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

ROGÉRIO DOS SANTOS FERREIRA, Ten Cel Int

Guerra Cibernética: uma análise teórica da sua influência sobre os conflitos armados modernos.

Rio de Janeiro
2021

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

ROGÉRIO DOS SANTOS FERREIRA, Ten Cel Int

Guerra Cibernética: uma análise teórica da sua influência sobre os conflitos armados modernos.

Trabalho de conclusão de curso apresentado ao Curso Avançado de Comando e Estado-Maior da Escola de Comando e Estado-Maior da Aeronáutica.
Linha de Pesquisa: Poder Militar.
Orientador: Cristiano Link Ten Cel Av

Rio de Janeiro
2021

RESUMO

O conflito armado moderno, também conhecido como guerra de 4ª geração, vem trazendo aos planejadores militares um novo universo de complexidades, caracterizadas essencialmente pela perda do monopólio da guerra pelo Estado, pelo amplo emprego de táticas de guerrilha e pela dificuldade de identificação de combatentes e da distinção destes da população civil. Somado a tudo isso, está a elevada dependência de comunicação, controle, computação e informação (C3I), bem como a dependência de meios tecnológicos interconectados para a sua realização, o que amplia o espectro do conflito para o campo da guerra cibernética. Nesse sentido, esta pesquisa analisa de que maneira a guerra cibernética influencia os conflitos armados modernos. Por meio da revisão bibliográfica de trabalhos acadêmicos, publicados entre os anos de 2016 e 2020, selecionados pelo grau de relevância apontado pelo número de citação de cada obra, foram coletados os trabalhos mais significativos por meio da busca pelos termos “guerra cibernética” e “conflito moderno”, nos idiomas português e inglês, nas bases de dados Scopus e *Web of Science*, sendo coletadas as obras com acesso gratuito ao conteúdo integral do seu texto. Após criteriosa análise do material coletado, foi possível observar a íntima relação entre a cibernética e o conceito tradicional de guerra quando observado de perto os ataques cometidos por meio do ambiente cibernético, também denominados como guerra cibernética. Por fim, não restam mais dúvidas acerca da influência direta da guerra cibernética na condução dos conflitos armados modernos, por meio do seu impacto em todas as Expressões do Poder Nacional, haja vista sua ampla capacidade de emprego nas mais variadas Expressões do Poder Nacional que influenciam diretamente no contexto de guerra tradicional, sendo eles econômico, científico-tecnológico, psicossocial, militar e político, este último nos âmbitos interno e externo.

Palavras-chave: guerra cibernética; conflito armado moderno; expressões; Poder Nacional.

ABSTRACT

Modern armed conflict, also known as 4th generation warfare, has brought military planners a new universe of complexities, essentially characterized by the loss of the State's monopoly of warfare, the widespread use of guerrilla tactics and the difficulty in identifying combatants and the distinction of these from the civilian population. Added to all this is the high dependence on communication, control, computing and information (C3I), as well as the dependence on interconnected technological means for its realization, which broadens the spectrum of conflict to the field of cyber warfare. In this sense, this research analyzes how cyber warfare influences modern armed conflicts. Through the bibliographic review of academic works, published between 2016 and 2020, selected by the degree of relevance indicated by the number of citations of each work, the most significant works were collected by searching for the terms "cyber war" and "modern conflict", in Portuguese and English, in the Scopus and Web of Science databases, with works being collected with free access to the full content of their text. After careful analysis of the collected material, it was possible to observe the close relationship between cybernetics and the traditional concept of war when closely observing the attacks committed through the cyber environment, also known as cyber warfare. Finally, there is no longer any doubt about the direct influence of cyber warfare in the conduct of modern armed conflicts, through its impact on all Expressions of National Power, given its broad capacity for employment in the most varied Expressions of National Power that influence directly in the context of traditional warfare, being them economic, scientific-technological, psychosocial, military and political, the latter in the internal and external spheres.
Keywords*: cyber warfare; modern conflict; expressions; National Power.*

SUMÁRIO

1. INTRODUÇÃO

A evolução dos meios e métodos de se fazer a guerra, bem como suas características, resultou em um novo modelo de conflito, denominado pelos teóricos como a guerra de 4ª geração, e trouxe aos planejadores militares um novo universo de complexidades, inexistentes nas gerações anteriores. Como aponta Lind (2004), a guerra de 4ª geração caracteriza-se, principalmente, pela perda do monopólio da guera pelo Estado, pelo emprego de táticas de guerrilha por parte de grupos não estatais e pela dificuldade de identificação de combatentes e da distinção destes da população civil.

Além destas complexidades, outra característica, oriunda da evolução tecnológica dos meios e métodos do combate moderno, está a elevada dependência de comunicação e controle. Nos conflitos militares modernos torna-se impossível a desvinculação de atividades básicas da necessidade de canais digitais de comunicação, estando estes amplamente dependentes dos seus meios de comunicação, controle, computação e informação, também conhecidos como C3I, os quais não são capazes de operar sem a interconexão através de canais digitais.

Somado a tudo isso, ressalta-se a necessidade recente de interconexão de infraestruturas consideradas críticas para o adequado funcionamento dos Estados a este canal global de comunicação, por meio da Internet, tais como as infraestruturas de fornecimento de energia, abastecimento de água, a rede ferroviária, as redes hospitalares e de telecomunicações, o mercado financeiro, as indústrias essenciais, dentre outros.

Essa atual dependência tecnológica e necessidade de interconexão propiciam ao cenário dos conflitos modernos um novo leque de possíveis alvos, capazes de proporcionarem, através de ações diretas ou indiretas, efeitos cinéticos ou não cinéticos, de primeira ou segunda ordem, impactando diretamente no adequado funcionamento do Estado ou de suas Forças Armadas e, consequentemente, no resultado do combate.

Vislumbrando este cenário, os Estados Unidos criaram e implementaram uma nova arma, essencialmente tecnológica, e criaram um comando militar específico, o Comando Cibernético dos Estados Unidos, organização destinada ao emprego da Tecnologia da Informação como arma no ambiente cibernético, como relatam Clarke

e Knake (2015). Além disso, os autores ressaltam que outros países como Rússia e China seguem pelo mesmo caminho, se preparando para o campo de batalha no ambiente cibernético, por meio do desenvolvimento de seus artefatos cibernéticos.

Nesse sentido, esta pesquisa aborda a influência do emprego da cibernética como vetor e arma de combate nos conflitos modernos, visando com isso responder ao seguinte questionamento: de que maneira a guerra cibernética influencia os conflitos armados modernos? Para isso, foram elaboradas algumas questões norteadoras no sentido de guiar a pesquisa: qual o conceito dos termos cibernética e guerra cibernética? Quais as principais características dos conflitos armados modernos? Como a guerra cibernética pode ser aplicada no contexto dos conflitos armados modernos?

Desta forma, o principal objetivo deste estudo é avaliar de que maneira a guerra cibernética influencia os conflitos armados modernos. Para tanto, foram realizados os seguintes passos: identificação dos principais conceitos relacionados aos termos cibernética e guerra cibernética; identificação das principais características dos conflitos armados modernos; e compreensão de como a guerra cibernética pode ser aplicada no contexto dos conflitos armados modernos.

Como justificativa, esta pesquisa visa gerar subsídios e informações de forma a propiciar aos futuros Comandantes de Estado-Maior Conjuntos um arcabouço sólido para a tomada de decisão acerca do emprego de meios cibernéticos como vetores e armas de combate nos conflitos ou operações conjuntas que assim o permitirem.

2. METODOLOGIA

Esta pesquisa ampara-se na revisão sistemática da literatura existente acerca do seu tema e, para obtenção do material bibliográfico analisado, foram selecionadas as bases de dados Scopus[1] e *Web of Science* junto ao portal de periódicos da CAPES[2]. A escolha de tais fontes de pesquisa deu-se em virtude do volume e da relevância de seus conteúdos, sendo a base de dados Scopus pertencente à ampla rede de informações analítica da moderna companhia de publicações Elsevier, reconhecida internacionalmente por sua postura de

1Scopus - https://www.scopus.com/home.uri.
2CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pertencente ao Ministério da Educação (MEC).

disseminação de conhecimento colaborativo através da adoção de práticas de ciência aberta, com mais de 20.000 produtos no mercado; e a base de dados da *Web of Science* consolida material de mais de 20.000 revistas acadêmicas de alta qualidade, revisadas por pares e publicadas em várias partes do mundo, contando com mais de 190.000 processos de conferência.

Após a seleção das bases de dados, foi realizada uma ampla pesquisa sobre os trabalhos publicados entre os anos de 2016 e 2020, que apresentassem os termos “guerra cibernética” e “conflito moderno”, nos idiomas português e inglês. Dentre os trabalhos relacionados, foram selecionados os de maior relevância, considerando-se para isto o número de citações de cada obra. Além disso, foi empregado um filtro para seleção apenas de trabalhos que permitissem acesso gratuito ao conteúdo integral do seu texto. Tais diretrizes foram adotadas para limitar o quantitativo de obras a serem analisadas e maximizar a qualidade do material empregado na pesquisa.

Sobre a classificação desta pesquisa, podemos afirmar que, do ponto de vista de sua natureza, a mesma pode ser classificada como de caráter aplicado, o que de acordo com Prodanov (2013, p. 51), significa que a mesma possui por objetivo “gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos”, o que corrobora com a justificativa apresentada para a sua realização. Acerca de seus objetivos, esta pesquisa pode ser classificada como descritiva, haja vista que, segundo o problema de pesquisa empregado e sob a ótica de Gil (2017), a mesma objetiva realizar o estabelecimento da relação entre duas variáveis, ou seja, a guerra cibernética e os conflitos armados modernos.

Como procedimento técnico, este trabalho empregará a pesquisa bibliográfica, por meio da consulta de artigos científicos coletados e selecionados através de procedimento bibliométrico, conforme já mencionado. Sobre isso Gil (2017) aponta que, a principal vantagem deste método reside na possibilidade do pesquisador realizar a cobertura de um grupo muito mais amplo de fenômenos do que seria capaz de pesquisar diretamente.

Por fim, a abordagem do problema de pesquisa proposto se dará qualitativamente, por meio da análise dos trabalhos coletados em busca realizada nas bases de dados acima mencionadas, método este que, segundo Gil (2017), distingue-se em virtude do seu enfoque interpretativista, onde o objeto da pesquisa

deve ser compreendido sob a perspectiva daqueles que já vivenciaram o problema. No mesmo sentido, Prodanov (2013) ressalta que, na pesquisa qualitativa, são premissas básicas a interpretação dos fenômenos observados e a atribuição de significado a estes, característica esta que nos permitirá responder ao questionamento central deste estudo.

3. REFERENCIAL TEÓRICO

O conflito moderno, conhecido como guerra de 4ª geração, é um marco radical em relação aos modelos de combate anteriores. Lind (2004), pesquisador e autor de diversos livros sobre guerras e suas características, nesta obra, apresenta-nos os principais diferenciais entre a 4ª geração e suas predecessoras. O ponto mais relevante, segundo o autor, está no fato da perda do monopólio acerca da guerra por parte do Estado, passando a mesma a ser composta por conflitos armados entre grupos não estatais, de fulcro ideológico, étnico ou religioso, ou entre estes grupos e Estados soberanos. Outra característica marcante encontra-se no fato da dificuldade de identificação dos atores não estatais envolvidos no combate, em virtude da não utilização de uniformes ou outros meios de identificação, da não ostentação de armamento, da sua integração com a população civil e da operação em áreas densamente povoadas.

Lind (2004) aponta, ainda, que os conflitos modernos são marcados pelo retorno a um mundo subdividido por culturas, e não mais por meio das demarcações territoriais tradicionais, consideradas motivo de conflito e disputa nas gerações anteriores; esse outro aspecto torna ainda mais complexa a identificação e localização de tais grupos beligerantes. Essa característica apontada por Lind corrobora com a teoria apresentada na década de 90, por Huntington (1993), influente cientista político norte-americano, por meio da qual previu que os conflitos futuros ocorreriam entre civilizações e não mais entre Estados soberanos, sendo caracterizados pelas diferenças culturais entre suas partes.

Outro autor que corrobora e contribui para esta análise é Alessandro Visacro, Coronel do Exército Brasileiro pesquisador e autor de várias obras de referência acerca dos conflitos armados modernos, o qual aponta que os conflitos da Era Industrial (2ª e 3ª geração) eram, em sua maior parte, previsíveis, por estarem pautados em um número pequeno e pré-definido de ameaças, o que permitia que o

planejamento militar fosse realizado com base em hipóteses de emprego muito claras (VISACRO, 2018). Ainda sob a ótica do mesmo autor, na Era da Informação (4ª geração), com a perda do monopólio estatal sobre a guerra, ocorreu uma fragmentação de ameaças e a proliferação de elementos não estatais nos conflitos armados.

Além destes fatores, em virtude da atual dependência tecnológica em todas as esferas estatais e de infraestrutura crítica, outro meio de combate foi inserido nos conflitos armados modernos, o cibernético. P. W. Singer, diretor do Centro de Segurança e Inteligência para o século XXI da *Brookings Institution*, e A. Friedman, diretor de pesquisas do Centro para Inovação Tecnológica da *Brookings Institution*, (SINGER; FRIEDMAN, 2017) descrevem o ocorrido na Operação Pomar, missão israelense que se iniciou como uma operação cibernética de espionagem, culminando em uma operação militar direcionada a uma base de processamento nuclear na Síria, em setembro de 2007. Nesta operação, sete caças F-15 israelenses adentraram no território sírio, sem serem detectados pelo sistema de segurança militar, e bombardearam o complexo nuclear de Kibar, graças a um artefato cibernético implantado no sistema de radares da Síria, que os fez observar, durante toda a operação, imagens falsas de um espaço aéreo completamente limpo.

Richard A. Clarke, professor da *Harvard Kennedy School*, consultor de segurança cibernética da *ABC News* e presidente da consultoria *Good Harbor*, e Robert K. Knake, membro do Conselho de Relações Exteriores dos EUA com mestrado em *Harvard* em segurança internacional, destacam a importância dada pelos EUA a este novo cenário de combate quando apontam a criação, em outubro de 2009, do Comando Cibernético dos Estados Unidos, órgão militar destinado ao emprego da Tecnologia da Informação como arma no ambiente cibernético (CLARKE; KNAKE, 2015). Além disso, os autores ressaltam que novos Estados também seguem por este mesmo caminho, no emprego de unidades militares cibernéticas, como Rússia e China.

Todo esse interesse por esta nova plataforma de combate mostra-se muito mais evidente após o lançamento da obra de Kim Zetter, jornalista premiada pela cobertura de cibercrime, liberdade civil, privacidade e segurança para a revista *Wired*, a qual divulga toda a pesquisa por detrás do emprego de um *worm*[3],

3*Worm* - programa de computador independente, do tipo malware, que se replica com o objetivo de se espalhar para outros computadores.

conhecido como Stuxnet, supostamente de forma conjunta entre os EUA e Israel, durante os anos de 2009 e 2011, empregado em um ataque cinético, por meio cibernético, à usina de enriquecimento de urânio de Natãnz, no Irã (ZETTER, 2017). Tal arma cibernética foi responsável pela destruição de centenas de centrífugas empregadas no processo de enriquecimento de urânio no Irã, durante os anos citados, por meio do aumento da frequência de rotação das mesmas, enquanto manipulava os dados de controle, de forma a exibir valores de rotação e temperatura nos padrões normais de operação, impossibilitando a percepção do ataque pela equipe técnica da usina e atrasando o programa nuclear iraniano.

Além disso, com o fulcro de simplificar nossa análise acerca do tema, cabe-nos destacar que, conforme apresentado pela Escola Superior de Guerra (ESG, 2019), para uma melhor compreensão da estrutura do Poder Nacional, que, apesar de uno e indivisível, podemos analisá-lo através de suas manifestações, em suas cinco expressões, que são: política, econômica, psicossocial, militar e científico-tecnológica; as quais estão intimamente relacionadas com o alcance e a manutenção dos Objetivos Nacionais, os quais influenciam diretamente na condução dos conflitos armados modernos.

Todo esse arcabouço de informações visa amparar a escolha do tema desta pesquisa, de forma a sustentar a motivação deste pesquisador em aprofundar sua análise acerca da aplicabilidade dos meios e métodos cibernéticos, bem como da sua influência sobre os conflitos armados modernos, através da análise da sua influência nas Expressões do Poder Nacional.

3.1. Conceituações

Em vista da natureza do assunto, importante se faz, em um primeiro momento, conceituar as características dos conflitos de 4ª geração. Autores como Lind (2004), Visacro (2018) e Huntington (1993) ajudam a entender as características desse conflito, marcado pela perda do monopólio estatal da guerra e pela consequente dificuldade de identificação das partes beligerantes.

Em seguida, e devidamente inserido nesse contexto, faz-se necessária a exposição de alguns conceitos relacionados à guerra cibernética. Nessa esteira de pensamento, autores como Edwards et al. (2017) relatam que o conflito cibernético é uma ocorrência comum e altamente perigosa, podendo ser iniciado pelo simples

ataque ou intrusão a um sistema informatizado, sendo devidamente alinhado às características de um conflito de 4ª geração, frequentemente impossibilitam a definição se os perpetradores estão agindo por conta própria ou como agentes de outra entidade política ou governamental.

Além desses ataques ou invasões, a guerra cibernética pode ser travada por propaganda, influência e recrutamento através de mídias sociais. Tal forma de atuação é empregada pelo Estado Islâmico, conforme apontado por Awan (2017), segundo o qual o grupo terrorista emprega vídeos, mensagens de texto e até mesmo um aplicativo próprio para disseminar mensagens radicais de ódio e para cooptar uma nova geração de ciber jihadistas.

Nesse escopo, quando se trata de ambiente cibernético, os ataques podem variar desde os praticados por criminosos em busca de ganhos pecuniários, que se apropriam, apagam ou resgatam dados, fraudam clientes de bancos, roubam identidades ou plantam *malwares*[4], até aqueles cujos motivos são políticos. Segundo Gross et al. (2016), alguns destes indivíduos são apenas “hacktivistas” ou parte de algum grupo de ciberativistas, tal com o Anonymous, porém, outros fazem parte de grupos terroristas como o Hamas ou o Estado Islâmico e, ainda outros, são agentes subsidiados por Estados nacionais como o Irã, a Coreia do Norte ou a Rússia. Gross et al. (2016) destacam ainda que estes últimos geralmente não estão em busca de obtenções financeiras, mas atendem a uma agenda política específica, de forma a fomentar uma mudança social obter concessões políticas ou paralisar um inimigo. Os autores ressaltam ainda que seus meios são geralmente pacíficos, porém, por vezes podem ser cruéis e violentos.

A análise da literatura disponível tanto para os conflitos de 4ª geração quanto para a guerra cibernética permitirá conclusões acerca da aplicação de meios e métodos modernos, ligados à cibernética, para o desenvolvimento e a solução de conflitos atuais e futuros. Desta forma, o presente estudo poderá auxiliar as Forças Armadas na tomada de decisão, no sentido de prepararem-se adequadamente para combater nesse novo ambiente.

4*Malware*: abreviação de "software malicioso" (do inglês, *malicious software*) e se refere a um programa de computador desenvolvido para infectar um computador ou outro ativo de informação.

3.2. Conflito armado moderno

Para contextualizar os modelos de engajamento em combate envolvidos no conflito armado moderno, será abordado, em primeiro lugar, o conceito de gerações de guerra desenvolvido por William S. Lind (2004). Este autor conduziu um estudo acerca da forma como as guerras foram se desenvolvendo ao longo dos períodos históricos, desde a Paz de Vestfália, em 1648, até os dias atuais.

Segundo Lind, a primeira geração teria sido marcada pela tática de linhas e colunas, com combates formais, ordenados, com grande distinção entre soldados e população civil. A segunda geração, chamada de guerra de atrito, teria sido desenvolvida pelos franceses durante a Segunda Guerra Mundial, caracterizando-se pelo grande poder de fogo, sendo a mesma sintetizada pela frase “a artilharia conquista, a infantaria ocupa”.

A terceira geração, também originada na Segunda Guerra Mundial, pelas tropas alemãs, ficou conhecida por *“blitzkrieg”*, ou guerra de manobra, e foi baseada não em poder de fogo ou atrito, mas na velocidade, surpresa e deslocamento mental e físico, e sua principal tática era atacar o inimigo pela retaguarda. Por fim, a quarta geração é representada pela mudança mais radical desde a Paz de Vestfália, sendo sua principal característica a perda do monopólio do Estado sobre a guerra. Nesta forma de combate não existe uma distinção clara entre combatentes e a população civil, combatentes estatais lutam contra organizações não-estatais, como grupos terroristas, sendo marcada pelo retorno a um mundo de culturas, e não mais de Estados.

Outro aspecto característico é que, na guerra de quarta geração, os combatentes não são necessariamente signatários das Convenções de Genebra e são de difícil identificação em virtude da ausência de insígnias distintivas e de sua mistura em meio à população civil. Como exemplo, células ligadas a grupos como Hamas, Hezbollah e às FARC podem estar infiltradas em qualquer ambiente e, ainda segundo o autor, em todos os lugares o Estado está perdendo a guerra.

Tais informações permitem-nos cumprir uma das etapas definidas para esta pesquisa, a identificação das principais características dos conflitos armados modernos, por meio dos apontamentos extraídos das obras de Lind, Visacro e Huntington.

3.3. Guerra cibernética

Nesse contexto de conflitos modernos, de quarta geração, importante notar o crescente uso, por agentes estatais ou não-estatais, de recursos da rede de comunicação e computação (recursos cibernéticos) para a realização dos mais variados tipos de agressão. Dessa forma, surge o conceito de Guerra Cibernética, ou seja, aquela que utiliza do ciberespaço para ser travada.

De acordo com Edwards et al. (2017), o conflito cibernético é relativamente comum, porém, com um potencial elevado de periculosidade. As agressões cibernéticas ocorrem diariamente no mundo todo, seja pela ação de *hackers* com interesses financeiros ou pela ação de grupos terroristas com uma agenda política bem definida, procurando fomentar uma mudança psicossocial, obter concessões políticas ou paralisar um inimigo, utilizando, muitas vezes, de meios cruéis e violentos (GROSS et al., 2016).

Pelo exposto, nem só de invasões virtuais e obtenção de dados ocorrem os conflitos cibernéticos. De fato, grupos como o Estado Islâmico (EI) se utilizam de vídeos, mensagens eletrônicas de texto, disseminando ódio, e até mesmo de um aplicativo próprio para radicalizar e criar uma nova geração de ciber jihadistas. Através de ferramentas modernas, como as mídias sociais, dentre elas Twitter, Facebook e YouTube, esses grupos difundem sua propaganda e sua ideologia a milhares de simpatizantes on-line ao redor do mundo, permitindo o recrutamento de novos membros e o envio de mensagens-chave (AWAN, 2017).

Sendo assim, podemos afirmar que, por meio das informações fornecidas pelas obras de autores como Singer, Friedman, Clarke, Knake, Zetter, Gross, Edwards e Awan, fomos capazes de cumprir mais uma etapa desta pesquisa, a identificação dos principais conceitos relacionados aos termos cibernética e guerra cibernética.

4. APRESENTAÇÃO DOS DADOS

De forma a alcançar os objetivos propostos no presente estudo, foi realizada uma síntese bibliográfica de uma série de trabalhos publicados, especialmente selecionados de forma metódica, como descrito na metodologia desta pesquisa, e as

considerações desses estudos auxiliarão na compreensão das formas como a guerra cibernética pode ser aplicada no contexto dos conflitos armados modernos.

Inicialmente, observa-se que a sociedade atual é marcada pela ampla dependência tecnológica, estando setores críticos para o Estado, como, por exemplo, os setores, energético, hídrico, petrolífero, logístico, financeiro e de telecomunicações, todos conectados a complexas redes de informação, por vezes globais, indispensáveis a seu funcionamento, tais como a Internet das Coisas (IoT) ou os sistemas ciber-físicos (IIoT), típicos da chamada Indústria 4.0, ou 4ª Revolução Industrial, a qual é baseada em processos automatizados de produção, como nos aponta Preuveneers e Ilie-Zudor (2017).

Contudo, os componentes tecnológicos de maneira geral são vulneráveis a ameaças, sejam elas naturais, tais como eventos climáticos, ou humanas, como terrorismo e ciberataques, com efeitos caracterizados pela incerteza, segundo Pescaroli et al. (2018). Porém, a conexão das instalações industriais à Internet e ao monitoramento em nuvem aumenta, exponencialmente, os riscos cibernéticos (PREUVENEERS et al., 2017), os quais variam desde mera curiosidade, passando pela obtenção de dados sensíveis e chegando até à sabotagem industrial.

Corroborando com essa preocupação, Scholz et al. (2018) explica que a revolução digital, caracterizada pela melhoria de todos os fatores ligados aos dados digitais, tais como velocidade, capacidade de armazenamento e forma de disponibilização/comunicação, representa uma grande transição na evolução humana, contudo, pode trazer consigo efeitos colaterais indesejados, podendo tais informações serem manipuladas, colocando em risco inclusive a democracia.

Além disso, de acordo com Preuveneers et al. (2017), danos a sistemas de tecnologia podem gerar eventos em cascata, ou seja, emergências secundárias, e, assim, promover grandes prejuízos a um Estado, principalmente em se tratando de um sistema crítico de infraestrutura. Cabe ressaltar que, independentemente da causa de um eventual dano a um sistema crítico de infraestrutura, como telecomunicação, transporte ou energia, por causa natural ou humana, cinética ou cibernética, os resultados podem ser semelhantes, dificultando o planejamento de uma defesa e o gerenciamento de emergências (IBIDEM, 2018).

Satchidanandan e Kumar (2017) ressaltam que, dentre os possíveis resultados, causados apenas por ataques cibernéticos, além dos prejuízos

econômicos, não podem ser descartados os riscos físicos de ferimentos e até de perda de vidas. Tal situação torna-se ainda mais preocupante enquanto estudos de vários autores, dentre eles, Ravi Sen (2018), mostram que ataques cibernéticos estão em crescente evolução, tanto em termo de quantidade de ataques quanto no volume de dados expostos, apesar de todo o investimento realizado em cibersegurança.

Tendo em vista as formas de ataque supracitadas, especialistas vêm se questionando sobre até que ponto um ataque cibernético pode desencadear uma guerra, que pode valer-se de meios cibernéticos ou até cinéticos. Nessa linha de pensamento, Sleat (2018) argumenta que, mesmo que os ataques não sejam físicos ou violentos, mesmo que não sejam utilizados os domínios tradicionais da guerra (terra, mar e ar) ou, ainda, mesmo que sejam contra atores não-humanos, eles são agressivos, gerando, normalmente, a necessidade de retaliação, o que pode gerar um movimento de escalada para um conflito armado.

Sleat (2018) compara ainda, como exemplo hipotético, um ataque cibernético que desabilite totalmente a operação de uma fábrica, mas sem ferir ninguém, como ocorreria no emprego de uma bomba que, além de destruir a fábrica causaria perdas de vidas humanas, alegando que, ainda assim, ambos os casos podem ser considerados bélicos em termos dos danos causados.

Sob outro enfoque, além da forma de guerra cibernética apontada até agora, que se caracteriza por uma invasão cibernética seguida de retaliação, cibernética ou cinética, Golovchenko et al. (2018) ressaltam o que chamaram de “guerra e desinformação on-line”, apontado como um dos dez maiores riscos globais, cujo principal alvo é a sociedade civil. Segundo dados levantados por esses estudiosos, na esteira da crise na Ucrânia que estourou entre os anos 2013 e 2014, o governo russo foi acusado de orquestrar campanhas de desinformação contra o governo ucraniano e países ocidentais, empregando ferramentas cibernéticas controladas pelo Estado, o que levou a uma onda de medidas contra-desinformação no ocidente, de forma a combater o que foi visto como uma ameaça à democracia, segurança e estabilidade internacionais.

Ainda segundo os mesmos autores, na era das mídias sociais um único indivíduo pode apresentar mais influência do que os meios convencionais de comunicação de massa (televisão, jornais ou revistas), ou até mesmo do que órgãos

estatais, de forma que a guerra de informação precise evoluir e adaptar-se adequadamente a este novo cenário.

Os estudos de Golovchenko et al. (2018) concluem, ainda, que a guerra de informação, ou seja, o uso estratégico de informação e desinformação para atingir objetivos políticos e militares, pode ser, em maior ou menor grau, patrocinada por governos, que estariam, portanto, utilizando a mente de cidadãos comuns para travar uma verdadeira batalha, cujas armas seriam as informações.

Outro aspecto extremamente relevante, a ser considerado perante a tais ameaças cibernéticas, é apontado por Daniel e Musgrave (2017), os quais concluem em sua pesquisa que grande parte das pessoas aprendem sobre política mundial a partir de fontes narrativas fictícias. Os autores argumentam que narrativas na ficção e na cultura popular são consideradas tão importantes como as fontes oficiais, como monografias e artigos científicos, para as definições relativas à crença da construção social e a disseminação de ideias e identidades (DANIEL; MUSGRAVE, 2017), propiciando dessa forma a ampliação de desinformação através de fontes não confiáveis.

Nesse sentido, deve ser destacado, primeiramente, o poder da mídia social para grupos como o Estado Islâmico (EI). Awan (2017) demonstra que, com o uso dessa ferramenta, o Estado Islâmico planejava seus ataques, motivo pelo qual o governo iraquiano foi obrigado a bloquear o acesso a muitas contas de mídias sociais. Além disso, Awan (2017) ressalta características-chave dos indivíduos simpatizantes com a narrativa do EI, bem como daqueles que lutam pela causa da organização. Com isso, a partir da coleta e da análise dos dados, o autor observa que, em alguns casos, tais indivíduos estão em busca apenas de uma descarga de adrenalina ou de um pouco de emoção, indicando a atração de pessoas distintas, com os mais variados objetivos e visões.

Em sua conclusão, o autor afirma que, devido à necessidade permanente do Estado de amparar os devidos processos penais de infratores identificados, é importante estar constantemente atualizado com relação às mídias sociais, enquanto se entende o papel dessa ferramenta para o EI e outros grupos equivalentes.

Outro aspecto relevante acerca das ações cibernéticas é a dificuldade de atribuição de culpabilidade. Edwards et al. (2017) apontam que, não raro, é difícil

identificar se o agente está ligado a órgãos oficiais de governo, se é um ativista ligado a grupos que podem ser, ou não, de cunho terrorista, ou, ainda, se se trata de um indivíduo independente, agindo por conta própria. Os autores ressaltam que, mesmo que o local de onde partiu o ataque seja uma agência estatal, como uma instalação militar, sempre haverá a possibilidade de dúvida quanto ao sancionamento ou não de tal operação, ou seja, pode ter sido um ato não autorizado, efetuado por um agente específico, de forma que somente o dado quanto ao local de origem não seja suficiente para a atribuição de culpa a um Estado.

Alinhados a este aspecto, Gartzke e Lindsay (2017) ressaltam a fragilidade inerente aos sistemas de comando e controle militares, incluindo neste o sistema de defesa nuclear, por sua dependência tecnológica, informacional e de redes de computação, que podem, portanto, tornarem-se alvos de ataques cibernéticos.

Observando por outro ângulo os efeitos relacionados aos ataques cibernéticos, Michael L. Gross, Daphna Canetti e Dana R. Vashdi foram responsáveis por, ao menos, dois estudos distintos sobre terrorismo cibernético (ou ciberterrorismo). No ano de 2016, os autores abordaram em sua pesquisa os efeitos psicológicos resultantes de ações de ciberterrorismo (GROSS et al., 2016) e, em 2018, em uma nova pesquisa, ressaltaram tais efeitos, ampliando-os ao bem-estar, à confiança pública e às atitudes políticas observadas.

Para Gross et al. (2016), normalmente o indivíduo comum, ao considerar uma ameaça cibernética, tem em mente a necessidade de proteção quanto a ações de hackers, os quais objetivam acesso a suas senhas e dados bancários. Por outro lado, ainda conforme os autores, ataques terroristas são normalmente percebidos apenas como tiroteios e bombardeios em locais públicos, que, portanto, ameaçariam mais que ataques cibernéticos.

No entanto, Gross et al. (2016) ressaltam que, ao se considerar o objetivo intrínseco de terroristas como sendo a destruição mental e física de seus alvos, os efeitos psicológicos das ameaças cibernéticas podem ser equivalentes aos do terrorismo cinético. Desta forma, o que se conhece popularmente como hacker, ou seja, aquele indivíduo que realiza agressões cibernéticas com os mais diversos objetivos, como fraudar clientes de bancos, apropriar-se de dados ou plantar *malwares* em sistemas de computação, pode ser considerado um criminoso político,

seja ele um ciberativista, agente de um Estado nacional (como Irã, Coreia do Norte ou Rússia) ou mesmo pertencente a um grupo terrorista, como o Hamas ou o Estado Islâmico.

Dessa forma, muitos destes ataques cibernéticos revestem-se de características terroristas, principalmente quando buscam obter concessões políticas, por meio da imposição do medo à população civil. Sendo assim, ainda que mais sutil, o terrorismo cibernético representa uma ameaça equivalente, em termos de resultados, ao terrorismo convencional.

Apesar disso, até a conclusão da pesquisa de Gross et al. (2016), nenhuma pessoa havia sido morta ou ferida por terroristas cibernéticos e nenhuma infraestrutura crítica havia sido destruída com sucesso, não sendo possível, entretanto, obter os motivos, seja por despreparo dos terroristas ou por ações defensivas adequadas, por parte dos governos ou outras agências.

Concluem, Gross et al. (2016), que a proteção cibernética das instalações, por si só, não é suficiente para eliminar os efeitos tóxicos do terrorismo cibernético, devido ao medo e à insegurança que movem as pessoas, além da militância dos ciberterroristas. Dessa forma, por mais que contem com preparo, investimento e medidas defensivas atualizadas, nenhum governo ou órgão civil poderia, de maneira efetiva, erradicar o terrorismo cibernético.

Assim, julgam os autores que os agentes responsáveis pela segurança cibernética devem considerar, sempre, o perigo que representa o terrorismo cibernético, buscando soluções que não apenas mantenham suas redes seguras, mas ampliem a sensação geral de segurança, principalmente para o cidadão comum, que está sujeito ao medo causado por estes ataques.

Cabe ressaltar, ainda, que nem todos os indivíduos têm o mesmo nível de percepção, sendo, em maior ou menor grau influenciados por ataques terroristas cibernéticos, conforme as informações que possuem. Sendo assim, aqueles que entendem claramente a natureza desse ataque e sua ameaça potencial, estão menos sujeitos a sofrerem as ações pretendidas pelos terroristas, como o próprio medo, ou, em alguns casos, o recrutamento ou a militância. Dessa forma, a avaliação de riscos e a comunicação tornam-se ferramentas importantes para o combate ao terrorismo cibernético (GROSS et al., 2016).

Além dos efeitos já apresentados, segundo Gross et al. (2018), o ciberterrorismo agrava o estresse e a ansiedade, intensifica os sentimentos de vulnerabilidade e endurece as atitudes políticas, sendo esses, entretanto, efeitos semelhantes aos causados pelo terrorismo convencional, porém, empregando de maneira maliciosa a tecnologia de computação para o seu fim. Soma-se, ainda, a tudo isso, que ambas as categorias de terrorismo (cinético e cibernético) promovem os mesmos objetivos, sejam políticos, religiosos ou ideológicos, por meio da debilitação física ou psicológica da população civil (GROSS et al., 2018).

Nessa linha de raciocínio, segundo os mesmo autores, o ciberterrorismo, mesmo quando não letal, impacta a população civil de várias maneiras, seja por meio do agravamento da ansiedade e da insegurança, pelo aumento da percepção de ameaça ou pelo estímulo às pessoas em apoiarem políticas governamentais rigorosas, sejam elas, internas (vigilância e controle da internet) ou externas (respostas militares cinéticas) (GROSS et al., 2018).

Dessa forma, à medida que se aumenta a percepção da ameaça, os indivíduos assumem opiniões políticas cada vez mais rígidas, cobrando do governo uma postura para maior regulamentação da Internet e respostas militares vigorosas em resposta a ataques cibernéticos (IBIDEM, 2018). Contudo, os pesquisadores alertam que, embora essas medidas tenham o objetivo de garantir a segurança nacional, tais políticas externas e, particularmente, internas podem afetar adversamente o discurso irrestrito necessário para uma sociedade democrática vibrante e aberta (IBIDEM, 2018).

Outro cenário avaliado pelas pesquisas analisadas é o cenário nuclear e sua capacidade de dissuasão. Segundo Gartzke e Lindsay (2017), nações que contam com essa categoria de armamento costumam anunciar seu poderio bélico abertamente, de forma a alertar aos potenciais adversários sobre os custos, de toda ordem, envolvidos em um possível ataque, reduzindo, desta forma, a possibilidade de escalada das tensões para um conflito armado.

De maneira diversa, ainda segundo os mesmos autores, os cibercriminosos normalmente ocultam suas capacidades, de modo a evitar que seus adversários sejam capazes de mitigarem determinada ameaça. Nessa esteira de pensamento, pode-se concluir que, enquanto as operações cibernéticas são, prioritariamente, de cunho efetivo (e ofensivo), as armas nucleares são melhor utilizadas apenas como

ameaça, sem a necessidade efetiva de emprego. Contudo, ao se combinar esses dois métodos de operação, verifica-se que ataques realizados através de operações cibernéticas podem representar um perigo real para a atividade de dissuasão nuclear (GARTZKE; LINDSAY, 2017).

Dessa forma, o aumento da incerteza acerca do equilíbrio de poder nuclear/cibernético pode aumentar o risco de erro de cálculo durante uma crise entre Estados, devendo ser esperado que a estabilidade estratégica em díades nucleares seja, em parte, influenciada pela capacidade cibernética ofensiva e defensiva (IBIDEM, 2017). Além disso, os autores concluem que qualquer ação que possa ser feita para proteger os sistemas de Comando, Controle e Comunicação Nucleares (NC3) contra intrusão cibernética tornará ainda mais perigosos possíveis comprometimentos bem-sucedidos, porém, não detectados, apesar de menos provável. Corroborando com essa assertiva, o governo dos EUA teria, no ano de 2013, por meio do órgão chamado *Defense Science Board*, recomendado uma ação imediata para avaliar se o poder de dissuasão nuclear norte-americano estaria plenamente apto a enfrentar uma ameaça cibernética (IBIDEM, 2017).

Tratando de aramentos modernos, não nucleares, Horowitz (2020) alerta que, embora se questione se as “novas” armas do século XXI são realmente novas, o emprego de tecnologias digitais por militares cresceu muito, assim com o conhecimento sobre tais tecnologias. Para exemplificar, o autor cita o papel da cibernética e dos drones na forma de combate por atores estatais e não-estatais, além dos avanços na área de inteligência artificial, que teriam potencial disruptivo em relação ao futuro da guerra.

Já Smeets (2017) chama a atenção para outra categoria de armamento moderno, as armas cibernéticas, ou seja, artefatos capazes de promover o acesso não autorizado a um sistema ou rede de computação, de forma a causar danos, humanos ou materiais. Stevens (2017) descreve essas armas como softwares maliciosos, empregados para invadir e danificar a rede do adversário, bem como para coleta de informações confidenciais, com potencial impacto político, social ou econômico.

Para Smeets (2017), as “ciberarmas” são, proporcionalmente, tão danosas hoje quanto foram as espadas ou metralhadoras em guerras do passado, com a diferença de serem transitórias, ou seja, uma ciberarma de hoje, muito

provavelmente, não será capaz de causar danos no futuro. Desta forma, dada essa transitoriedade, constantes investimentos são necessários para a manutenção de uma capacidade ofensiva cibernética ativa e atualizada, exigindo investimentos defensivos na mesma medida (IBIDEM, 2017).

Taddeo (2017) aponta que, com o objetivo de prepararem defesas adequadas, nações ameaçadas costumam elaborar estratégias voltadas para impedir o emprego pelo adversário de novos armamentos, ainda mais eficazes, cada vez que eles são projetados e implantados, sejam bombas, aeronaves, armas químicas, nucleares e, mais recentemente, as armas do ciberespaço. Quanto a essas últimas, as “ciberarmas”, convém ressaltar que elas possuem um custo relativamente baixo e probabilidade de sucesso muito alta. Dessa forma, elas vêm sendo muito empregadas por atores estatais e não-estatais em seus objetivos políticos (IBIDEM, 2017).

Um aspecto que contribui para o emprego dessas armas é a ineficácia de uma dissuasão cibernética, principalmente devido a fatores como o anonimato dos atores envolvidos, o alcance global dos ataques, a natureza dispersa do ciberespaço e a interconexão de redes de informação (LAN et al., 2010, apud TADDEO, 2017), ou seja, existem ainda poucos controles dos mecanismos de defesa em relação aos ataques cibernéticos.

Além disso, considerando que todo sistema digital tem suas vulnerabilidades de segurança, qualquer indivíduo com tempo, meios e determinação adequados consegue identificar e explorar tais fragilidades, mais cedo ou mais tarde, independente do nível de sofisticação do mecanismo de defesa, que tem, portanto, limitado seu potencial na dissuasão de novos ataques (TADDEO, 2017).

Outro ponto a se destacar é que a defesa cibernética pode não levar a uma vantagem estratégica, mesmo se bem-sucedida, dado que o adversário, raramente, será derrotado de uma vez, mas persistirá na ofensiva (HARKNETT; GOLDMAN, 2016, apud TADDEO, 2017). Dessa forma, no ambiente virtual o ataque torna-se tática e estrategicamente mais vantajoso do que a defesa, ou seja, a defesa continua sendo relevante e necessária no ambiente cibernético, porém, mais para garantir que, após o lançamento do ataque, o sistema resista e não como uma estratégia de dissuasão (BOLOGNA et al., 2013; BENDIEK; METZGER, 2015, apud TADDEO 2017).

Dessa forma, a defesa cibernética assemelha-se à engenharia de segurança, mitigando e gerenciando o risco após um ataque, mas não o evitando (LIBICKI 1997; RATTRAY 2009, apud TADDEO, 2017), ou seja, os esforços da defesa estão na retaliação, e não na dissuasão.

Abordagens de dissuasão como retaliação a ações cibernéticas costumam fazer referência aos modelos de dissuasão nuclear e algumas chegam a considerar a destruição mútua assegurada (*mutual assured destruction* – MAD) como adequada para dissuasão cibernética, visto que podem limitar a liberdade dos principais atores políticos na efetuação de ataques. Tal abordagem se baseia na ideia de que análises e práticas de dissuasão nuclear podem lançar luz sobre a dissuasão cibernética (TADDEO, 2017). Contudo, ao contrário da dissuasão nuclear, a dissuasão cibernética precisa ser constante, já que retaliações não cinéticas são improváveis de derrotar o oponente definitivamente, muito menos de representar ameaças finais (LIBICKI, 2009; apud TADDEO, 2017), deixando, portanto, o agressor capaz de contra-atacar e favorecendo múltiplas interações entre defensor e ofensor.

Análises iniciais (LIBICKI, 2009; apud TADDEO, 2017) afirmam que a dissuasão cibernética entre Estados é simétrica, pois ocorre entre pares, e assume-se que o defensor e o infrator compartilhem o mesmo terreno estratégico. Contudo, apesar de correta, essa visão não aborda cenários complexos, desconsiderando a capacidade de retaliação cinética do defensor com menos capacidades cibernéticas, ou vice-versa.

Tem-se, portanto, que, na teoria da dissuasão no ciberespaço, as diferenças entre conflitos cinéticos e cibernéticos, e seus impactos nas relações internacionais e nas estratégias militares, devem ser consideradas, de forma a reconhecer e superar os limites envolvidos (TADDEO, 2017). De maneira geral, Taddeo (2017) aponta que alguns conceitos tradicionalmente envolvidos em conflitos, tais como dano, violência, alvo, combatentes, armas, ataque e poder político, foram redefinidos graças à natureza não-cinética dos conflitos cibernéticos, de forma que apenas com uma compreensão clara do tema pode ser desenvolvida uma teoria de dissuasão cibernética efetiva.

Urquhart e Mcauley (2018) relatam em sua pesquisa que um crescente alvo de ataque cibernético é a internet das coisas industrial (*Industrial Internet of Things* – IIoT), principalmente por meio da negação de serviço distribuído (*Distributed Denial*

of Service – DDoS) direcionados a redes de energia elétrica, ou a invasão de sistemas de controle industrial (*Industrial Control Systems* – ICS) comumente presente em fábricas. A Internet das coisas industrial (IIoT) é uma tendência comercial emergente que visa melhorar a gestão da criação, movimentação e consumo de bens e serviços, contribuindo para os sistemas ciberfísicos (*Cyber Physical Systems* – CPS), que podem ser traduzidos como as integrações existentes entre processos físicos e sistemas de computação.

A IIoT difere da Internet das Coisas (IoT) do consumidor geral, que é aquela onde a detecção do ambiente ocorre por objetos físicos constantemente conectados e controláveis remotamente, embutidos em ambientes domésticos, ao aplicar tais tecnologias no ambiente das indústrias, contribuindo para o gerenciamento da cadeia de suprimento (IBIDEM, 2018).

Zeng et al. (2017) relatam que a China de Xi Jinping procurou reformular as práticas da governança cibernética global por meio da promoção da “soberania da Internet”, contudo, fazendo-o de maneira frágil e subdesenvolvida. Além disso, observa-se que, por conta do padrão em evolução da formação política chinesa, foram encontradas divergências e incertezas sobre o conceito supracitado, restringindo a capacidade do país de fornecer normas alternativas no ciberespaço global (IBIDEM, 2017).

Desta forma, apesar da contribuição da Internet no enfraquecimento ou dissolução de regimes autoritários na China, que, além de ser o maior deles, ainda tem a maior população em termo de Internet comercial, essa ferramenta vem sendo empregada para promoção de ambições políticas (IBIDEM, 2017).

Além da China, pelo menos mais um regime autoritário realiza o controle da Internet em seu território, a Rússia. Todavia, diferente do chinês, o governo russo não impõe obstáculo de acesso, preferindo valer-se de censuras e intimidação. Além disso, já estaria criando mecanismos para desconectar a rede russa da rede global, em caso de crise, sendo, contudo, o conceito de “crise” não divulgado (MARÉCHAL, 2017).

Denardis (2014, apud MARÉCHAL, 2017) ressalta, ainda, a existência de casos de países que desativam o acesso de sua população às redes sociais, em momentos sensíveis, tais como protestos ou eleições, sendo o caso, por exemplo, do Egito, de Uganda e do Irã.

A segurança cibernética ganhou destaque, com uma série de incidentes de segurança amplamente divulgados, dentre ataques de hackers e violações de dados que chegaram ao noticiário nos últimos anos, fato este apontado por Zimmermann e Renaud (2019). Como efeito, atores humanos, em uma variedade de funções, são geralmente considerados “um problema”, e as soluções implantadas se concentram principalmente na prevenção de eventos adversos, construindo resistência pela implementação de novas camadas de segurança e políticas que controlam humanos e restringem seus comportamentos considerados problemáticos.

Dessa forma, parte-se do pressuposto de que todos os humanos no sistema podem ter intenções maliciosas e que as soluções visam evitar tais comportamentos escusos (IBIDEM, 2019). Entretanto, o estudo de Zimmermann e Renaud (2019) propõe uma mudança na forma de enxergar o humano como um problema, de forma a apreciar o potencial desse ator no sentido de contribuir para o sucesso, em uma mentalidade de “ser humano como solução”. Essa nova abordagem incentiva a deferência à especialização, flexibilidade e aprendizado, gerando comunicação e colaboração, e depende do equilíbrio entre resistência e resiliência para o aprimoramento da segurança cibernética.

5. ANÁLISE DE CENÁRIOS

A análise dos artigos selecionados deixa claro que a segurança é um tema que precisa ser aplicado em uma gama variada de cenários, não ficando restrita a apenas ao risco de ameaça à segurança física, caracterizada pelo emprego de meios ciberfísicos, mas sim que as possibilidades são inúmeras e encontram-se em constante evolução, o que dificulta o trabalho do Estado e demais agências quanto à proteção de suas informações e sistemas. Cabe-nos ressaltar que tais cenários estão intimamente relacionados às cinco Expressões do Poder Nacional, anteriormente mencionadas, as quais influenciam diretamente na condução dos conflitos armados modernos, como será explicitado ao longo da análise desta pesquisa.

Como primeiro cenário analisado, e talvez um dos mais críticos, está o industrial e das infraestruturas críticas, relacionados com as expressões Econômica e Científico-tecnológica do Poder Nacional, de extrema relevância para o Estado, apontado por Preuveneers e Ilie-Zudor (2017) como Indústria 4.0, caracterizada pela

ampla automatização da produção, pela interconexão de suas instalações com a Internet e o amplo monitoramento em ambiente de nuvem, o que aumenta exponencialmente, os riscos quanto ataques cibernéticos.

Autores que corroboram com essa visão são Urquhart e Mcauley (2018), que relatam em sua pesquisa o crescente aumento no número de ataques cibernéticos à, por eles denominada, Internet das Coisas Industrial (IioT), com ênfase nas redes de energia elétrica ou em sistemas de controle industrial empregados em diversos setores. Sleat (2018) ressalta que, mesmo que tais ataques não sejam físicos ou violentos são agressivos, capazes de gerar necessidade de retaliação por parte do Estado, o que pode levar à escalada para conflito armado convencional.

Outro campo propício ao ataque cibernético é o informacional, relacionado com a expressão Psicossocial do Poder Nacional, apontado por Golovchenko et al. (2018), que o denominam como “guerra e desinformação on-line”, cujo principal alvo é a sociedade civil. Os autores demonstram que, duranta a crise na Ucrânia, nos anos de 2013 e 2014, o governo russo foi acusado de orquestrar campanhas de desinformação contra o governo ucraniano e países ocidentais, usando ferramentas cibernéticas controladas pelo Estado. Além disso, os autores relatam que tal emprego estratégico de informação e desinformação visam atingir objetivos políticos e militares, utilizando a mente dos cidadãos comuns para a condução de uma verdadeira batalha.

Indo além do campo meramente informacional, Awan (2017) chama a atenção para o poder das mídias sociais, principalmente quando empregadas para o atingimento de objetivos de grupos como o Estado Islâmico, empregada para o planejamento de seus ataques ou para o recrutamento e a militância, como apontam Gross et al. (2016).

Michael L. Gross, Daphna Canetti e Dana R. Vashdi, realizaram dois estudos sobre ciberterrorismo, abordando no primeiro seus efeitos psicológicos sobre a população e no segundo ampliando-os ao bem-estar, à confiança pública e às atitudes políticas observadas. Gross et al. (2016) ressaltam que os efeitos psicológicos das ameaças cibernéticas podem ser equivalentes aos do terrorismo cinético e que muitos destes ataques cibernéticos revestem-se de características terroristas, além disso, afirmam que a proteção cibernética, por si só, não é

suficiente para eliminar os efeitos tóxicos do terrorismo cibernético, por isso, faz-se necessária a ampliação da sensação geral de segurança dos cidadãos.

Sob a ótica da expressão Militar do Poder Nacional, Gartzke e Lindsay (2017) ressaltam a fragilidade e dependência tecnológica inerente aos sistemas de comando e controle militares, incluindo o sistema de defesa nuclear, apontando-os como possíveis alvos de ataques cibernéticos. Gartzke e Lindsay (2017) apontam, ainda, para a divergência entre os possíveis cenários de dissuasão nuclear e cibernética, onde o primeiro ampara-se na ameaça e o segundo na aplicação ofensiva dos meios, além disso, ressaltam que a combinação deses dois métodos de operação podem representar um risco para dissuasão nuclear.

Nesse sentido, Taddeo (2017) afirma que a dissuasão cibernética entre Estados é simétrica, pois, ambos, defensor e atacante, compartilham o mesmo terreno estratégico e, além disso, a tentativa de uma dissuasão cibernética torna-se ineficaz devido a fatores como o anonimato dos atores envolvidos, o alcance global dos ataques, a natureza dispersa do ciberespaço e a interconexão de redes de informação.

Ainda sob a mesma ótica, Edwards et al. (2017) relata a dificuldade de atribuição de culpabilidade dos agentes, pois, não raro, é difícil identificar se os mesmos estão ligados a órgãos oficiais e, mesmo que o local de onde partiu o ataque cibernético seja uma agência estatal, sempre haverá a possibilidade de dúvida quanto ao sancionamento ou não de tal operação.

Além disso, Taddeo (2017) afirma que retaliações não cinéticas a ataques cibernéticos são improváveis de derrotarem o oponente definitivamente, deixando o agressor capaz de contra-atacar, o que nos move em direção à escalada de um conflito cibernético para um conflito cinético.

Stevens (2017) descreve as armas cibernéticas como softwares maliciosos, empregados para invadir e danificar redes adversárias, bem como para coleta de informações confidenciais, e tais armas são apontadas por Smeets (2017) como tão danosas hoje quanto foram as espadas ou metralhadoras em guerra do passado, com a diferença de serem transitórias, o que requer constantes investimentos para a manutenção de uma capacidade ofensiva cibernética ativa e atualizada, exigindo investimentos defensivos na mesma medida (IBIDEM, 2017). Porém, por outro lado, o simples emprego destas armas representa um custo relativamente baixo e

probabilidade de sucesso muito alta, por isso, vêm sendo muito empregadas por atores estatais e não-estatais em seus objetivos políticos (IBIDEM, 2017).

Subindo para a expressão Política do Poder Nacional, Gross et al. (2018) apontam que, com o agravamento da ansiedade e da insegurança causadas pelo aumento da percepção de ameaças cibernéticas há um estímulo às pessoas em apoiarem políticas governamentais mais rigorosas, sejam internas ou externas. Nesse sentido, indivíduos assumem opiniões políticas cada vez mais rígidas, cobrando do governo uma postura para maior regulamentação da Internet e respostas militares vigorosas em resposta a ataques cibernéticos, podendo afetar diretamente certos preceitos democráticos (IBIDEM, 2018).

Além destes, outro cenário diretamente influenciado pelas ações cibernéticas é o âmbito internacional, também parte da expressão Política do Poder Nacional, onde, de acordo com Zeng et al. (2017), a China vem tentando reformular práticas de governança cibernética global por meio da promoção de uma “soberania da Internet”. Com isso, a China vem empregando o controle sobre a Internet dentro de seu território para a promoção de suas ambições políticas (IBIDEM, 2017).

Maréchal (2017) ressalta ainda que, além da China, pelo menos mais um regime autoritário realiza o controle da Internet em seu território, a Rússia, não através de obstáculo de acesso, mas valendo-se de censuras e intimidação, e criando mecanismos para desconectar a rede russa da rede global em caso de crise. Maréchal (2017) ressalta, ainda, a existência de casos de países que desativam o acesso de sua população às redes sociais, em momentos sensíveis, tais como protestos ou eleições, sendo o caso, por exemplo, do Egito, de Uganda e do Irã.

Diante de todos esses dados é possível afirmar que, diferentemente da opinião popular, na qual ataques cibernéticos estão limitados à ação de hackers, com o intuito de obterem vantagens financeiras ilícitas, ou ainda, da visão puramente belicosa, onde ações cibernéticas estariam voltadas exclusivamente para obtenção de informações e na promoção de danos a ativos de computação do oponente, ações cibernéticas podem e estão sendo amplamente empregadas nos mais variados cenários. Além disso, tais informações permitem-nos cumprir mais uma das etapas propostas para este estudo, a compreensão de como a guerra cibernética pode ser aplicada no contexto dos conflitos armados modernos, afetando diretamente todas as esferas do Poder Nacional.

Por fim, a análise de tais informações permitem-nos responder o problema de pesquisa proposto por esta pesquisa, comprovando que a guerra cibernética vem influenciando diretamente na condução das operações dos conflitos armados modernos, por meio do seu impacto sobre todas as Expressões do Poder Nacional, limitando, desta forma, o alcance e a manutenção dos Objetivos Nacionais.

6. CONSIDERAÇÕES FINAIS

Em virtude da crescente dependência tecnológica, vivenciada pela sociedade moderna, e pela ampla necessidade de interligação dos mais variados setores com sistemas gerenciados e monitorados por meio da Internet observa-se a necessidade de ampliarmos a atenção acerca das principais ameaças cibernéticas, bem como a sua influência no contexto dos conflitos armados modernos.

Diante dos dados analisados, observa-se que o conceito de cibernética perpassa todas as esferas que compõem a sociedade moderna, resultante da interligação e dependência tecnológica atualmente existente. Diferentemente do que se imagina no senso comum, de que o termo cibernética está relacionado unicamente aos computadores e dispositivos móveis com os quais lidamos diariamente, este estudo nos mostra que a cibernética pode estar relacionada com a forma com a qual compreendemos o mundo e até mesmo com a sensação de segurança percebida pelo cidadão comum.

Além disso, a pesquisa aponta para a íntima relação entre a cibernética e o conceito tradicional de guerra, o qual no cotidiano é percebido apenas como uma sequência de ataques cinéticos hostis entre Estados ou entre estes e atores não estatais, mas que, se mostra muito evidente quando observado de perto os ataques cometidos por meio do ambiente cibernético, os quais também são denominados como guerra cibernética.

Observa-se ainda, sob a ótica dos autores visitados, que os conflitos armados modernos seguem, de perto, o modelo proposto por Lind, marcado pelo amplo envolvimento de grupos não estatais e pela dificuldade de identificação dos atores envolvidos. Além disso, por conflito armado moderno entendem-se tanto os meios cinéticos com os não cinéticos, haja vista o amplo emprego de sofisticadas ferramentas digitais empregadas para a manipulação de informações, coleta de

dados sigilosos, planejamento de ataques terroristas ou até mesmo a sabotagem de infraestruturas críticas para o funcionamento do Estado.

Desta forma, fica clara a influência direta da guerra cibernética sobre as operações relacionadas aos conflitos armados modernos, por meio do seu impacto direto sobre todas as Expressões do Poder Nacional, podendo ser empregada em diversos cenários, seja nos campos econômico e científico-tecnológico, afetando o setor industrial e demais instalações que demandam de controle remoto de automação, seja no campo informacional, com a manipulação de informações visando a percepção da população acerca do conflito, seja no campo psicossocial, buscando alterar o comportamento da sociedade em virtude da sua percepção acerca da segurança, ou mesmo nos campos mais tradicionais, com enfoque puramente militar, visando danos estratégicos a infraestruturas essenciais ao funcionamento do Estado oponente e ao seu sistema de comando e controle, ou com enfoque político, seja no âmbito interno ou externo, buscando o atingimento de determinado objetivo.

Cabe ressaltar que, para um adequado emprego do meio cibernético em conflitos armados faz-se necessária uma parcela considerável de investimento, haja vista a característica de transitoriedade das ferramentas e vulnerabilidades exploráveis para o conflito. Além disso, mostram-se primordiais o contínuo investimento e a capacitação dos recursos humanos voltados para o emprego neste ambiente de combate.

Sendo assim, não restam mais dúvidas acerca da influência direta da guerra cibernética na condução dos conflitos armados modernos, por meio do seu impacto em todas as Expressões do Poder Nacional, limitando, desta forma, o alcance e a manutenção dos Objetivos Nacionais, haja vista sua ampla capacidade de emprego nas mais variadas esferas de poder que influenciam diretamente no contexto de guerra tradicional, com impacto comprovado nos âmbitos econômico, científico-tecnológico, psicossocial, militar e político, este último nos âmbitos interno e externo.

REFERÊNCIAS

AL-MHIQANI, M. N.; AHMAD, R.; YASSIN, W.; HASSAN, A.; ABIDIN, Z. Z.; ALI, N. S.; ABDULKAREEM, K. H. Ciber-Security Incidents: A Review Cases in Cyber-Physical Systems. **(IJACSAS) International Journal of Advanced Computer Science and Applications**, Reino Unido, ano 2018, v. 9, ed. 1, p. 499-508, janeiro 2018. Disponível em: https://thesai.org/Publications/ViewPaper?Volume=9&Issue=1&Code=IJACSA&SerialNo=69. Acesso em: 29 abr. 2021.

AWAN, I. Ciber-Extremism: Isis and the Power of Social Media. **Soc**, [*s. l.*], ano 2017, v. 54, ed. 1, p. 138-149, 15 mar. 2017. Disponível em: https://link.springer.com/article/10.1007/s12115-017-0114-0. Acesso em: 29 abr. 2021.

CLARKE, R. A.; KNAKE, R. K. **Guerra cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

DANIEL, J. F.; MUSGRAVE, P. Synthetic Experiences: How Popular Culture Matters for Images of International Relations. **International Studies Quaterly**, [*s. l.*], ano 2017, v. 61, p. 503-516, 15 mar. 2017. Disponível em: https://academic.oup.com/isq/article/61/3/503/4616603. Acesso em: 29 abr. 2021.

EDWARDS, B.; FURNAS, A.; FORREST, S.; AXELROD, R. Strategic aspects of cyberattack, attribution, and blame. **PNAS**, Estados Unidos da América, ano 2017, v. 114, n. 11, p. 2825-2830, 14 mar. 2017. Disponível em: https://www.pnas.org/content/114/11/2825. Acesso em: 29 abr. 2021.

ESG. Escola Superior de Guerra. **Fundamentos do Poder Nacional**. Rio de Janeiro: ESG, 2019.

GARTZKE, E.; LINDSAY, J. R. Thermonuclear cyberwar. **Journal of Cybersecurity**, Estados Unidos da América, ano 2017, v. 3, n. 1, p. 37-48, 14 fev. 2017. Disponível em: https://academic.oup.com/cybersecurity/article/3/1/37/2996537. Acesso em: 29 abr. 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

HUNTINGTON, S. P. The Clash of Civilizations? **Foreign Affairs**, v. 72, nº 3. 1993, pp. 22-49.

GOLOVCHENKO, Y.; HARTMANN, M.; ADLER-NISSEN, R. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. **International Affairs**, Reino Unido, ano 2018, v. 94, n. 5, p. 975-994, 14 fev. 2017. Disponível em: https://academic.oup.com/cybersecurity/article/94/5/975/5092080. Acesso em: 29 abr. 2021.

GROSS, M. L.; CANETTI, D.; VASHDI, D. R. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. **Journal of Cybersecurity**, Estados Unidos da América, ano 2016, v. 3, n. 1, p. 49-58, 15 fev. 2017. Disponível em: https://academic.oup.com/cybersecurity/article/3/1/49/2999135. Acesso em: 29 abr. 2021.

GROSS, M. L.; CANETTI, D.; VASHDI, D. R. The psychological effects of cyber terrorism. **Bull At Sci.**, Estados Unidos da América, ano 2016, v. 72, n. 5, p. 284-291, 04 ago. 2017. Disponível em: https://pubmed.ncbi.nlm.nih.gov/28366962/. Acesso em: 29 abr. 2021.

HOROWITZ, M. C. Do Emerging Military Technologies Matter for International Politics? **Annual Review of Political Science**, Estados Unidos da América, ano 2020, v. 23, p. 385-400, 15 fev. 2017. Disponível em: https://doi.org/10.1146/annurev-polisci-050718-032725. Acesso em: 29 abr. 2021.

HUMAYED, A.; LIN, J.; LI, F.; LUO, B. Cyber-Physical Systems Security – A Survey. **IEEE Internet of Things Journal**, Estados Unidos da América, ano 2016, v. 4, n. 6, p. 1802-1831, 10 maio 2017. Disponível em: https://ieeexplore.ieee.org/document/7924372. Acesso em: 29 abr. 2021.

LIND, W. S. Understanding Fourth Generation War. **Military Review**, v. 84, n.º 5, September/October. 2004, pp. 12-16.

MARÉCHAL, N. Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. **Media and Communication**, [*s. l.*], ano 2017, v. 5, n. 1, p. 29-41, 22 mar. 2017. Disponível em: https://www.cogitatiopress.com/mediaandcommunication/article/view/808. Acesso em: 29 abr. 2021.

PESCAROLI, G.; WICKS, R.T.; GIACOMELLO, G.; ALEXANDER, D. E. Increasing resilience to cascading events: The M.OR.D.OR. scenario. **Safety Science**, Reino Unido, ano 2018, v. 110, parte C, p. 131-140, 05 jan. 2018. Disponível em: https://nrl.northumbria.ac.uk/id/eprint/43503/. Acesso em: 29 abr. 2021.

PREUVENEERS, D.; ILIE-ZUDOR, E. The intelligent industry of the future: A survey on emerging trends, research challenges and opportunities in Industry 4.0. **Journal of Ambient Intelligence and Smart Environments**, [*s. l.*], ano 2017, v. 9, n. 3, p. 287-298, 12 abr. 2017. Disponível em: https://www.semanticscholar.org/paper/The-intelligent-industry-of-the-future%3A-A-survey-on-Preuveneers-Zudor/37d45ca24637d34aaa58a6c25bb3e5cc6ded312a. Acesso em: 29 abr. 2021.

PREUVENEERS, D.; JOOSEN, W.; ILIE-ZUDOR, E. Trustworthy Data-Driven Networked Production for Customer-Centric Plants. **Industrial Management & Data Systems**, [*s. l.*], ano 2017, v. 117, n. 10, p. 2305-2324, 04 dez. 2017. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/IMDS-10-2016-0419/full/html. Acesso em: 29 abr. 2021.

PRODANOV, C. C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

SATCHIDANANDAN, B.; KUMAR, P. R. Dynamic Watermarking: Active Defense of Networked Cyber-Physical Systems. **Proceedings of the IEEE**, [*s. l.*], ano 2017, v. 105, n. 2, p. 2019-240, fevereiro 2017. Disponível em: https://ieeexplore.ieee.org/document/7738534. Acesso em: 29 abr. 2021.

SCHOLZ, R.W.; BARTELSMAN, E.J.; DIEFENBACH, S.; FRANKE, L.; GRUNWALD, A.; HELBING, D.; HILL, R.; HILTY, L.; HÖJER, M.; KLAUSER, S.; MONTAG, C.; PARYCEK, P.; PROTE, J.P.; RENN, O.; REICHEL, A.; SCHUH, G.; STEINER, G.; VIALE PEREIRA, G. Unintended Side Effects of the Digital Transition: European Scientists' Messages from a Proposition-Based Expert Round Table. **Sustainability**, [*s. l.*], ano 2018, v.10, n. 2001, p. 1-48, 13 jun. 2018. Disponível em: https://doi.org/10.3390/su10062001. Acesso em: 29 abr. 2021.

SEN, R. Challenges to Cybersecurity: Current State of Affairs. **Communications of the Association for Information Systems**, Estados Unidos da América, ano 2018, v. 43, n. 1, p. 22-44, agosto 2018. Disponível em: https://aisel.aisnet.org/cais/vol43/iss1/2/. Acesso em: 29 abr. 2021.

SINGER, P. W.; FRIEDMAN, A. **Segurança e guerra cibernéticas**: o que todos precisam saber. Rio de Janeiro: Biblioteca do Exército, 2017.

SLEAT, M. Just cyber war?: Casus belli, information ethics, and the human perspective. **Cambridge University Press**, Reino Unido, ano 2018, p. 324-342, abril 2018. Disponível em: https://doi.org/10.1017/S026021051700047X. Acesso em: 29 abr. 2021.

SMEETS, M. A matter of time: On the transitory nature of cyberweapons. **Journal of Strategic Studies**, Reino Unido, v. 41, n. 1-2, p. 6-32, 16 fev. 2017. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01402390.2017.1288107. Acesso em: 29 abr. 2021.

STEVENS, T. Cyberweapons: Power and the governance of the invisible. **International Politics**, Reino Unido, v. 55, ed. 3-4, p. 482-502, 19 out. 2017. Disponível em: https://doi.org/10.1057/s41311-017-0088-y. Acesso em: 29 abr. 2021.

TADDEO, M. Just Information Warfare. **Topoi**, n. 35, p. 213-224, abril 2016. Disponível em: https://link.springer.com/article/10.1007/s11245-014-9245-8#citeas. Acesso em: 29 abr. 2021.

TADDEO, M. The Limits of Deterrence Theory in Cyberspace. **Philos. Technol.**, n. 31, p. 339-355, outubro 2017. Disponível em: https://link.springer.com/article/10.1007/ s13347-017-0290-2#citeas. Acesso em: 29 abr. 2021.

URQUHART, L.; MCAULEY, D. Avoiding the internet of insecure industrial things. **Computer Law & Security Review**, v. 34, n. 3, p. 450-466, junho 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917303217. Acesso em: 29 abr. 2021.

VISACRO, A. **A guerra na era da informação**. São Paulo: Contexto, 2018.

ZENG, J., STEVENS, T. C., CHEN, Y. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'. **Politics and Policy**, v. 45, ed. 3, p. 432-464, 09 jun. 2017. Disponível em: https://doi.org/10.1111/polp.12202. Acesso em: 29 abr.2021.

ZETTER, K. **Contagem regressiva até Zero Day**: Stuxnet e o lançamento da primeira arma digital do mundo. Rio de Janeiro: Brasport, 2017.

ZIMMERMANN, V.; RENAUD, K. Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. **International Journal of Human-Computer Studies**, v. 131, p. 169-187, nov. 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S1071581919300540. Acesso em 29 abr. 2021.