ACADEMIA DA FORÇA AÉREA
DIVISÃO DE ENSINO

UTILIZAÇÃO DA GUERRA CIBERNÉTICA COMO GUERRA IRREGULAR E INFORMACIONAL: O CASO DO CONFLITO RUSSO-UCRANIANO [1]

LUCAS LACERDA DOS SANTOS MONTEIRO DA SILVA[2]
CLAUDIO PASSOS CALAZA[3]

RESUMO

O ambiente cibernético está incorporado na sociedade contemporânea, estando presente em diversos setores, como educacional e econômico, por exemplo. Dessa forma, no setor bélico não seria diferente, sendo desenvolvidos e pesquisados métodos para utilização e exploração desse meio com interesses políticos e militares. Portanto, a importância do estudo da guerra cibernética se refere no entendimento e identificação desses métodos, seja para defesa ou ataque. Além disto, o combate moderno se desenvolve por diversos meios, sendo o ambiente cibernético apenas um deles. Assim surge, também, a importância de estudar como esse tipo de guerra se relaciona com ouros métodos de combate. Por isso, este artigo tem como objetivo analisar a guerra cibernética, relacionando-a com a guerra irregular e informacional, unindo estes conceitos com o conceito de guerra híbrida e, através de um estudo de caso do conflito russo-ucraniano, esclarecer de que forma a guerra cibernética atua em conformidade com outro métodos de combate regular e irregular.

Palavras-chave: Guerra Cibernética. Guerra Informacional. Guerra Irregular. Guerra Híbrida.

---

1 Artigo apresentado para Avaliação Final do Trabalho de Conclusão de Curso, como pré-requisito para a conclusão do Curso de Formação de Oficiais Aviadores da Academia da Força Aérea de Pirassununga/ SP.

2 Cadete do 4º Esquadrão da Academia da Força Aérea – Pirassununga/ SP.

3 Coronel Dentista R1, mestre em Ciências Aeronáuticas pela UNIFA, especialista em História Militar pela UNISUL, docente da disciplina de História Militar da Academia da Força Aérea (AFA) - Pirassununga/ SP

USES OF CYBER WARFARE AS IRREGULAR AND INFORMATIONAL WARFARE: THE CASE OF THE RUSSIAN-UKRAINIAN CONFLICT

ABSTRACT

The cyber environment is incorporated in contemporary society, being present in several sectors, such as educational and economic, for example. Thus, in the military sector it wouldn't be different, being developed and researched methods for the use and exploitation of this context with political and military interests. Therefore, the importance of studying cyber warfare refers to the understanding and identification of these methods, whether for defense or attack. In addition, modern combat is developed by various ways, being the cyber environment just one of them. Thus arises, also, the importance of studying how this type of war relates to other methods of combat. Therefore, this article aims to analyze cyber warfare, relating it to irregular and informational warfare, uniting these concepts with the concept of hybrid warfare and, through a case study of the Russian-Ukrainian conflict, clarifying how cyber warfare acts in accordance with other methods of regular and irregular combat.

Keywords: *Cyber Warfare. Informational Warfare. Irregular Warfare. Hybrid Warfare.*

INTRODUÇÃO

O documentário *Code* 2600 (2012) mostra como a era da informação influencia e controla o cotidiano de grande parte da população. Além de sua importância, essa obra também conscientiza seu público sobre o porquê deve-se temê-la, afirmando sobre a necessidade de controle da privacidade e segurança individual ao acessar o mundo cibernético.

Não apenas esta, mas também muitas outras obras como Snowden (2016), por exemplo, abordam a utilização do ambiente cibernético e os perigos que a acompanham. Isso se deve ao fato que desde sua criação, o ambiente cibernético tem sido explorado, expandido e aprimorado. Beneficiado pela popularização da internet e o crescente desenvolvimento da tecnologia, sua utilização tem sido diversificada e, atualmente, encontra-se presente em diversos setores da sociedade, como bancos, sistemas governamentais, empresas, escolas e até mesmo na esfera domiciliar.

Com sua disseminação e utilização em massa, o ambiente cibernético atraiu o interesse de diversos governos e organizações para ser utilizado como instrumento político e bélico, como é o caso do ataque cibernético de Israel a uma usina nuclear do Irã em abril de 2021, ou então, as sucessivas incursões cibernéticas da Rússia contra a Ucrânia, que precederam a invasão russa em fevereiro de 2022, ou até mesmo, investidas contra o Brasil, como foi o caso dos ataques ocorridos contra o Superior Tribunal de Justiça (STJ) em novembro de 2020, que resultaram no vazamento de dados e arquivos confidenciais das eleições.

Dessa forma, percebe-se que o ambiente cibernético pode ser alvo de diferentes instituições e ser utilizado para inúmeros fins, tornando difícil sintetizar o combate cibernético em um único conceito. Causando, portanto, o seguinte indagação: em que medida podemos caracterizar o combate cibernético diante das táticas de guerra convencionais e não convencionais?

Por isso, este artigo tem como objetivos específicos analisar os conceitos de guerra cibernética, irregular e informacional, relacionar estas definições entre si e com o conceito de guerra híbrida e realizar um estudo de caso sobre o conflito russo-ucraniano, de forma que, ao término deste artigo, seja atingido o objetivo geral de esclarecer de que forma a guerra cibernética pode ser utilizada em conformidade com outros métodos de combate regulares ou irregulares.

Para isso, este artigo busca definir os conceitos de guerra cibernética, segundo autores como Richard Clarke, Robert Knake, Raymond Parks e David Duggan; guerra informacional, de acordo com Alessandro Visacro e o documento *Cornerstones of Information Warfare,* 1997; e guerra irregular de acordo com Alessandro Visacro. E, após uma análise, buscar relacioná-los como um conceito mais abrangente do combate cibernético, comparando-o com o conceito de guerra híbrida segundo Frank G. Hoffman em seu trabalho *Hybrid Warfare and Challenges* e DANYK, MALIARCHUK e BRIGGS, no artigo *Hybrid War: High-Tehc, Information and Cyber Conflicts*. Por conseguinte, será submetido a análise o conflito russo-ucraniano, pelo viés do ambiente cibernético, para que, ao término desta pesquisa, seja atingido o objetivo deste trabalho.

Destarte, tomando conhecimento de sua utilização heterogênea, será possível não apenas saber como utilizá-lo, mas também como identificá-lo e combatê-lo. Por isso, com sua crescente popularização, como visto anteriormente, é de interesse para o oficial da Força Aérea Brasileira (FAB), independente de quadro, conhecer o ambiente cibernético e buscar desenvolver os sistemas brasileiros, protegendo suas vulnerabilidades e incrementar programas para aperfeiçoar o emprego desse método de combate, assim como outras potências no mundo já apresentaram pesquisas e investimentos em projetos com este mesmo fim, sendo elas, Estados Unidos da América (EUA) [4], Rússia, China[5], dentre outras.

1 CONCEITUALIZANDO AS DEFINIÇÕES

1.1 Breve Conceitualização Da Guerra Cibernética

Antes de relacionar a guerra cibernética como guerra irregular e informacional, é necessário que, previamente, sejam definidos estes conceitos, separadamente. O primeiro conceito a ser estabelecido, impreterivelmente, deverá ser o de guerra cibernética, podendo ser definida como “uma combinação de ataque e defesa de uma rede de computadores e operações técnicas especiais” (PARKS, DUGGAN, 2011).[6]

---

4 Para maiores informações, consultar DE RÊ, 2021.

5 Para maiores informações, consultar OLIVEIRA,2015.

6 Tradução livre: *“Cyberwarfare is a combination of computer network attack and defense and special technical operations.”*

Outra possível definição a ser abordada diz que “a guerra cibernética é o subconjunto da guerra da informação que envolve ações realizadas no mundo cibernético” (PARKS, DUGGAN, 2011).[7]

Outra elucidação do combate cibernético sugere:

> A guerra cibernética não é um novo tipo de guerra, limpa e sem vítimas, que devemos adotar. Longe de ser uma alternativa para a guerra convencional, a guerra cibernética, na verdade, pode até mesmo aumentar a chance de que um combate mais tradicional aconteça, com explosivos, balas e mísseis (CLARKE, KNAKE, 2015).

Analisando as definições apresentadas, percebe-se que elas muito diferem entre si. A principal causa disto está relacionada na forma como cada autor abordou sua caracterização da guerra cibernética.

Primeiramente, foi exposta sua definição mais técnica, que interpreta este tipo de guerra como a utilização de uma rede de computadores para ataque e defesa. Já a segunda elucidação, no entanto, aborda o conflito cibernético através do ponto de vista da guerra informacional. E, por último, sua terceira designação, explora as consequências de sua utilização, levantando a hipótese de que seu uso pode acarretar outros tipos de combate.

Reunindo os conceitos antes apresentados, pode-se inferir, portanto, que a definição de guerra cibernética é abrangente e complexa, existindo diversos pontos de vista para caracterizá-la. Por isso, ao término deste artigo será exposta a conceitualização que, de acordo com este autor, expõe de que forma ela pode se relacionar com outro meios de combate.

1.2 Conceituando Guerra Informacional

Sun Tzu, apud SCHWANFELDER (2011, p.92), em seu livro a Arte da Guerra, diz que:

> Se conheces o inimigo e a ti mesmo, então tu não precisas amedrontar-te o resultado de cem batalhas. Se conheces a ti mesmo, mas não ao inimigo, então a vitória e a derrota têm igual peso. Se não conheces nem o inimigo, nem a ti mesmo, então tu perdes qualquer batalha (2011, p.20).

---

7 Tradução livre: *“Cyberwafare is the sub-set of information warfare that involves actions taken within the cyber world.”*

Tendo este ensinamento em pauta, podemos concluir que a busca pelo conhecimento é primordial para o desempenho em qualquer conflito e que a procura pela informação e seu rigoroso controle não são uma novidade nos métodos de combate modernos.

Por isso, o segundo conceito a ser discutido será guerra informacional, podendo ser definida como "qualquer ação para negar, explorar, corromper ou destruir as informações inimigas e suas funções; protegendo-nos contra essas ações; e explorando nossas próprias funções de informação militar" (USA, 1997).[8]

Visacro, em seu livro *A Guerra na Era da Informação*, diz que "antes de ser um fenômeno político, a guerra é um fenômeno social" (2018, p. 25). Destarte, como estamos na Era da Informação, as táticas de combate serão diretamente influenciadas pela tecnologia e os fenômenos da globalização e conectividade. Em uma sociedade completamente interligada, a coleta de informações torna-se cada vez mais acessível e o interesse por essas informações aumenta a cada dia.

Entretanto, como citado anteriormente, esse fascínio pela informação para adquirir vantagens sobre outrem não é uma novidade das técnicas de combate moderno. Por isso, os grupos/entidades nacionais ou internacionais responsáveis por essas tecnologias e por promover essa conectividade trabalham todos os dias para a proteção dos seus usuários, gerando, portanto, a seguinte questão, qual a grande influência que a Era Informacional causa nos conflitos que a difere dos métodos de combate convencionais?

A resposta está na fonte dessa informação. O ambiente cibernético surge como um espaço ainda inexplorado e com possibilidades ilimitadas. A busca e a proteção da informação deixam de ser objetivos secundários do conflito e por vezes se tornam o objetivo principal, conduzindo o conflito moderno por métodos cada vez mais complexos seja por meio de disseminação de *fake news*[9] ou invadindo os sistemas de órgãos governamentais, ou causando vazamento/venda de dados, dentre outros usos.

Percebe-se, portanto, que a guerra informacional possui uma grande diversificação de seu emprego. Diante disso, este artigo abordará sua utilização na

---

8 Tradução livre: *"any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."*

9 *false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke* (Cambridge, 2022)

esfera cibernética, através da manipulação e controle de fontes de informação e bancos de dados.

1.3 Conceituando Guerra Irregular

Os filmes Apocalipse Now (1979) e Platoon (1986) dão um amostra dos horrores e das adversidades encontradas pelos combatentes na guerra do Vietnã. Contudo, essas obras retratam também a utilização da guerra irregular e as dificuldades encontradas pelo exército americano, mesmo com grandes vantagens bélicas e tecnológicas.

Este conflito evidenciou-se como um dos mais famosos exemplos do combate irregular, principalmente por conta da disseminação televisiva deste conflito. Todavia, não houve sinais claros da utilização direta da guerra cibernética nesta contenda, portanto, surge a grande questão, como relacionar a guerra cibernética com a guerra irregular?

Visacro diz, em seu livro *Guerra Irregular: terrorismo, guerrilha e movimento de resistência ao longo da história*, que:

> Em termo práticos, guerra irregular é todo conflito conduzido por uma força que não dispõe de organização militar formal e, sobretudo, de legitimidade jurídica e institucional. Ou seja, é uma guerra travada por força não regular (2009, p. 13).

Analisando este fragmento do livro, podemos afirmar, portanto, que um exército militar formal não poderia, por definição, exercer o combate irregular, tampouco poderia aplicá-lo de forma legítima nos conflitos. Entretanto, nada impede de o Estado subordinar um grupo independente para exercer seus interesses e executar esse meio de combate de forma indireta.

Por isso, ainda neste mesmo livro, Visacro diz que:

> O caráter informal, dinâmico, flexível e mutável do combate irregular tem contrariado o cientificismo acadêmico, frustrando as expectativas daqueles que procuram, em vão, por padrões doutrinários rígidos, aplicáveis com a mesma abrangência encontrada na guerra regular (2009, p. 221).

Diante desse pressuposto, pode-se inferir, então, que não é possível definir a guerra irregular em uma definição única. Parte deste problema, surge pelo combate irregular ser bem abrangente, sendo reconhecido em diferentes formas pelos conflitos

ao longo da história, como a guerra do Vietnã, ou a Guerrilha do Araguaia, por exemplo.

Outro obstáculo que emerge para dificultar sua conceitualização são os agentes desse tipo de combate. Usualmente associado a guerrilhas, a guerra irregular, atualmente, é utilizada, não somente por grupos e entidades particulares, mas também por governos e entidades internacionais, como a Rússia, por exemplo, se utilizando de mercenários ou grupos independente para executar ações sem legitimidade legal, conforme demonstrado posteriormente neste artigo no conflito russo-ucraniano.

Outra dificuldade que irrompe para complicação de sua conceitualização é a mutabilidade da guerra irregular e seu constante desenvolvimento. Este tipo de combate se desenvolve e torna-se mais complexo a cada dia, surgindo táticas e estratégias diferentes de acordo com o tipo de oponente, desenvolvimento tecnológico e cultura, dessa forma, torna-se impossível sintetizá-lo em um único conceito.

Por isso, neste artigo, abordamos o ambiente cibernético como uma de suas manifestações mais recentes, apresentando os motivos e os métodos que possibilitam relacioná-lo com o conflito irregular.

2 COMO RELACIONAR A GUERRA CIBERNÉTICA À GUERRA IRREGULAR E INFORMACIONAL?

Conforme demonstrado anteriormente, é difícil definir cada um desse conceitos em uma única elucidação por conta da abrangência de meios e usos desses métodos de combate. Tendo isto em mente, surge a oportunidade de haver semelhanças entre suas definições, dessa forma, possibilitando relacioná-los.

O primeiro conceito a ser relacionado será a Guerra Informacional. A Força Aérea dos EUA (USA, 1997) em seu documento *Cornerstones of Information Warfare*, cita como exemplo da guerra informacional: “Fortalecer e defender uma instalação de computadores contra ataques aéreos é guerra de informação. Assim como usar um programa antivírus para proteger o software dessa instalação” (1997, p. 5)[10]

[10] Tradução livre: “*Hardening and defending the switching facility against air attack is information warfare. So is using an anti-virus program to protect the facility's software.”*

Analisando este trecho e corroborando com o que já foi discutido anteriormente neste artigo, na Era da Informação, um dos campos de atuação da guerra informacional será o ambiente cibernético. Dessa forma, o combate cibernético opera conjuntamente com o combate informacional por meio de ações alinhadas em um mesmo objetivo: "visar as informações e suas respectivas funções do inimigo, enquanto protege suas próprias, com a intenção de degradar sua vontade ou capacidade de lutar" (USA, 1997, p. 4).[11]

O segundo conceito a ser relacionado será o de Guerra Irregular. O Departamento de Defesa dos Estados Unidos da América, em seu *Joint Operation Concept* (JOC), Irregular Warfare: Countering Irregular Threats, nos mostra que:

> Uma das principais maneiras pelas quais o combate irregular aumenta seu alcance e impacto é através do ciberespaço, que fornece um ambiente virtual seguro para recrutar, treinar, financiar e planejar operações usando técnicas sofisticadas de ocultação. As contramedidas são complicadas pela onipresença do ciberespaço e pela facilidade e onipresença de estabelecer ou restabelecer uma presença lá. Além de se defender contra ataques, a força conjunta pode tomar medidas ofensivas para interromper o uso crescente e mais sofisticado do ciberespaço pelos adversários. Para isso, a força conjunta deve possuir acesso avançado e conhecimento tecnológico em operações de redes de computadores para explorar, atacar e defender sites, tecnologias móveis, vários sistemas de mensagens e ambientes de redes sociais, e obter sinergia entre as várias operações e mídias de redes de computadores. (2010, p. 33).[12]

Ponderando o excerto mencionado e analisando o que já foi dito antecipadamente neste artigo, sendo o combate irregular mutável e flexível, um de seus meios atuação, em decorrência de estarmos na Era da Informação, será o ambiente cibernético. Por isso, pode-se afirmar que a guerra cibernética pode exercer suas atividades alinhadas com o combate irregular, utilizando-o este conceito para agir de formas inovadora e não convencional, conforme elucidado a seguir no conceito de guerra híbrida.

---

11 Tradução livre: "*targeting the enemy's information and information functions, while protecting our own, with the intent of degrading his will or capability to fight."*

12 Tradução livre: "*One of the chief ways in which irregular threats increase their reach and impact is through cyberspace, which provides a virtual safe haven to recruit, train, finance, and plan operations by using sophisticated concealment techniques. Countermeasures are complicated by the ubiquity of cyberspace and the ease and ubiquity of establishing or reestablishing a presence there. In addition to defending against attacks, the joint force may take offensive measures to disrupt adversaries' expanding and more sophisticated use of cyberspace. To do so the joint force must possess advanced access and technological expertise in computer network operations to exploit, attack, and defend websites, mobile technologies, various messaging systems, and social network environments, and achieve synergy among the various computer network operations and media.*"

Por conseguinte, em concordância com as conclusões alcançadas, existem métodos para o combate cibernético se utilizar do combate irregular e informacional para atingir seus objetivos, porém o contrário também pode ocorrer? O conceito de guerra híbrida, que será definido a seguir neste trabalho, nos mostra que todos esses tipos de combate podem agir conjuntamente, utilizando-se uns dos outros para atingir seus próprios objetivos.

2.1 Como a Guerra Cibernética se relaciona com a Guerra Híbrida?

De acordo com o que foi concluído anteriormente, as guerras cibernética, informacional e irregular podem atuar no mesmo ambiente e agir conjuntamente. Tendo isto em mente, outro conceito que pode ser abordado para justificar seu emprego conjunto seria o de guerra híbrida.

De acordo com Hoffman em seu trabalho *Hybrid Warfare and Challenges,* o combate híbrido pode ser abordado como:

> O conceito de guerra híbrida não é particularmente novo, representando uma combinação de guerra convencional e não convencional/irregular, estendendo-se além do campo de batalha para abranger informações econômicas diplomáticas (incluindo psicológicas, cibernéticas e desinformação) e guerra política. (2009, p. 34-39).[13]

Outra abordagem sobre este método combativo pode ser extraída de DANYK, MALIARCHUK e BRIGGS, no artigo *Hybrid War: High-Tehc, Information and Cyber Conflicts,* que diz que:

> A guerra híbrida é uma combinação racional de componentes convencionais e não convencionais, com ênfase em múltiplas fontes e modos de ataque, sinergia de resultados e um alto nível de incerteza para os oponentes sobre os quais podem ser os objetivos estratégicos finais (2017, p. 9).[14]

Assim, de acordo com os excertos apresentados, a guerra híbrida pode ser definida como uma combinação de métodos de combate tradicionais e não

---

13 Tradução livre: "*The concept of hybrid warfare is not particularly new, representing a combination of conventional and unconventional/irregular warfare, extending beyond the battlefield to encompass economic, diplomatic, information (including psychological, cyber and misinformation), and political warfare."*

14 Tradução livre: "*Hybrid war is rationally combined with conventional and unconventional components, an emphasis on multiple sources and modes of attack, synergy of results and a high level of uncertainty for opponents of what final strategic goals may be."*

tradicionais buscando atingir objetivos de interesse em diversos setores, como político, econômico, social, entre outros.

Por isso, corroborando com as conclusões alcançadas anteriormente, podemos inferir que, a utilização do combate cibernético em conjunto com outros métodos de combate pode ser considerada também como guerra híbrida devido a sua flexibilidade e mutabilidade de emprego e objetivos.

Além disto seu emprego torna-se diversificado, tendo em vista que cada método de combate pode agir acompanhado de outro meio combativo, assim possibilitando inúmeras combinações e instrumentos para cada tipo de guerra atingir seu próprio objetivo em sinergia com os outros objetivos definidos para cada tipo de combate.

3 COMO A GUERRA CIBERNÉTICA VEM SENDO UTILIZADA, ATUALMENTE?

Uma vez que a guerra cibernética tenha sido conceitualizada, atingindo parcialmente o objetivo deste artigo, resta agora observar a sua aplicação nos conflitos mais recentes, de modo a ratificar os argumentos apresentados. Para isso será analisado o conflito russo-ucraniano, mas especificamente, pelo viés do ambiente cibernético.

Entretanto, antes de analisar o conflito, é necessário entender como ele surgiu. Segundo Aparecido e Aguilar (2022), no artigo *A Guerra entre a Rússia e a Ucrânia*, os atritos entre a Rússia e a Ucrânia são profundos. Dominado pela Rússia e Polônia, após sua independência, o nascimento de um nacionalismo ucraniano cresceu em oposição a esses países. Essa oposição surgiu, principalmente, do desejo do povo ucraniano de ser reconhecido como Estado e ser mais visível no cenário internacional.

Essa oposição fez com que as tensões entre esses dois países aumentassem ainda mais, principalmente por conta de sua identidade cultural. Por um lado, existe uma parte do povo ucraniano, majoritariamente no oeste do país, que possui a política pró-ocidente, buscando integrar-se ainda mais com o cenário ocidental. Por outro lado, existe a outra parte do povo ucraniano, majoritariamente no leste do país, que se opõe ao ocidente, buscando confrontá-lo e apresentando ideais parecidos com os ideais russos.

Outra característica dessa separação cultural se refere à quantidade de pessoas com etnia russa na Ucrânia, sendo a maior parte dessa população localizada

no leste do território ucraniano, dessa forma corroborando com a fragmentação ideológica da região, conforme a imagem a seguir (Figura 1)

Figura 1 – Divisão cultural na Ucrânia

Fonte: Página da Washington Post.[15]

Essa divisão cultural beneficiou a ascensão de movimentos separatistas que, apoiados pela Rússia, levaram, em 2014, à invasão russa da Criméia, com a consequente anexação deste território, e da independência dos territórios de Donetsk e Lugansk, apoiados e reconhecidos pela Rússia.

Por fim, o episódio mais recente deste conflito, se consagrou com a invasão em massa das tropas russas sobre a Ucrânia, em fevereiro de 2022, com as tensões entre os dois países aumentando ainda mais, tendo este conflito se estendido até a data de publicação deste artigo, conforme o mapa a seguir (Figura 2).

---

15 Disponível em: https://www.washingtonpost.com/news/worldviews/wp/2014/02/21/there-are-two-competing-stories-about-whats-happening-in-ukraine-theyre-both-right. Acesso em 03 jul. 2022.

Figura 2 – Mapa do Conflito Russo-Ucraniano

Fonte: Página da BBC News.[16]

Conhecendo as origens do conflito, resta agora entender como a guerra cibernética atuou e ainda atua neste embate. De acordo com SOUZA, et al, em seu artigo *Guerra Híbrida e Ciberconflitos: Uma Análise das Ferramentas Cibernéticas nos Casos da Síria e Conflito Rússia-Ucrânia*, o início das ações cibernéticas contra a Ucrânia ocorreu em 2014, conjuntamente com a invasão do território da Crimeia e dos movimentos separatistas nos territórios de Lugansk e Donetsk.

> As tropas russas tomaram o controle dos aeroportos internacionais de Sevastopol e Simferopol. Ao mesmo tempo, as tropas do Kremlin avariaram cabos de fibra óptica e invadiram o sistema operacional da empresa de telecomunicações Ukrtelecom, interrompendo, por completo, o serviço de telefonia e o acesso à internet de usuários da Crimeia (SOUZA et al, 2016, p. 5).

[16] Disponível em: https://www.bbc.com/portuguese/internacional-60517760. Acesso em 27 jun. 2022.

Analisando o trecho acima, é possível identificar alguns elementos antes descritos neste artigo. Primeiramente, a utilização da guerra cibernética na interrupção do acesso à telefonia e internet através dos ataques aos cabos de fibra óptica e ao sistema operacional da empresa Ukrtelecom, fato que corrobora com a guerra informacional através do bloqueio dos meios de comunicação do oponente.

Por outro lado, percebe-se também as ações de guerra irregular, alvejando alvos civis como aeroportos e a empresa de telecomunicações, que afetam, não apenas o exército ucraniano na região, mas também a própria população nativa, fator que corrobora, portanto, com a definição de guerra híbrida, conforme discutido anteriormente neste trabalho.

> Em maio, um dos grupos pró-Rússia, denominado “CyberBerkut”, assumiu a responsabilidade por violar o sistema central da comissão eleitoral e tentar apagar os resultados da votação presidencial. O grupo obteve, ainda, acesso a documentos confidenciais e passou a disponibilizá-los, periodicamente, em sua página na rede (SOUZA et al, 2016, p. 5).

Observando esse outro excerto, nota-se a utilização da guerra cibernética por meio da invasão do sistema central da comissão eleitoral, agindo conjuntamente com a guerra informacional através da divulgação da documentos confidenciais. Entende-se também o uso da guerra irregular por meio do fato ser utilizado para instaurar o caos ao sistema político da região, episódio que ratifica a utilização da guerra híbrida no que se refere à utilização de diferentes métodos de combate atacando o setor político/social.

> A empresa de segurança cibernética Symantec diz que um malware destrutivo foi implantado contra alvos na Ucrânia e outros países da região horas antes da invasão russa nesta quinta-feira, 24. Os ataques teriam acontecido contra organizações do sistema financeiro, de defesa, aviação e serviços de tecnologia da informação (GOULART, 2022).

Examinando este fragmento de uma publicação de uma revista, identificamos novamente os elementos da guerra cibernética sendo utilizada no combate do conflito russo-ucraniano. Dessa vez, se utilizando também dos preceitos de combate híbrido, atacando setores diversos da sociedade por métodos não convencionais com o objetivo de causar o caos, irregular – por fazer um ataque amplo e não convencional contra alvos específicos antes do início da invasão – e informacional, por atacar setores de tecnologia da informação, dificultando a comunicação e deixando-os vulneráveis para a consequente invasão das tropas russas sobre o território.

> Em 2013, surge a Operação "Armageddon", campanha russa de ciberespionagem sistemática nos sistemas de agências de governo, policiais e de defesa, a fim de apoiar a Rússia no campo de batalha. Entre 2013 e 2014, os sistemas de TI de agências governamentais ucranianas foram afetados pelo vírus computacional "*Snake" / "Uroburos" / "Turla"* (PAGLIUSI, 2022).

Analisando esse trecho extraído de um artigo, podemos perceber inicialmente a notabilidade do uso do combate cibernético pela Rússia, utilizando-se deste meio para atingir os objetivos da guerra informacional. Além disto, percebe-se também a utilização ofensiva do combate cibernético para atacar pontos de interesse que corroboram com os objetivos propostos pelo conceito de guerra híbrida.

> Em 2015, pesquisadores identificaram dois grupos de hackers russos ativos na guerra cibernética contra a Ucrânia: o APT29 (conhecido *como Cozy Bear* ou *Cozy Duke)* e o APT28 (conhecido como *Sofacy Group*, Team Czar, *Pawn Storm* ou *Fancy Bear*) (PAGLIUSI, 2022).

Nesse outro excerto, retirado da mesma pesquisa citada anteriormente, nota-se agora a utilização da guerra cibernética conjuntamente com o uso da guerra irregular, utilizando-se de grupos não estatais para atingir os objetivos do Estado, neste caso, a Rússia. Esta ação corrobora ainda os conceitos antes discutidos de guerra híbrida, se utilizando de forças legitimadas e não legitimadas para atingir o mesmo objetivo.

Assim, pôde-se afirmar que, ao longo dos anos, nesse conflito, a guerra cibernética foi utilizada de formas diferentes, porém, sempre agindo conjuntamente com outros meios de combate, agindo em conformidade com o que havia sido proposto anteriormente neste artigo.

4 RESULTADOS E DISCUSSÕES

Assim, após a revisão literária, baseada nas definições apresentadas anteriormente, e estudo de caso do conflito russo-ucraniano, chega-se à estruturação de um conceito mais abrangente sobre o assunto, sendo este que o combate cibernético é a utilização do ambiente cibernético para ataque, defesa ou instrumento de consulta e exploração de dados, contudo sua influência não se desdobra apenas dentro deste ambiente, mas também influencia e age direta e indiretamente com o

mundo exterior e sendo utilizado de forma mais ampla por entidades legais ou não em conflitos nacionais ou internacionais.

Além disso destaca-se a importância do combate cibernético em seu emprego conjunto com outros métodos de combate, de forma que tanto a guerra cibernética, quanto outro tipo de guerra podem se tornar um instrumento para atingir os próprios objetivos específicos de cada método de combate, para que no final, o objetivo principal seja alcançado, conforme destacado, exemplificado e analisado no estudo de caso do conflito russo-ucraniano.

Com esta definição mais abrangente formulada, pode-se afirmar, portanto, em que medida é possível caracterizar o combate cibernético diante das variadas táticas de guerra convencionais e não convencionais. Assim, passando por todos os objetivos específicos deste artigo e atingindo o objetivo principal de esclarecer de que forma a guerra cibernética pode ser utilizada em conformidade com outros métodos de combate regulares ou irregulares.

5 CONSIDERAÇÕES FINAIS

Ao término deste artigo, foi possível visualizar o conceito de guerra cibernética por diferentes pontos de vista dos autores citados; conceitualizar guerra informacional como qualquer ação de busca/proteção de informações para diferentes objetivos e táticas; conceitualizar guerra irregular como um método de combate mutável, flexível e dinâmico que não pode ser caracterizado tão facilmente como os métodos de combate tradicionais. E, por fim, relacioná-los para que fosse atingido o objetivo deste trabalho.

Entretanto, ao relacioná-los percebeu-se também a semelhança com um outro tipo de conceito de combate: a guerra híbrida, sendo ela uma combinação de métodos de guerra convencionais e não convencionais buscando atingir objetivos de interesse em diversos setores, como político, econômico, social, entre outros. Dessa forma, atingindo um conceito mais completo e abrangente ao término desta pesquisa.

Por conseguinte, foi submetido a análise o conflito russo-ucraniano, que, conforme exposto por trechos retirados de reportagens e pesquisas sobre o conflito, retrata como a guerra cibernética age em conjunto com outros métodos de combate na prática, corroborando com as relações que haviam sido propostas anteriormente neste trabalho.

Em vista disso, pôde-se atingir o objetivo proposto neste artigo, esclarecendo em que medida podemos caracterizar o combate cibernético diante das táticas de guerra convencionais e não convencionais e a importância indubitável deste tema.

Por isso, com a crescente utilização deste método combativo por outras forças armadas ao redor do globo, conforme exemplificado no início deste artigo, torna-se impreterível para os futuros oficiais da Força Aérea Brasileira (FAB), assim como os demais militares, desta e de outras forças, conhecer e aprender sobre a flexibilidade e mutabilidade da guerra cibernética para atingir diferentes objetivos, assim como a defesa e exploração deste método de combate.

REFERÊNCIAS

APARECIDO, J. M.; AGUILAR, S. L. C. A Guerra entre a Rússia e a Ucrânia. **Série Conflitos Internacionais**, v. 9, n. 1, p. 1-13, fev 2022. Disponível em: https://www.marilia.unesp.br/Home/Extensao/observatoriodeconflitosinternacionais/v.-9-n.-1fev.-2022.pdf. Acesso em 27 maio 2022.

APOCALYPSE NOW. Direção: Francis Ford Coppola. Zoetrope Studios. Estados Unidos. **Paramount Pictures**, 1979. 1 DVD.

CLARKE, R. A.; KNAKE, R. K. **Guerra Cibernética:** A próxima ameaça a segurança e o que fazer a respeito. Rio de Janeiro-RJ: Brasport Livros e Multimídia Ltda. 2015. 224 p.

CODE 2600. Direção: Jeremy Zerechak. ZyPIX. Estados Unidos. **ZyPIX**, 2012. Amazon Prime Video.

DANYK, Y. et al. Hybrid War: High-tech, Information and Cyber Conflictis. **Connections: The Quarterly Journal**, v. 16, n. 2, p. 5-24, 2017. Disponível em: https://www.jstor.org/stable/10.2307/26326478. Acesso em 05 maio 2022.

DE RÊ, E.; **Ciberespaço e segurança cibernética:** as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil, maio 2021. Disponível em: https://repositorio.ufsc.br/handle/123456789/223136. Acesso em 29 set 2022.

FAKE NEWS. *In*: **CAMBRIDGE DICTIONARY**. Cambridge University, 2022. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/fake-news. Acesso em 1 ago 2022

GOULART, J. Ucrânia sofreu um ciberataque horas antes da invasão russa, diz Symantec. **VEJA**, 24 fev. 2022. Disponível em: https://veja.abril.com.br/coluna/radar-economico/ucrania-sofreu-um-ciberataque-horas-antes-da-invasao-russa-diz-symantec/#:~:text=Rússia%20fez%20os%20primeiros%20ataques%20militares%20na%20região%20nesta%20quinta-feira&text=A%20empresa%20de%20segurança%20cibernética,nesta%20quinta-feira%2C%2024. Acesso em 30 maio 2022.

HOFFMAN, F. G. Hybrid Warfare and Challenges. **Strategic Studies**. Routledge, 2014. p. 329-337. Disponível em: https://smallwarsjournal.com/documents/jfqhoffman.pdf. Acesso em 05 maio 2022.

OLIVEIRA, A. R. S. **O Comprometimento Asiático Com o Desenvolvimento Cibernético da Região e a Utilização Sínica do Ciberespaço Como Extensão de Sua Estratégia Tradicional**, 2015. Disponível em: http://tede.bc.uepb.edu.br/jspui/handle/tede/3013. Acesso em 18 jul 2022.

PAGLIUSI, P. S. Guerra Cibernética russo-ucraniana: lições para o Brasil e para o mundo. **Revista do Clube Naval**, v. 2, n. 402, ago 2022. Disponível em:

http://portaldeperiodicos.marinha.mil.br/index.php/clubenaval/article/view/3189. Acesso em 30 setembro 2022.

PARKS, R. C.; DUGGAN D. P. Principles of Cyber Warfare. **IEEE Security and Privacy**, v. 9, n. 5, p. 30-35, set 2011. Disponível em: https://ieeexplore.ieee.org/document/6029360. Acesso em 10 maio 2022.

PLATOON. Direção: Oliver Stone. Hemdale Film Corporation. Estados Unidos. **Orion Pictures**, 1987. Amazon Prime Video.

PINHEIRO, A. S. A tecnologia da informação e a ameaça cibernética na guerra irregular do século XXI. **Coleção Meira Mattos: Revista Das Ciências Militares**, n. 18, 2008. Disponível em: http://ebrevistas.eb.mil.br/RMM/article/view/83. Acesso em 23 maio 2021.

SOUZA, D. R. O. et al. Guerra Hibrida e Ciberconflitos: Uma Análise das Ferramentas Cibernéticas nos Casos da Síria e Conflito Rússia-Ucrânia. **Revista Eletrônica da Estácio Recife**, Recife/PE, v. 5, n. 3, 2019. Disponível em: https://reer.emnuvens.com.br/reer/article/view/346. Acesso em 23 maio 2021.

SCHWANFELDER, W. **Sun Tzu:** A arte da Guerra. 4. ed. Petrópolis-RJ: Vozes Ltda. 2011. 92 p.

SNOWDEN. Direção: Oliver Stone. BIM Distribuizone. Estados Unidos; Alemanha; França. **Kraut Pack Entertainment**, 2016. Amazon Prime Video.

USA. UNITED STATES AIR FORCE. **Cornerstones of information warfare**. USAF, 1997. Disponível em: https://www.hsdl.org/?view&did=439911. Acesso em 21 maio 2021.

USA. UNITED STATES DEPARTAMENT OF DEFENSE. **Irregular Warfare (IW) Joint Operating Concept (JOC)**, version 2.0. USDOD, maio 2010. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf. Acesso em 21 maio 2021.

VISACRO, A. **A Guerra na Era da Informação**. São Paulo: Contexto. 2018. 224 p.

_____. **Guerra Irregular:** terrorismo, guerrilha e movimentos de resistência ao longo da história. São Paulo: Contexto. 2009. 384 p.