar da Ucrânia, comprometendo sua defesa nacional ao roubar dados críticos sobre operações militares e planos estratégicos, proporcionando relativa vantagem estratégica aos russos.

A campanha de *phishing* também criou uma “névoa da guerra”, onde as forças de defesa ucranianas enfrentaram incertezas sobre a extensão das

informações comprometidas e a origem dos ataques.

A campanha destacou uma resposta ucraniana combinada de medidas imediatas, fortalecimento das defesas cibernéticas e cooperação internacional, enfatizando a necessidade de uma abordagem criteriosa para enfrentar ameaças complexas.

Diante do exposto, as teorias de Carl von Clausewitz, formuladas no século XIX, continuam a ser extremamente relevantes no contexto das operações militares contemporâneas, mesmo com as significativas mudanças tecnológicas. Especialmente na guerra cibernética, os princípios de Clausewitz, como fricção, infraestruturas críticas, centro de gravidade e névoa da guerra, demonstram sua contínua aplicabilidade aos conflitos modernos.

A fricção, definida como as dificuldades inevitáveis e imprevistas nas operações militares, agora se manifesta nas complexidades técnicas e na imprevisibilidade das operações cibernéticas.

As infraestruturas críticas, embora não nomeadas explicitamente por Clausewitz, foram implicitamente abordadas em suas discussões sobre fortificações e pontos estratégicos, e permanecem centrais na segurança moderna, abrangendo setores como energia e comunicações.

O conceito de centro de gravidade, um ponto de força decisivo cuja neutralização pode desestabilizar o adversário, é mais relevante do que nunca, especialmente quando consideramos alvos cibernéticos que afetam capacidades econômicas e militares.

A névoa da guerra, caracterizada pela incerteza e confusão no campo de batalha, é intensificada no ambiente digital, onde a sobrecarga de informações e a dificuldade em distinguir entre dados precisos e enganosos complicam a tomada de decisões estratégicas.

Eventos como os ataques cibernéticos BlackEnergy e NotPetya, e a campanha de *phishing* contra o setor de defesa ucraniano, exemplificam como os princípios de Clausewitz continuam a orientar a compreensão estratégica e a resposta a ameaças cibernéticas.

Portanto, longe de estarem ultrapassadas, as teorias de Clausewitz adaptaram-se e permanecem essenciais para a análise e estratégia militar moderna. Elas não só mantêm sua relevância como são enriquecidas pela integração de novas tecnologias e pela necessidade de uma abordagem estratégica abrangente,

que inclua tanto elementos convencionais quanto cibernéticos. Assim, a aplicabilidade contínua das teorias de Clausewitz reforça sua importância no entendimento e na condução das operações militares no contexto atual de guerra cibernética.

REFERÊNCIAS

ALAM, Shahid. **Cybersecurity: Past, Present and Future**. arXiv, 2022. Disponível em: https://arxiv.org/abs/2207.01227. Acesso em: 24 jun. 2024.

ALVAREZ, Joshua. **Stuxnet: The world's first cyber weapon.** Center for International Security and Cooperation, Freeman Spogli Institute, Stanford University, february, 2015. Disponível em: https://cisac.fsi.stanford.edu/news/stuxnet, Acesso em: 12 jun 2024.

BAKER, Catherine. **As Guerras Iugoslavas da década de 1990**. Palgrave Macmillian. 2015.

BARBOSA, Alexandre Henrique Batista, **A desinformação como ferramenta da Guerra Híbrida**, Escola de Guerra Naval, 2020.

BATEMAN, Joe. **Russia's wartime cyber operations in Ukraine: military impacts, influences, and implications**. Carnegie Endowment for International Peace, 2022. Disponível em: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en. Acesso em: 22 jun. 2024.

BRASIL, Ministério da Defesa, **Política Nacional de Defesa – Estratégia Nacional de Defesa**. Brasília, DF, 2020.

BRASIL(a), Ministério da Defesa, **Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

BRASIL(b), Ministério da Defesa, **Doutrina Militar de Defesa**. Brasília, DF, 2020.

BRASIL(c), Ministério da Defesa, Exército Brasileiro, Comando de Operações Terrestres, **Manual de Campanha de Guerra Cibernética,** Brasília, DF, 1ª Edição 2017.

CARR, Jeffrey. **Inside Cyber Warfare: Mapping the Cyber Underworld**. 2. ed. Sebastopol: O'Reilly Media, 2011.

CLARKE, Richard A.; KNAKE, Robert. **Guerra Cibernética: A Próxima Ameaça à Segurança e o Que Fazer a Respeito**. Tradução de Alan Oliveira de Sá, Fabian Martins da Silva e Misael Sousa de Araújo. Rio de Janeiro: Brasport, 2015.

CLARKE, Richard A.; KNAKE, Robert K. **The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats**. New York: Penguin Press, 2019.

CLAUSEWITZ, Carl Von. **On war**. Da Guerra. São Paulo: WWF Martins Fontes, 1979.

EDELMAN, R David, 'introdução', **Repensando a Guerra Cibernética: As Relações Internacionais da Disrupção Digital** (Nova York, NY, 2024; edn online,

Oxford Academic, 21 de fevereiro de 2024), https://doi.org/10.1093/9780197509715.003.0001, acessado em 05 de junho de 2024.

EGLOFF, Florian J. **A Brief History of Cyberspace: Origins and Challenge**s. In: SHACKELFORD, Scott J. et al. The Cambridge Handbook of International and National Cyber Security Law. Cambridge: Cambridge University Press, 2020. Disponível em: https://academic.oup.com/book/41488/chapter/352894622. Acesso em: 24 jun. 2024.

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER (E-ISAC). **Analysis of the Cyber Attack on the Ukrainian Power Grid**. Disponível em: https://icscsi.org/library/Documents/Cyber_Events/E-ISAC%20-%20Analysis%20of%20the%20Cyber%20Attack%20on%20the%20Ukrainian%20Power%20Grid.pdf. Acesso em 20 Jul. 2024.

FEATHERLY, Kevin, **ARPANET**. Disponível em: https://www.britannica.com/topic/ARPANET, acesso em: 05 de jun 2024.

GREENBERG, Andy. **Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers**. New York: Doubleday, 2019.

KASPERSKY. **Types of malware**. Kaspersky Resource Center. Disponível em: https://www.kaspersky.com.br/resource-center/threats/types-of-malware. Acesso em: 27 jun. 2024.

KREPINEVICH, Andrew F. **Cyber warfare: a “nuclear option”?** Washington, DC: CSABA, 2012.

LANGNER, Ralph. **Stuxnet: dissecting a cyberwarfare weapon**. Focus, maio-jun. 2011.

LEWIS, James Andrew. **Cyber War and Ukrain**e, Center for Strategic International Studies, publicado em jun 2022, disponível em: https://www.csis.org/analysis/cyber-war-and-ukraine, acesso em 05 de mai de 2014.

LIBICKI, Martin C. **Cyberspace is not a warfighting domain**. I/S: a Journal of Law and Policy for the Information Society, v. 8, n. 2, 2012.

LILES, Samuel; et a.. **Applying traditional military principles to cyber warfare**. In: C. CZOSSECK; OTTIS, R.; ZIOLKOWSKI, K. (Ed.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012.

LIMNEL, Jarno. **The Exploitation of Cyber Domain as Part of Warfare: Russo-krainian War**. International Journal of Cyber-Security and Digital Forensics, vol 4, 2015).

MAHNKEN, Thomas G. **Strategic theory**. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. Strategy in the contemporary world. 3. ed. Oxford: Oxford University Press, 2010.

MUELLER, Grace B.; JENSEN, Benjamin; VALERIANO, Brandon; MANESS, Ryan C.; MACIAS, Jose M. **Cyber Operations during the Russo-Ukrainian War**. Center for Strategic International Studies, 13 jul. 2023. Disponível em: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Acesso em: 17 jul. 2024.

OSADCHUK, R. **Undermining Ukraine: How the Kremlin employs information operations to erode global confidence in Ukraine**. Atlantic Council, 22 fev. 2023. Disponível em: https://policycommons.net/artifacts/3495932/undermining-ukraine-final/4296522/. Acesso em: 16 jul. 2024.

PERON, Alcides E. dos R. **Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA.** In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). Relações Internacionais Cibernéticas (CiberRI): oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Editora da UFPE, 2016. (Defesa & muros virtuais, 3).

PROENÇA JR, Domício. **Promessa tecnológica e vantagem combatente**. Revista Brasileira de Política Internacional, v. 54, n. 2, 2011, p. 173-188. Disponível em: http://www. scielo.br/pdf/rbpi/v54n2/v54n2a09.pdf. Acesso em: 30 mai. 2024.

ROVNER, Joshua. **Warfighting in Cyberspace. War on the Rocks**, publicado em 17 mar. 2021. Disponível em: https://warontherocks.com/2021/03/warfighting-in-cyberspace/. Acesso em: 24 jun. 2024.

SALUSCHEV, Sergey. **Annexation of Crimea: Causes, Analysis & Global Implications**, Global Societies Journal, Volume 2, 2014, Disponível em: https://escholarship.org/content/qt5vb3n9tc/qt5vb3n9tc.pdf?t=ndsd8r. Acesso em 29 jul 2024.

SANGER, David E. **The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age**. New York: Crown, 2018.

SHELDON, John B. **The rise of cyberpowe**r. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Org.). Strategy in the contemporary world: an introduction to Strategic Studies. 4. ed. Oxford, NY: Oxford University Press, 2013.

SINGER, P.W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know**. New York: Oxford University Press, 2014.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes; LOPES, Gills Vilar; FREITAS, Marco Túlio Delgobbo. **As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica**. Revista Carta Internacional, v. 12, n. 3, p. 30-53, 2017. Disponível em: https://www.researchgate.net/publication/322156162_As_tres_tendencias_da_guerra_cibernetica_novo_dominio_arma_combinada_e_arma_estrategica. Acesso em: 24 jun. 2024.

TEMNYCKY, Mark. **Russian cyber threat: US can learn from Ukraine**. Atlantic Council, 27 maio 2021. Disponível em:

https://www.atlanticcouncil.org/blogs/ukrainealert/russian-cyber-threat-us-can-learn-from-ukraine/. Acesso em: 24 jun. 2024.

TULIO, Alvarez de Souza, **Guerra Cibernética: Conceitos Básicos, Situação Atual no Brasil e no Mundo**, O Anfíbio, Revista do Corpo de Fuzileiros Navais, 2016.

USCYBERCOM, Command Vision for US Cyber Command, **Achieve and Maintain Cyberspace Superiority**, Disponível em: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf. Acesso em: 07 jun. 2024.

ZETTER, Kim, **Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**, Crown; First Edition (November, 2014).