AS POSSIBILIDADES DO DIREITO INTERNACIONAL HUMANITÁRIO NO ESPAÇO CIBERNÉTICO: AS NAÇÕES UNIDAS E O *CYBER PEACEKEEPING*

André Soares Oliveira

Faculdade Paraíso do Ceará (FAP), Ceará.
asoliveira3@gmail.com

José Armando Ferreira Oliveira

Faculdade Paraíso do Ceará (FAP), Ceará.
ferreiraarmando927@gmail.com

Resumo: A regulação dos conflitos armados no Direito Internacional ganha impulso depois das Guerras Mundiais e, em especial, durante os anos de Guerra Fria e a ameaça de uso de armas nucleares em grande escala novamente. O conceito de armas, porém, sempre foi sendo ampliado diante de novas tecnologias. O surgimento e consolidação do espaço cibernético criou uma arena para atividades bélicas impensáveis na origem dos instrumentos normativos. Existe uma demanda para que a promoção e manutenção da paz alcance também esse espaço. Diante disso, tem-se o objetivo de demonstrar as possibilidades e limites de aplicação do Direito Internacional Humanitário a possíveis guerras realizadas através do ciberespaço, trazendo-se um debate a partir da necessidade de aplicação equiparada do *peacekeeping* neste domínio. Para tanto, utiliza-se de metodologia dedutiva e qualitativa com levantamento bibliográfico e análise das normas internacionais pertinentes. Destarte, compreende-se que o Direito Internacional Humanitário é extensível ao ciberespaço, haja vista que a internet pode ser considerada um meio e método de guerra, pois ao mesmo tempo que não há tratado que a proíba como instrumento da guerra, também não há nenhum que a regulamente enquanto tal. Com isso, o mandato das Nações Unidas para a manutenção da paz deve se estender ao espaço cibernético.

Palavras-chave: Guerra. *Cyber Peacekeeping*. Direito Internacional Humanitário

The possibilities of humanitarian international law on cyberspace: the United Nations and the cyber peacekeeping

Abstract: The regulation of armed conflicts in International Law gains momentum after the World Wars and during the Cold War years and the threat of the use of nuclear weapons on a large scale again. The concept of weapons, however, has always been expanded in the face of new technologies. The emergence and consolidation of cybernetic space created an arena for unthinkable warfare activities at the origin of normative instruments. There is a demand for the promotion and maintenance of peace to also reach this space. In view of this, the aim is to demonstrate the possibilities and limits of applying International Humanitarian Law to possible wars carried out through cyberspace, bringing up a debate based on the need for an equal application of *peacekeeping* in this domain. For that, a deductive and qualitative methodology is used with a bibliographical survey and analysis of relevant international norms. Thus, it is understood that International Humanitarian Law is extended to cyberspace, given that the internet can be considered a means and method of war, because while there is no treaty that prohibits it as an instrument of war, there is also no that regulates it as such. With this, the United Nations mandate for *peacekeeping* must extend to cyberspace.

Keywords: War. *Cyber Peacekeeping*. International Humanitarian Law

INTRODUÇÃO

Os tempos mudam, mas o conflito é uma constante atemporal. E quando se trata de Guerra, o seu conceito mais clássico remete a um ambiente hostil, onde os militares não distinguem quem faz e quem não faz parte do combate. Após a publicação da Carta da Organização das Nações Unidas (1945), a cooperação internacional e o princípio que veda a intervenção passaram a reger as relações dos signatários, proibindo, pelo menos em tese, a ameaça ou uso efetivo de força entre os Estados. Conquanto, pode-se observar que a comunidade internacional também implementou formas de humanização da própria guerra, sobretudo com o advento do Direito Internacional Humanitário, que busca assegurar direitos em tempos bélicos.

Hodiernamente, por intermédio da alta performance da ascensão científico-tecnológica, a internet vem linearmente ganhando destaque nas relações interpessoais e jurídicas como um modo instrumental de crescimento e desenvolvimento, mas também de ataques e vulnerabilidades notórias. Essa evolução influencia totalmente as relações internacionais, até porque o âmbito digital é um domínio onde não há fronteiras, isto é, as relações e fatos acontecem de forma instantânea.

Diante de toda essa facilidade existente no mundo cibernético, nota-se que os conflitos também chegam e podem ocorrer neste meio. Não se fala de conflitos entre usuários e sim entre dois ou mais estados com o ataque de bases digitais e tecnológicas através do ciberespaço. É desta realidade que surge o conceito de Guerra Cibernética, em que a internet é utilizada como instrumento, método ou meio em uma guerra já existente ou até mesmo é ela o pontapé inicial para a existência de uma.

A possibilidade de uma guerra com a internet sendo o seu principal método é uma discussão que vem ganhando cada vez mais notoriedade nos debates acadêmicos internacionais. Isso porque o Direito Internacional quanto à tipificação do crime de guerra no art. 8º do Estatuto de Roma não especifica a aplicação da internet como método ou meio em nenhum instrumento normativo. Nesse sentido, vê-se que essa discussão se justifica ao fomentar uma ideia de que diferentemente das grandes guerras do passado, que tiveram início sobretudo com bombardeios, uma futura guerra vai começar com uma invasão cibernética, sendo preciso prever uma possível adequação desta situação ao entendimento comum do que é uma guerra.

Ante a todo o supracitado, entende-se necessário o questionamento: Nesse contexto de guerra cibernética, partindo de uma concepção no Direito Internacional, o Estatuto de Roma abarca essa possibilidade uma possível ensejando responsabilização internacional dos comandatários da guerra cibernética? O Direito Internacional Humanitário aplica-se a esta situação? E como a ONU atuaria para a manutenção da paz no espaço digital?

Diante dessa perspectiva, esse trabalho tem como objetivo geral compreender a manutenção da paz no ciberespaço como um princípio necessário à comunidade internacional observando se o Direito Internacional Humanitário é aplicável neste domínio. Especificamente, procura-se explicitar o que é o uso da força no Direito Internacional, e como os avanços tecnológicos fomentam as novas armas e métodos de guerras, destacando-se a internet enquanto instrumento de conflito.

A hipótese é que o espaço cibernético se configura como um novo domínio de guerra na era digital, não restando dúvidas que à guerra cibernética é aplicado o art. 8º do Estatuto de Roma e a consequente responsabilização frente ao Tribunal de Haia. Além disso, mesmo não existindo uma referência específica acerca da guerra entre Estados no ciberespaço nas Convenções de Genebra, o Direito Internacional Humanitário é cabível nesse ambiente no que toca aos conflitos, pois as normas e princípios observados nos tratados que regulamentam os meios e métodos da

guerra para impedir violações a direitos humanos e civis representam o momento histórico de sua criação mas não se prendem a ele, podendo haver a ampliação ante a evolução dos meios e ambientes de guerra.

Para tanto, o método é crucial para a consecução dos objetivos. Nisto, utiliza-se do método dedutivo, partindo da ideia de premissas generalizadas e focando-as mais restritamente mediante o decorrer da pesquisa. Quanto à abordagem utilizada, trata-se de pesquisa qualitativa; quanto à sua natureza, de pesquisa básica; quanto aos seus objetivos, de pesquisa descritiva; e quanto aos procedimentos técnicos, em pesquisa bibliográfica viabilizada por meio de uma revisão de livros, artigos, trabalhos acadêmicos e de outras naturezas que tratam do crime de guerra cibernética e sua responsabilização.

1 SOBRE GUERRA E GUERRA CIBERNÉTICA: DO ESPAÇO FÍSICO AO DIGITAL

Se o conflito é algo sempre presente no cotidiano das sociedades humanas, tal conflito nem sempre tomou a forma de uma guerra. Aliás, cumpre salientar como a atividade de guerra esteve presentes nas primeiras sociedades que apresentaram características de estatalidade e, sem dúvidas, continua constante desde a Antiguidade Clássica até hoje. Inclusive, é interessante notar como a forma de fazer guerra foi modificando-se ao longo do tempo e moldando inclusive os próprios Estados (SINGER et al., 2021)

A fim de delimitar o objeto dessa pesquisa, é importante delimitar um conceito de guerra. As reflexões sobre a guerra ocupam um espaço importante nos debates teóricos desde a Antiguidade Clássica, quando se pode citar a obra ‘A Guerra do Peloponeso’, de Tucídides, ou mesmo as reflexões esparsas de pensadores tais como Maquiavel, Bodin, Rousseau, Hobbes e mesmo o próprio Locke, já que todos viveram em períodos sempre agitados por guerras no continente europeu.

Em 1832, ainda no contexto de uma Europa pós-napoleônica, surge a obra ‘Da Guerra’, publicada postumamente, e de autoria do general prussiano Carl Von Clausewitz. Essa obra inacabada constitui-se um paradigma na teoria da guerra dentro do estudo das relações internacionais. Trata-se de uma obra extensa e rica em reflexões, mas importa aqui uma reflexão seminal trazida pelo seu autor quando se propõe a conceituar a guerra. Segundo o autor, ainda que a guerra seja composta de um intrincado conjunto de variáveis, é necessária uma reflexão sobre a natureza do todo. Nesse sentido, ele evita uma conceituação enciclopédica e prefere definir a natureza da guerra como um duelo em larga escala. Trata-se de um ato de força orientado a fazer com que o seu oponente sucumba a sua vontade (VON CLAUSEWITZ, 1984). Enquanto general escrevendo em meados do século XIX, claro que a força mencionada é a força militar, porém o conceito não exclui a possibilidade de compreender o manuseio de outras forças por um Estado, com intenção de impor sua vontade a outrem, como uma guerra.

Do ponto de vista jurídico, dentro do direito internacional, o conceito de guerra deve ser procurado prioritariamente no âmbito do direito internacional vigente. Nesse sentido, a guerra constitui-se como o uso da força a fim de dirimir uma controvérsia entre Estados. A Carta das Nações Unidas de 1945, no artigo 2.4, diz que os Membros devem evitar “[...] a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado [...]” e o artigo 51 do mesmo documento consagra a legítima defesa quando afirma quando ocorrer “[...] um ataque armado contra um Membro das Nações Unidas [...]”.

A lógica esculpida na Carta das Nações Unidas é que o uso da força deve ser evitado nas relações internacionais, sendo possível a ela recorrer como legítima defesa de forma unilateral em um primeiro momento e, depois, apenas com autorização do Conselho de Segurança. De fato, o interesse aqui repousa em algumas definições desses artigos que demonstram o quão complexo é buscar uma definição legal de guerra.

Crawford (2012) chama atenção, primeiro, para a expressão ‘ameaça ou uso da força’. O autor lembra que a ameaça é uma prática comum e até bem tolerada nas relações internacionais como um desdobramento do exercício da legítima defesa. A expressão ‘uso’ é de interpretação clara, mas ‘força’ não é um conceito unívoco. A visão prevalente inclui apenas forças armadas, excluindo a força decorrente de coerção política e/ou econômica. A própria expressão ‘ataque armado’, constante do artigo 51, também reflete dificuldades por ser vista, em sua maioria, com um pensamento próprio da Segunda Guerra Mundial e ignorando a evolução das armas e do próprio modo de usá-las.

Conforme Mazzuoli (2019, p.1660), a definição de guerra deve se pautar estritamente em termos jurídicos, sendo considerada “todo conflito armado entre dois ou mais Estados, durante um certo período de tempo e sob a direção dos seus respectivos governos, com a finalidade de forçar um dos adversários a satisfazer a(s) vontade(s) do(s) outro(s)”. Não obstante, após a situação devastadora provocada pelos conflitos bélicos no século XX, a comunidade internacional passou a tratar a guerra como um ato de violência inadmitido no Direito Internacional, ou seja, internacionalmente ilícito (MAZZUOLI, 2019).

Os atos envolvendo guerras passaram a ensejar responsabilidade na esfera externa perante o Tribunal Penal Internacional, uma vez que o Estatuto de Roma prevê em seu art. 8º um rol de condutas que configuram o crime de guerra, estas que vão desde humilhações e ultrajes à dignidade da pessoa até o descumprimento das Convenções de Genebra de 1949 (ESTATUTO DE ROMA, 1998).

Nesse sentido, a Carta da Organização das Nações Unidas (ONU) contempla em seu art. 2º a proibição do uso da força no Direito Internacional, compreendendo a necessidade da manutenção da paz e da segurança internacional com pilares para o exercício dos Direitos Humanos, inclusive determinando a responsabilidade do Conselho de Segurança de zelar pela paz e segurança internacional. Essa vedação decorre das experiências devastadoras das primeira e segunda guerras mundiais, por isso o *peacekeeping*¹ tornou-se uma das principais agenda da organização.

NÓS, OS POVOS DAS NAÇÕES UNIDAS, RESOLVIDOS a preservar as gerações vindouras do flagelo da guerra, que por duas vezes, no espaço da nossa vida, trouxe sofrimentos indizíveis à humanidade, e a reafirmar a fé nos direitos fundamentais do homem, na dignidade e no valor do ser humano, na igualdade de direito dos homens e das mulheres, assim como das nações grandes e pequenas, e a estabelecer condições sob as quais a justiça e o respeito às obrigações decorrentes de tratados e de outras fontes do direito internacional possam ser mantidos, e a promover o progresso social e melhores condições de vida dentro de uma liberdade ampla (ONU, 1945).

Entretanto, a despeito dos esforços para manter a paz e para a solução pacífica das controvérsias, nota-se que a guerra em sempre ocupou um espaço nos capítulos da história da humanidade, estes que ainda continuam sendo escritos e fomentados através de novos métodos, meios e armas que conseqüentemente requerem novas estratégias e regras para manter ou buscar

¹Aqui utiliza-se este termo original para referenciar-se à manutenção da paz da ONU, que tem o objetivo de “ajudar os países a navegar pelo caminho difícil do conflito à paz (...) com a capacidade de enviar tropas e policiais de todo o mundo, integrando-os com os pacificadores civis para abordar uma série de mandatos estabelecidos pelo Conselho de Segurança da ONU e pela Assembleia Geral (UNITED NATION PEACEKEEPING, 2021 n.p.).

a paz (SALDAN, 2012). E é justamente esta característica mutável da guerra e do conflito que deixa, muitas vezes, a ONU lutando para se adaptar (ROBINSON et al, 2019).

É interessante pensar na guerra, seja qualquer de suas espécies, como um campo desconhecido, onde a informação é preciosa. Sobre isso, Arquila e Rondfeldt (1993) sugerem uma analogia em que a capacidade de informação na guerra assemelha-se a uma partida de xadrez, onde se você consegue ver todo o tabuleiro e o seu oponente apenas as próprias peças:

Para suas forças, a guerra não é mais uma função primordial de quem coloca mais capital, trabalho e tecnologia no campo de batalha, mas de quem tem as melhores informações sobre o campo de batalha. O que distingue os vencedores é o seu alcance de informações - não apenas do ponto de vista de saber como encontrar o inimigo, mantendo-o no escuro, mas também em termos doutrinários e organizacionais (ARQUILA; RONDFELDT, 1992 p. 23, tradução nossa).²

Portanto, pesquisar acerca da guerra é também estudar sua dinamicidade. Por isso, quando se insere o meio digital nessa empreitada entende-se que atualmente as relações internacionais se integram também a um ciberrelacionamento e não apenas à diplomacia e cooperação. Os conflitos internacionais ganham novos contornos ao longo do tempo, novas possibilidades, áreas, espaços e armas. Nesse sentido, a internet – tal como outros avanços tecnológicos do passado – representa, ao mesmo tempo, um instrumental de desenvolvimento e aproximação, mas também de ataques e vulnerabilidades notórias (NUNES, 2015).

Sobre isto, sabe-se que a tecnologia à serviço da guerra é uma constante na história da humanidade. Momentos de guerra representam um forte impulso de inovação, principalmente nos setores militares. Isso leva ao incremento do estado da arte ou mesmo na criação de novas tecnologias – a exemplo dos computadores, dos aviões, motores automobilísticos e mesmo da própria internet – que mais tarde servem também a fins pacíficos).

De fato, foi a Guerra Fria que intensificou o uso da tecnologia como representação de poder em um mundo em conflito. Essas eventualidades associam a guerra à tecnologia e devem ser enxergadas como de necessária compreensão temporal na era da globalização (FERNANDES, 2019), uma vez que as relações entre os Estados no tecido internacional cada vez mais são cruzadas e dependentes no ciberespaço.

Saindo de uma concepção clássica da guerra, é sabido que hodiernamente os conflitos na comunidade internacional passaram a enfrentar outro desafio: a internet e todos os desdobramentos inerentes à era digital, haja vista que a utilização da rede mundial de computadores torna a sociedade cada vez mais dependente desse mundo *on-line*, fato esse que traz consigo a ameaça inexorável de um ataque cibernético. Portanto, essa vulnerabilidade é observada por determinados grupos como uma oportunidade, onde “o mundo passa a conviver com a sombra do ciberterrorismo e, no caso dos Estados, com a possibilidade de hostilidades no ciberespaço, ou seja, uma Guerra Cibernética” (NUNES, 2010 p.11).

A guerra cibernética surge então como um novo episódio belicoso, decorrente da inevitável transformação e adequação dos conflitos à era digital (SILVA E SILVA, 2019), o seu conceito vincula-se à massiva participação dos Estados no meio digital concomitantemente à presença de atores não estatais, tais como grupos terroristas, por exemplo, porém é preciso deixar claro que o Direito Internacional Humanitário por sua natureza não se aplica a casos de cibercriminalidade ou ciberterrorismo (MELZER, 2011).

²⁴For your forces, warfare is no longer primarily a function of who puts the most capital, labor and technology on the battlefield, but of who has the best information about the battlefield. What distinguishes the victors is their grasp of information—not only from the mundane standpoint of knowing how to find the enemy while keeping it in the dark, but also in doctrinal and organizational terms”

Entretanto, em uma definição geral, considera-se guerra cibernética o conflito travado por dois ou mais estados no ciberespaço (NUNES, 2010), em que há a invasão de computadores ou redes de outra nação com o objetivo de causar transtornos, obter informações, corromper dados, entre outros danos que podem ser irreversíveis (CLARKE; KNAKE, 2015).

Há, no cerne da cibernética, uma preocupação com a relação entre comando, controle, comunicação e fluxo de informações em máquinas, em seres vivos e entre ambos. Na Guerra Fria, o desenvolvimento de tecnologias militares de inteligência artificial permitiu um debate comparativo entre indivíduo e máquina, sugerindo a possibilidade de uma convergência entre mente e *software* (LOBATO; KENKEL, 2015 p. 637)

Por sua vez, o ciberespaço pode ser aqui descrito como uma “rede globalmente interconectada de informações digitais infraestruturas de comunicações, incluindo a Internet, redes de telecomunicações, sistemas informáticos e as informações neles residentes” (MELZER, 2015 p.4). O ciberespaço é a principal elementar da guerra cibernética, isso porque graças aos efeitos da virtualização da vida social, o meio digital passou a representar um espaço intangível, em que não há fronteiras e tem-se uma cultura própria, sendo um local totalmente potencial para conflitos.

Neste sentido, o ciberespaço configura-se como um terreno em que o mundo todo está presente, sem barreiras:

As relações econômicas, jurídicas e sociais (afetivas, educacionais, familiares, interpessoais e profissionais), bem como as funcionalidades do espaço cibernético estão em constante reconfiguração, orientada pela crescente cultura da conectividade, convergência, instantaneidade e interatividade de portais, blogs e redes sociais, que se multiplicam em progressão geométrica, enquanto as tentativas de regramento sequer estão em progressão aritmética (SALDAN, 2012 p. 16)

Mesmo aqui trazendo-se um conceito ampliado de guerra cibernética e ciberespaço, enfatiza-se que, no entanto, há pouco consenso sobre muitos aspectos acerca de tais fenômenos, principalmente sobre como ele deve ser definido. Mesmo havendo ausência de compreensão, muitos núcleos militares ao longo do globo consideram o ciberespaço um domínio de guerra e tem desenvolvido doutrinas e metodologias para lutar nele. Tal falta de compreensão somada ao aumento das tensões cibernéticas é uma situação deveras preocupante, pois é inédita, em que não se tem noção dos limites e nem tampouco arcabouço no Direito Internacional (ROBINSON et al, 2018).

O século XXI tem mostrado que a guerra cibernética pode se tornar mais prevalente que a física. Destarte, infere-se que a utilização da internet e de suas ferramentas para efetivar as práticas violadoras pode inclusive ser observada nessa situação como equiparadas a utilização de armamento previsto no conceito clássico de guerra, uma vez que da mesma forma a internet é o meio para alcançar tal desiderato.

Pode-se então inferir que a segurança cibernética dos Estados passou a ser um ponto importantíssimo decorrente da crescente necessidade de utilização destes meios, e por conta disso, quando se analisa as problemáticas que envolvem o ciberespaço e o crime de guerra percebe-se uma certa dificuldade na caracterização das atividades hostis e degradantes que ocorrem nesta conjuntura colocam em dúvida a aplicabilidade do Direito Internacional Humanitário (JAS-TRAM E QUINTIN, 2011).

Diante disso, o século XXI tem mostrado que a guerra cibernética prevalecerá mais do que a física. E para de fato combater este fenômeno moderno é preciso primeiro assegurar a sua repressão equiparada nos moldes da guerra propriamente dita, uma vez que o enfraquecimento

de bases digitais provocado por ataques cibernéticos pode ser o estopim para um futuro e próximo conflito. Por a sociedade estar extremamente conectada, as redes digitais trazem uma vulnerabilidade de ameaças cibernéticas oriundas de qualquer lugar do mundo.

2 O DIREITO INTERNACIONAL HUMANITÁRIO APLICADO NO CIBER-ESPAÇO

No Direito Internacional há diversos instrumentos com o intuito de garantir a proteção do indivíduo. “Sob o título de direito internacional dos direitos humanos, os padrões são estabelecidos para a responsabilidade dos Estados com relação aos direitos e liberdades de indivíduos e dos povos” (CICV, 2005 p.35). Dessa forma, o Direito Internacional Humanitário (DIH) oferece a padronização necessária a ser aplicada em uma guerra, objetivando restringir os efeitos da guerra ao proteger os que dela não fazem parte e limitar os meios e métodos aplicados por ela. Não se trata de legitimar a guerra, mas diante da autonomia dos Estados, o DIH busca que quando necessário o conflito sofra limitações com fulcro na proteção internacional dos direitos humanos.

Esta ideia de que a proteção dos direitos humanos na guerra poderia legitimá-la já foi assunto de debates inter-governamentais. Conquanto, em 1977, no preâmbulo do Protocolo Adicional I à Convenção de Genebra³ ficou definido que “nenhuma disposição (...) pode ser interpretada no sentido de legitimar ou autorizar qualquer ato de agressão ou qualquer outro uso da força incompatível com a Carta das Nações Unidas” (CONVENÇÃO DE GENEBRA, 1977). Destarte, o próprio Direito Internacional tratou de desmistificar o pensamento de que o tratamento da guerra nas normas internacionais a tornavam legítima.

Principalmente depois das experiências aterrorizantes da 2ª Guerra Mundial, houve na esfera internacional, a reivindicação de que os conflitos se tornassem menos desumanos e violentos, confeccionando-se instrumentos como tratados que aproximaram a guerra à uma humanidade por intermédio dos conceitos de *jus ad bellum* (o direito da guerra, ou seja, o direito ao uso da força), e o *jus in bello* (o direito na guerra, que visa regulamentar a maneira como a guerra é conduzida), percebidos tanto no próprio Estatuto de Roma como nos protocolos adicionais à Convenção de Genebra, consolidando o DIH como um mecanismo previsto na agenda internacional (CICV, 2010).

Por este ser um fenômeno frequentemente estudado, nota-se que o Direito Internacional Humanitário (DIH) já previu antecipadamente as formas evolutivas no uso de armas e o aprimoramento ou desenvolvimento de meios e métodos novos para instrumentalizar a guerra, presumindo-se que o DIH é aplicável também ao contexto de conflito cibernético (CICV, 2019). O art. 36 do Protocolo adicional I de 1977 à Convenção de Genebra disciplina o estudo, preparação, aquisição ou adoção de uma nova arma, isto é, de novos meios ou de um novo método de guerra, coisa que não o faz de forma específica, haja vista ao estabelecer-se que a alta parte contratante tem a obrigação de determinar se o emprego da nova arma seria proibido por alguma norma ou tratado de Direito Internacional, deixa-se uma lacuna na norma, pois nem o DIH nem outro instrumento internacional disciplinou as proibições ou limitações no uso dos meios cibernéticos durante a guerra (SILVA E SILVA, 2019).

Dessa maneira, os princípios e normas humanitárias que mitigam a violência da guerra podem ser aplicáveis a um conflito cibernético atribuído a um Estado, mas somente por razão de

³ Ratificado pelo Brasil em 05 de maio de 1992.

algo que supere um eventual incidente, bem como possua o propósito de causar danos, destruição, ferimentos e até mesmo a morte, ainda que as forças armadas não se manifestem em seu sentido clássico, isto é, presencialmente (SCHIMITT, 2012).

Outrossim, para o Comitê Internacional da Cruz Vermelha (CICV, 2019) é indubitável a noção de que o DIH limita também as operações cibernéticas durante conflito armado, fala-se, inclusive, que esse fato se atrela de forma fundamental na Opinião Consultiva do Corte Internacional de Justiça (CIJ) acerca da legalidade da ameaça ou uso de armas nucleares, onde o tribunal lembrou que os princípios e regras do DIH são conferidos às diversas formas de guerra e a todos as espécies de armas, as quais se incluem as “armas do futuro”, como a Internet (CIJ, 1996).

De fato, as preocupações ocasionadas pelo fenômeno da guerra cibernética dizem respeito à organização humanitária. Muitas operações de crimes e espionagem no ciberespaço ocorrem diariamente, não raro sendo patrocinadas pelos Estados. Contudo, a estas não se aplica o DIH, pois não se trata de ações cibernéticas executadas no contexto de um conflito armado. Mas, partir do momento que neste contexto há uma ameaça iminente de que os ataques cibernéticos possam suprimir o funcionamento da estrutura e serviços para a população civil, esta passa a ser um ponto importante dentro do DIH:

Embora alguns Estados tenham reconhecido publicamente que recorreram a meios cibernéticos em apoio às suas operações militares, estima-se que mais de 100 Estados tenham desenvolvido ou estejam desenvolvendo capacidades cibernéticas militares. Felizmente, operações cibernéticas durante conflitos armados não ocorrem em um vácuo jurídico: são regidas pelo Direito Internacional Humanitário (DIH) (CICV, 2021 n.p.).

Nesse sentido, conclui-se que proteções que objetivam resguardar a comunidade civil frente às hostilidades do conflito armado, são também notadas no ciberespaço. Por exemplo, nos ataques cibernéticos, o princípio fundamental da distinção (previsto no art. 48 do Protocolo adicional I de 1977 à Convenção de Genebra) é imprescindível para evitar atentados indiscriminados, visto que os beligerantes devem distinguir em todos os momentos a população civil e combatentes, bem como diferenciar os objetos civis e objetivos militares, e encaminhar suas operações apenas contra os objetivos militares.

Além disso, é sabido que no que toca à responsabilização do ator comandante da guerra no ciberespaço nota-se que o ambiente digital fornece outro desafio, pois nesse espaço os beligerantes podem falsificar a identificação ou utilizar-se de meios que camuflam ou escondem totalmente a identificação dos ataques, o que dificulta a atribuição de guerra por outros atores internacionais, e isso acaba por refletir também na aplicação do *jus in bello*, pois o DIH somente se aplica às operações que se relacionem com o conflito (CICV, 2019).

Essa noção de guerra em um espaço que há pouco tempo não era tão utilizado representa, ao olhos do Direito Internacional e do Direito Humanitário, um complexo que ainda requer em determinadas questões uma especialização jurídica internacional por meio de um tratado, que pode por intermédio que possa estabelecer medidas que resolvam omissões acerca da aplicação do DIH à guerra cibernética e à configuração do crime de guerra nos termos do art. 8º do Estatuto de Roma, isso porque esse é um campo em crescente constante e que quando não cooperado entre atores internacionais ocasiona sérios riscos à humanidade.

3 O *CYBER PEACEKEEPING* COMO PRINCÍPIO PARA AS NAÇÕES UNIDAS NO CIBERESPAÇO

Para compreender a guerra cibernética é preciso levar em consideração os seus elementos, visto que ela faz parte de um contexto ampliado entre modernização e geopolítica dos conflitos armados. O que se sabe é que a guerra no ciberespaço, assim como os crimes cibernéticos fazem parte da paisagem planetária hodierna. Aqui não cabe explicitar as nações, organizações ou indivíduos que rotineiramente violam as leis domésticas e tratados internacionais através do domínio espacial da internet, mas cumpre salientar que são muitos.

As nações têm, de forma indiferente, atacado outras, não objetivando apenas roubar dados e informações sigilosas, desacreditar pessoas ou interferir em resultados eleitorais, mas também para derrubar os sites de órgãos e ministérios governamentais. O *cyber peacekeeping* é uma estratégia para lidar com as várias formas de conflito cibernético e sobretudo com a guerra, visto que assim como o *peacekeeping* se tornou uma ferramenta imprescindível para o tratamento dos conflitos físicos, a aplicação deste ao ciberespaço pode ser útil na gerência dos conflitos cibernéticos (DORN, 2017).

A manutenção da paz promovida pela ONU representa, conforme Robinson et al (2018), uma atividade que se sobrepõe a um conjunto mais amplo de operações de paz. Estas outras atividades podem ser vistas em operações de prevenção de conflitos, em que há uma intervenção precoce para evitar o uso da força, em operações de *peacemaking*, onde observam-se medidas diplomáticas com o fito de trazer um cessar-fogo, e por fim em operações de construção da paz, onde busca-se lançar bases para a longo prazo alcançar-se a paz sem recaídas.

Deste debate acerca do *peacekeeping* em sentido estrito, pode-se extrair alguns princípios aplicados que também repercutem quando toca-se na manutenção da paz cibernética, são eles o consentimento das partes, que sucintamente representa que as operações de paz são implementadas apenas com a manifestação favorável das partes conflitantes, tornando a intervenção legítima; a imparcialidade, onde enfatiza-se que as operações ocorrem de forma isenta do conflito, sem prestação de favores a nenhuma das partes; e o não uso da força, que veda a utilização da força na operação, ressaltando esta possibilidade em caso de legítima defesa.

Tendo o exposto em vista, pode-se agora compreender que da mesma forma que a *peacekeeping* se tornou um meio imprescindível para lidar com os conflitos no espaço físico, é ela também indispensável para a gerência dos conflitos ocorridos no ciberespaço (DORN, 2017). Lembrando que o uso do ciberespaço para fins de guerra é um fenômeno recente e que nunca se viu de fato uma guerra ocorrida inteiramente neste domínio pode surgir dúvidas sobre até que pontos o *peacekeeping* é precisa nesta conjuntura (ROBINSON et al, 2018). Contudo, de encontro à essa visão entende-se que a própria Carta da ONU (1945) pode responder esta questão:

Artº. 1- Os objetivos das Nações Unidas são: 1. Manter a paz e a segurança internacionais e para esse fim: tomar medidas colectivas eficazes para prevenir e afastar ameaças à paz e reprimir os actos de agressão, ou outra qualquer ruptura da paz e chegar, por meios pacíficos, e em conformidade com os princípios da justiça e do direito internacional, a um ajustamento ou solução das controvérsias ou situações internacionais que possam levar a uma perturbação da paz.

Ao definir a manutenção da paz e segurança internacional como objetivo já no seu primeiro artigo, a ONU se compromete a não se abster de situações que impliquem na ameaça, violação ou lesão a ambas. Ou seja, sendo o ciberespaço um ambiente potencial para conflitos que transgridem as normas internacionais, deve ser aplicado a mesma resposta que se garante à violação da paz e segurança internacional no espaço físico.

Sob essa ótica, é preciso pensar no *cyber peacekeeping* como uma ação realizada no ciberespaço com o objetivo principal de preservar a paz através de métodos implementados pacificadores, que são indivíduos atuando em prol da manutenção da paz cibernética. Para Dorn (2017), o mundo precisa de investigadores e protetores diante de ataques no ciberespaço e da mesma forma que no ambiente físico, os pacificadores podem ser implantados pelas Nações Unidas no mundo digital para realizar funções análogas.

O futuro é incerto e cada vez mais tecnológico quanto aos novos métodos, meio e armas de guerras desenvolvidos para o uso da força e expansão no ciberespaço, pois “esse lugar se desenvolve a cada momento de forma descontrolada, agravando a vulnerabilidade estrutural e informacional para aqueles se utilizam dele” (OLIVEIRA et al, 2018, p.12). Logo, o que move a comunidade internacional a colocar a guerra cibernética como um ponto importante na agenda da ONU é justamente o fato de que sua ameaça é iminente e silenciosa, devendo-se prevê-la mesmo antes de se concretizar um evento totalmente cibernético, pois diante do caráter atemporal do conflito inter-pessoal e dos já mencionados avanços científicos, ela é inevitável.

Destarte, sobre as funções de um pacificador no contexto do *cyber peacekeeping* ressalta que eles serviriam de monitores das vagas “fronteiras digitais” e poderiam evitar ou alertar acerca de qualquer ataque, atuariam também na investigação de ataques cibernéticos, realizariam acordos no ciberespaço e a supervisão das “camadas seguras” para garantir que os usuários civis não conflitantes sejam excluídos dos atacantes (DORN, 2017). Diante de todas estas atribuições, é interessante perceber que haveria uma equiparação de fato do domínio físico e do domínio virtual para a realização de conflitos, observando sempre as normas e tratados internacionais que regulam o direito à guerra, na guerra e pós-guerra.

Em síntese, uma capacidade digital de manutenção da paz seria capaz de contribuir com a proteção do mundo, pois há uma grandeza diretamente proporcional entre crescimento digital e vulnerabilidade. Porém, para a concretização do *cyber peacekeeping* como fundamental para as nações no ciberespaço é preciso antes superar outros desafios no tocante à regulamentação específica deste tema no Direito Internacional, este que ainda caminha lentamente diante da novidade do tema, que daqui há alguns anos, talvez décadas, não soará tão desconhecido e inofensivo como atualmente.

CONSIDERAÇÕES FINAIS

Com este trabalho pode-se entender que a funcionalidade da internet enquanto meio ou método de guerra decorre da ausência uma norma especial para regulamentar a guerra no ciberespaço. Por causa disso, cria-se uma notória insegurança jurídica, haja vista que os conflitos digitais ocorrem sem deixar rastros, com por exemplo invasões, espionagem e furto de dados. E quando se trata destes atos associados a um conflito armado, a situação torna-se mais ameaçadora ainda.

Nesse sentido, o Direito Internacional, ao mesmo tempo que não proíbe o uso da internet na como meio de guerra, também não o regulamenta, criando um paradoxo que só faz com que a comunidade internacional fique cada vez mais sob a onda de um ataque cibernético entre dois ou mais países. Situação essa que muitos doutrinadores, e personalidades internacionais temem fervorosamente.

Assim, diante dessa abstenção, neste trabalho restou demonstrado que o crime de guerra cibernética não é expressamente previsto pelo Estatuto de Roma como uma tipificação especial.

Entretanto, a utilização da internet para fins de ataque entre estados gera sim os comandos tipificados no crime de guerra do art. 8º do Estatuto. Portanto, estados que se valem de internet para promover conflitos no ciberespaço contra outros podem sim ser responsabilizados internacionalmente perante o Tribunal Penal Internacional.

Outrossim, o Direito Internacional Humanitário é plenamente aplicável ao ciberespaço, podendo haver o exercício de todos os seus princípios com o objetivo de garantir direitos em meio a conflitos cibernéticos. A analogia aqui trazida é totalmente necessária para garantir a manutenção da paz e segurança internacional, porque ao tempo que há pacificadores nos conflitos físicos e já houve experiências bem-sucedidas, a existência de pacificadores no ciberespaço serve tanto para prevenir quanto para atuar em possíveis situações litigantes.

REFERÊNCIAS

ARQUILLA, John; RONFELDT, David. Cyberwar is coming! Comparative Strategy, [S.L.], v. 12, n. 2, p. 141-165, abr. 1993. Informa UK Limited. <http://dx.doi.org/10.1080/01495939308402915>. Disponível em: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf. Acesso em: 25 maio 2021.

CICV. Comitê Internacional da Cruz Vermelha. **Direito Internacional Humanitário e Operações Cibernéticas durante conflitos armados: Documento de posição do CICV**. Disponível em: <https://www.icrc.org/pt/document/direito-internacional-humanitario-e-operacoes-ciberneticas-durante-conflitos-armados>. Acesso em: 06 nov. 2020.

CICV. Comitê Internacional da Cruz Vermelha. **Guerra cibernética e Direito Internacional Humanitário**. Disponível em: <https://www.icrc.org/pt/document/guerra-cibernetica-e-direito-internacional-humanitario>. Acesso em: 20 mai. 2021.

CICV. Comitê Internacional da Cruz Vermelha. **O DIH e outros regimes legais – jus ad bellum e jus in bello**. 2010. Disponível em: <https://www.icrc.org/pt/doc/war-and-law/ihl-other-legal-regimes/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm>. Acesso em: 06 nov. 2020.

CICV. Comitê Internacional da Cruz Vermelha. **Para servir e Proteger: Direitos Humanos e Direito Internacional Humanitário para forças policiais de segurança**. 4ª ed. Genebra: CICV, 2005. 236 p.

CICV. Comitê Internacional da Cruz Vermelha. **Protocolo I de 1977 adicional às Convenções de Genebra**. Disponível em: <https://www.icrc.org/pt/guerra-e-o-direito/tratados-e-direito-consuetudinario/convencoes-de-genebra..>Acesso em: 21 mai. 2021.

CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012.

DORN, Walter. Cyberpeacekeeping: a new role for the united nations?. *Georgetown Journal Of International Affairs*, [S.L.], v. 18, n. 3, p. 138-146, 2017. Project Muse. <http://dx.doi.org/10.1353/gia.2017.0046>. Disponível em: https://www.walterdorn.net/pdf/Cyberpeacekeeping_GeorgetownJIntAff_Dorn_Fall2017.pdf. Acesso em: 25 maio 2021.

FERNANDES, José Pedro Teixeira. **Geopolítica em Tempo de paz e Guerra**. 1 ed. São Paulo: Almedina, 2019.

JASTRAM, Kate; QUINTIN, Anne. The internet in bello: cyber war law, ethics & policy. In: CYBERWARFARE SEMINAR, 2011, Berkeley. **Proceedings...** Berkeley, 2011. Disponível em: https://www.law.berkeley.edu/files/cyberwarfare_seminar--_summary_032612.pdf. Acesso em: 6 nov. 2020.

KNAKE, Robert K.; CLARKE, Richard A. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015. 280 p.

LOBATO, Luisa; KENKEL, Kai Michael. A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra. *Contexto Internacional*, [S.L.], v. 37, n. 2, p. 629-660, ago. 2015. FapUNIFESP (SciELO). <http://dx.doi.org/10.1590/s0102-85292015000200010>. Disponível em: <https://www.scielo.br/j/cint/a/RQqF3Ztm49nqj4BqK-PJGF5J/?lang=pt>. Acesso em: 20 ago. 2020.

MAZZUOLI, Valerio de Oliveira. **Curso de Direito Internacional Público**. 12. ed. Rio de Janeiro: Forense, 2019. 1797 p.

MELZER, N. **Cyberwarfare and international law**. Genebra, Suíça: United Nations Institute for Disarmament Research, 2011. Disponível em: <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. Acesso em: 6 nov. 2020.

NUNES, Luiz Artur Rodrigues. **GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL: Aplicabilidade do Jus ad Bellum e do Jus in Bello**. 2015. 60 f. TCC (Graduação) - Curso de Altos Estudos de Política e Estratégia, Escola Superior de Guerra, Rio de Janeiro, 2015. Disponível em: <https://egov.ufsc.br/portal/conteudo/guerra-cibern%C3%A9tica-e-o-direito-internacional-aplicabilidade-do-jus-ad-bellum-e-do-jus-bello>. Acesso em: 05 nov. 2020.

NUNES, Luiz Artur Rodrigues. **GUERRA CIBERNÉTICA: Está a MB preparada para enfrenta-la?**. 2020. 99 f. TCC (Graduação) - Curso de Política e Estratégia Marítimas., Escola de Guerra Naval, Rio de Janeiro, 2010. Disponível em: <http://www.redebim.dphdm.mar.mil.br/vinculos/000006/000006d7.pdf>. Acesso em: 06 nov. 2020.

OLIVEIRA et al. Aspectos Jurídicos da Ciberguerra como Proeminente Modalidade de Conflito Internacional do Século XXI. In: XVI Congresso Acadêmico sobre Defesa Nacional: 2018, Agulhas Negras. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/ensino-e-pesquisa/congressos-e-simposios/congresso-academico-sobre-defesa-nacional/artigos-e-palestras-do-14-congresso-academico-sobre-defesa-nacional..>Acesso em: 20 mai. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**. 1945. Disponível em: <http://www.onu.org.br/conheca-a-onu/documentos>. Acesso em: 26 mai. 2021.

ROBINSON, Michael et al. An introduction to cyber peacekeeping. *Journal Of Network And Computer Applications*, [S.L.], v. 114, p. 70-87, jul. 2018. Elsevier BV. <http://dx.doi.org/10.1016/j.jnca.2018.04.010>. Disponível em: https://www.scopus.com/record/display.uri?eid=2-s2.0-85046171364&origin=inward&txGid=9cac0c4ea4c14205af93876d7851c014&featureToggles=FEATURE_NEW_MAIN_SECTION:1,FEATURE_NEW_SOURCE_INFO:1,FEATURE_NEW_REAXYS_SECTION:1,FEATURE_NEW_SCIIVAL_TOPICS:1,FEATURE_VIEWS_COUNT:1. Acesso em: 20 out. 2020.

ROBINSON, Michael et al. Developing cyber peacekeeping: observation, monitoring and reporting. *Government Information Quarterly*, [S.L.], v. 36, n. 2, p. 276-293, abr. 2019. Elsevier BV. <http://dx.doi.org/10.1016/j.giq.2018.12.001>. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X18302831>. Acesso em: 20 out. 2020.

SALDAN, Eliane. Os Desafios Jurídicos da Guerra no Ciberespaço. 2012. 118 f. Dissertação (Mestrado) - Curso de Direito, Instituto Brasiliense de Direito Público – Idp., Brasília, 2012. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/1223/1/Disserta%C3%A7%C3%A3o_Eliane%20Saldan.pdf. Acesso em: 24 maio 2021.

SCHMITT, Michael N.. Wired warfare: computer network attack and jus in bello. *Revue Internationale de La Croix-Rouge/International Review Of The Red Cross*, [S.L.], v. 84, n. 846, p. 365, jun. 2002. Cambridge University Press (CUP). <http://dx.doi.org/10.1017/s1560775500097741>.

SILVA, Rodrigo Cardoso; SILVA, Eliza Odila Conceição. O dilema do Jus ad Bellum e Jus in Bellum na Guerra Cibernética: como aplicar o direito da guerra na era digital? In: JUBILUT, Liliana Lyra *et al* (org.). **Direitos Humanos e Vulnerabilidade e o Direito Humanitário**. Boa Vista: Editora da UFRR, 2019.

SINGER, André et al. **Estado e democracia**: uma introdução ao estudo da política. Rio de Janeiro: Zahar, 2021.

VON CLAUSEWITZ, Carl. **On War**. Princeton: Princeton University Press, 1984.