ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM GABRIEL MAYRINK PEDRO DA SILVA

Possibilidades e limitações das ações de Guerra Cibernética: O Amparo legal e as implicações para o Direito Internacional dos Conflitos armados

Rio de Janeiro
2023

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM GABRIEL MAYRINK PEDRO DA SILVA

Possibilidades e limitações das ações de Guerra Cibernética: O Amparo legal e as implicações para o Direito Internacional dos Conflitos armados

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Organizacional

Rio de Janeiro
2023

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

SI586

Silva, Gabriel Mayrink Pedro da Silva.
Possibilidades e limitações das ações de Guerra Cibernética: : o amparo legal e as implicações para o direito intenracional dos conflitos armados / Gabriel Mayrink Pedro da Silva Silva - 2023
51 f. il. color.

Trabalho de Conclusão de Curso - Escola de Aperfeiçoamento de Oficiais - EsAO, Rio de Janeiro, 2023.

1. Cibernética 2. Direito I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

CAP COM GABRIEL MAYRINK PEDRO DA SILVA

Possibilidades e limitações das ações de Guerra Cibernética: O Amparo legal e as implicações para o Direito Internacional dos Conflitos armados

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Organizacional

Aprovado em_____de_____de 2023

COMISSÃO DE AVALIAÇÃO

_____

ANDERSON GUSTAVO LIMA DOS SANTOS – MAJ
Presidente

_____

HUGO FARIA BRITO FRANCISQUINI – Cap
Membro

_____

WAGNER DE FARIAS FIGUEIREDO – Maj
Membro

AGRADECIMENTOS

Primeiramente à Deus, pois sem ele nada seria possível.

À minha esposa Manoela, pelo amor e apoio para superar mais uma etapa da trilha do conhecimento.

Aos meus pais Wanda e Huedson que me criaram e educaram.

RESUMO

Este trabalho de conclusão de curso teve por objeto explicar conceitualmente as atividades cibernéticas realizadas pelos operadores de guerra cibernética. Explicar a doutrina do direito relacionada com as ações cibernéticas dentro da seguinte área: direito internacional dos conflitos armados e dos direitos humanos. Verificar a doutrina e a legislação nacional que versam sobre as ações cibernéticas. Verificar se uma ação cibernética pode ser considerada uma agressão militar sob a óptica do direito internacional dos conflitos armados. Portanto, este trabalho visou realizar um estudo bibliográfico acerca da legislação nacional e internacional sobre as ações cibernéticas, bem como esclarecer as possibilidades e limitações dessas ações.

Palavras-chave: Cibernética. possibilidades. limitações

ABSTRACT

This course completion work aimed to conceptually explain the cybernetic activities carried out by cyberwarfare operators. Explain the doctrine of law related to cyber actions within the following area: international law of armed conflict and human rights. Check the doctrine and national legislation that deal with cyber actions. Check whether a cybernetic action can be considered a military aggression from the perspective of the international law of armed conflicts. Therefore, this work aimed to carry out a bibliographical study about the national and international legislation on cybernetic actions, as well as to clarify the possibilities and limitations of these actions.

Keywords: Cybernetics. possibilities. limitations

SUMÁRIO

1. INTRODUÇÃO

Com a evolução tecnológica, a internet proporcionou grandes avanços nos meios de comunicação e transmissão de dados. Essa evolução não ficou restrita apenas aos meios de comunicação. A humanidade acompanha essa evolução. Desta maneira, a forma como os países se relacionam e a própria arte da guerra acompanham esse movimento.

Corroborando com esse entendimento, a guerra evolui sob uma perspectiva teórica baseada em 3 fatores (tecnológico, econômico e político- sociais), e são retratados em 5 gerações, conforme tabela 1:

Tabela 1 - Geração das Guerras

Geração das Guerras	Principais Características
1ª Geração	emprego da massa e do combate linear
2ª Geração	emprego do poder de fogo e do combate linear
3ª Geração	emprego do movimento, da manobra e do combate não linear
4ª Geração	emprego massivo de tecnologia, assimétrica e perda do monopólio do uso da força por parte do Estado
5ª Geração’	emprego massivo da cyber war, assimétrica, informacional e híbrida

Fonte: SANTOS, Daniel Mendes Aguiar et al. “A arte da guerra no século XXI: avançando à Multi-Domain Battle”. Coleção Meira Mattos, v. 13, n. 46, janeiro/abril 2019, pp. 83-105 apud Lind et al. (1989)

A 1ª geração das guerras é baseada no emprego da massa e do combate linear, podendo referenciar o período de 1648 até 1865. A 2ª geração tem como característica o emprego do poder de fogo e do combate linear, podendo destacar os combates ocorridos durante a 1ª Guerra Mundial. A 3º geração tem por base o emprego do movimento, da manobra e do combate não linear, que foi empregada destacadamente pela Exército Alemão durante a 2ª Guerra Mundial. Na 4ª e 5ª gerações é possível perceber que a tecnologia definitivamente alcançou o campo de batalha, e o século XXI passa a ser marcado pelas investidas cibernéticas como forma de se alcançar objetivos estratégico-políticos-militares, sem emprego decisivo de força bélica (SANTOS 2019 apud Lind, 1989).

Entretanto, com a ampliação do espaço cibernético, ataques e explorações cibernéticas poderiam ser combinadas com ações de movimento, manobras e

fogos no campo de batalha a fim de se alcançar a maximização do poder de combate e redução de danos colaterais, baixas e preservação de materiais militares.

A combinação de ações cibernéticas durante o curso de operações militares tem ocorrido em alguns conflitos no mundo. Uma dessas ações ocorreu quando Israel realizou um ataque aéreo bombardeando uma complexo industrial em construção no leste do território da Síria, no ano de 2007. Informações de Israel apontavam que o local estava sendo utilizado para construção de uma fábrica de artefatos nucleares com a ajuda de Norte-Coreanos. Aviões de ataque F-15 e F-16 Israelenses, que são identificáveis por radares, entraram no espaço aéreo Sírio sem que os sistemas de defesa aérea indicassem qualquer atividade. Misseis de defesa da Síria não foram disparados, nem tão pouco jatos de defesa decolaram neste dia pois não existiam alvos detectados nos radares da Síria. Os Israelenses haviam realizado um ataque cibernético combinado com a missão aérea de bombardeio, sem baixas de pessoal e material (CLARKW; KNAKE, 2010).

Outro caso de ataque cibernético ocorreu no ano de 2008, durante um conflito entre Rússia e Geórgia. Ao mesmo tempo que o exército da Rússia avançava contra tropas da Geórgia localizadas na região de Ossétia do Sul, sites do governo Georgeano, e site de jornalismo como CNN e BBC ficaram inacessíveis. Esse ataque cibernético é conhecido como DDoS (ataque de negação de serviço). Especialistas na época apontaram que a localização do ponto de partida dos ataques se encontrava conectado ao aparato de inteligência Russa. Entretanto, a Rússia informou que tais ações tinham origem popular e que o Kremlin não tinha controle sobre isso (CLARKW; KNAKE, 2010).

1.1 PROBLEMA

Com a virada do século XX para o século XI, a internet e o mundo em redes tornou-se acessível a todos. Cidadãos, empresas e órgãos governamentais passaram a ter grande dependência de sistemas informatizados interligados pela rede mundial de computadores. Em um mundo cada vez mais digital e conectado, uma vulnerabilidade no espaço cibernético quando explorado por pessoas mau intencionadas pode acarretar grandes danos à infraestrutura de TI, destruição de bancos de dados, vazamento de informações confidenciais,

modificação do funcionamento de máquinas e equipamentos, grandes prejuízos financeiros e até mesmo a perda de vidas humanas. Para que isso ocorra, basta que uma ação cibernética seja realizada, de qualquer parte do mundo.

Dentro do Brasil, os legisladores tem feito modificações no arcabouço jurídico nacional a fim de comportar e acompanhar as evoluções factuais trazidas pelo avanço tecnológico cibernético. Exemplo disso são as promulgações do Marco Civil da Internet, da Lei de Crimes Cibernéticos (“Lei Carolina Dieckmann”) e da Lei Geral de Proteção de Dados.

No campo internacional, a evolução proporcionada pelo espaço cibernético também provoca modificações na forma como as nações se relacionam. O direito internacional busca também legislar sobre a forma com que os conflitos armados ocorrem entre os países, estipulando regras gerais sobre o que pode ou não ocorrer entre nações frente a um conflito armado. O computador tornou-se uma arma. Assim, é fundamental que se tenha a compreensão sobre as possibilidade de uma ação cibernética ser considerada uma agressão que possa justificar a legítima defesa entre nações e os princípios norteadores do direito internacional dos conflitos armados

Dentro deste cenário, e afim de cooperar com o desenvolvimento da pesquisa e da doutrina militar e jurídica, visualizou-se o seguinte problema: **Quais as limitações que a legislação internacional (direito internacional dos conflitos armados) impõem para as capacidades de guerra cibernética do exército brasileiro?**

1.2 OBJETIVOS

O trabalho tem por objetivo avaliar as possibilidades e limitações das ações de cibernética realizadas pelos operadores de cibernética do Exército Brasileiro com base na legislação nacional e sob a óptica do direito internacional dos conflitos armados.

Para alcançar esse objetivo, será explicado conceitualmente as principais atividades de guerra cibernética que poderiam ser realizadas pelos operadores de guerra cibernética do Exército Brasileiro, bem como as limitações jurídicas dessas ações.

Explicar conceitualmente as atividades cibernéticas realizadas pelos operadores de guerra cibernética. Explicar a doutrina do direito relacionada com

as ações cibernéticas dentro das seguintes áreas: penal, constitucional, direito internacional dos conflitos armados e dos direitos humanos. Verificar a doutrina e a legislação internacional que versam sobre as ações cibernéticas. Verificar se uma ação cibernética pode ser considerada uma agressão militar sob a óptica do direito internacional dos conflitos armados. Avaliar as possibilidades e limitações das ações de guerra cibernética.

Para desenvolver o objetivo geral do trabalho, realizaremos as seguintes etapas:

- Explicar conceitualmente as atividades cibernéticas mais comuns;
- Apresentar o amparo legal para as atividades de guerra cibernética realizadas pelo Exército Brasileiro;
- Explicar os conceitos principiológicos do Direito internacional;
- Explicar os conceitos principiológicos do Direito internacional dos Conflitos Armados;
- explicar os conceitos principiológicos dos Direitos Humanos;
- Apresentar a política nacional de defesa e a estratégia nacional de defesa;

1.3 QUESTÕES DE ESTUDO

Com a finalidade de se alcançar a solução do problema apresentado e tendo em vista os objetivos elencados, foram levantadas as seguintes questões de estudo:

- Quais são as limitações jurídicas sobre a atividade de guerra cibernética?
- uma ação pode ser considerada uma agressão sob a óptica do direito internacional dos conflitos armados?
- uma ação cibernética pode ser considerada um crime de guerra sob a jurisdição do tribunal internacional penal?

As respostas às questões de estudo formuladas acima são necessárias a fim de orientar para a solução do problema apresentado.

1.4 JUSTIFICATIVAS

O tema justifica-se pela necessidade de compreender quais ações cibernéticas podem ou não ser realizadas pelos operadores de guerra

cibernética do Exército Brasileiro, levando em consideração a legislação internacional.

Em um momento onde o espaço cibernético tem cada vez mais importância, o Exército Brasileiro percebendo a importância de tal atividade, entendeu que “atuar no espaço cibernético com liberdade de ação deveria constar como um Objetivo Estratégico do Exército OEE nº 4 do PEEX 2020-2023. O presente trabalho se justifica na medida que a guerra cibernética passou a ser um de seus Objetivos Estratégicos do Exército. Os militares que realizam a atividade cibernética devem ter total conhecimento sobre as limitações legais impostas à essa atividade. O operador de guerra cibernética deve ter conhecimento também sobre as implicações dessas atividades para o direito internacional e para o direito internacional dos conflitos armados, a fim de que as relações institucionais e diplomáticas com outros países seja mantida conforme os princípios constitucionais das relações internacionais.

2. REVISÃO DE LITERATURA

A revisão de literatura foi realizada com o intuito de apresentar um embasamento teórico robusto por fontes confiáveis.

Para que seja possível analisar as limitações legais impostas à atividade de guerra cibernética, é fundamental explorar e descrever o sistema jurídico brasileiro, e após isto, debruçar-se sobre o direito internacional dos conflitos armados. Dessa forma, será possível compreender como todos esses aspectos jurídicos se relacionam com a atividade militar de cibernética.

2.1 NORMAS CONSTITUCIONAIS

A Constituição da República Federativa do Brasil, no seu artigo 142, determina que as Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.

A Carta Magna Brasileira é explícita ao determinar que as relações internacionais do Brasil devem ser pautadas sob os princípios da prevalência

dos direito humanos, da não-intervenção, da defesa da paz, da solução pacífica dos conflitos, dentre outros.

2.2 POLÍTICA NACIONAL DE DEFESA

A Política Nacional de Defesa, instituída por meio de decreto presidencial no ano de 2005, tinha por finalidade estabelecer as diretrizes para o desenvolvimento das capacidades do poder nacional de defesa, para fazer frente contra ameaças externas. Como uma de suas diretrizes, ficou estabelecido que seriam aperfeiçoados equipamentos e dispositivos, bem como reduzidas as vulnerabilidades dos sistemas de defesa contra ataques cibernéticos.

Fruto da política nacional de defesa, é instituída no ano de 2008 a Estratégia Nacional de Defesa. Neste decreto, ficou definido o setor cibernético como sendo estratégico e essencial para o desenvolvimento da defesa nacional.

Dessa forma, é possível perceber que a evolução tecnológica desenvolveu no campo político a preocupação com a questão do setor cibernético nacional, estimulando o desenvolvimento das bases de defesa nesta área.

2.3 INCIDENTES CIBERNÉTICOS

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR) é uma organização do governo federal que tem por objetivo realizar a análise e resposta de notificações de incidentes de segurança em computadores.

O CTIR realiza também a divulgação de estatísticas relacionadas ao tema de incidentes cibernéticos no país. O CTIR apresentou informações a respeito dos tipos de incidentes ocorridos no ano de 2023, atualizado até o dia 01/03/2023 com os incidentes confirmados por categoria, conforme figura 1 abaixo:

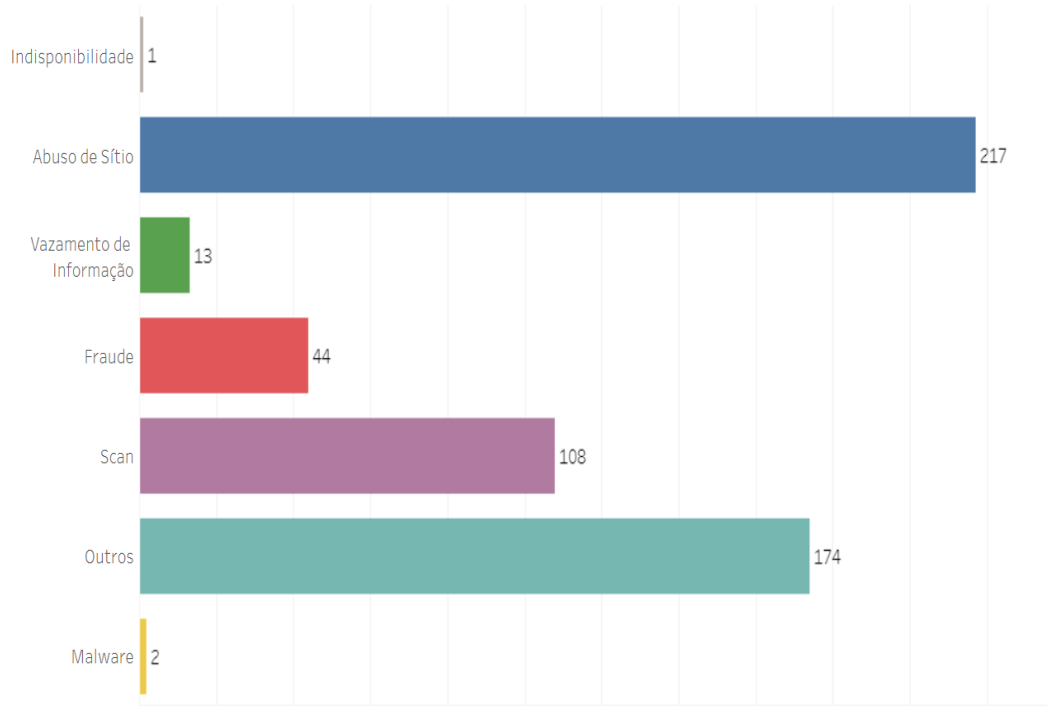

Figura 1- Incidentes confirmados por categoria em 2023

Fonte: CTIR (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/incidentes)

É possível observar que 217 incidentes foram relacionados a abuso de sítio, 108 incidentes de Scan, 44 incidentes relacionados a fraude, 13 de vazamento de informação, 2 malware, 1 de indisponibilidade e 174 classificado como outros.

Com relação ao número de incidentes que ocorrem no exterior que tem a origem no Brasil, o CTIR divulgou que 4.318 incidentes foram reportados ao Brasil. O Brasil fica atrás somente dos Estados Unidos da América quando se trata da quantidade de incidentes no mundo que tem a origem da ação identificada como sendo de outro país.

A figura 2 abaixo ilustra a quantidade de incidentes reportados pelo mundo, no qual o Brasil aparece a frente de países como Rússia, China, Inglaterra e Canadá.

Figura 2

Fonte: CTIR (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/incidentes)

2.4 GUERRA CIBERNÉTICA

Os exemplos citados sobre o conflito entre Israel e Síria, bem como entre Rússia e Geórgia podem ser considerados como os primeiros conflitos de guerra cibernética ocorridos publicamente entre estados-nação. Essas ações no campo cibernético demonstraram para o mundo que a guerra cibernética não reside apenas no campo teórico, mas está ocorrendo claramente ocorrendo no mundo fático. Mostraram também que a guerra cibernética não se limita ao campo de batalha podendo alcançar pessoas e instituições que não estão diretamente envolvidas no conflito bélico, como por exemplo sistemas bancários e sites de notícias (CLARKW; KNAKE, 2010).

A definição do significado de guerra cibernética não é simples, pois envolve diversos conceitos correlatos (conceito de guerra, cibernética e a junção de ambos). O espaço cibernético, do ponto de vista técnico, pode ser compreendido como um campo digital no qual as informações são enviadas, recebidas e armazenadas por meio de redes de computadores. Se trata de um domínio global que consiste em uma interdependência de tecnologia, informação e estruturas (computadores, servidores, roteadores). Para a estratégia militar, o espaço cibernético é entendido como um domínio caracterizado pelo uso do

espectro eletrônico e eletromagnético que tem por finalidade guardar, modificar ou trocar informações por meio do uso de estruturas de tecnologia da informação (redes de computadores) (ANDRESS; WINTERFELD, 2011).

A Organização das Nações Unidas (ONU) define cibernética como sendo um sistema global de computadores, sistemas de comunicações e banco de dados conectados por meio da Internet, mas também pode se referir ao sistema local de computadores que não esteja ligado a internet mas faça parte da infraestrutura de uma empresa, força armada ou governo (ANDRESS; WINTERFELD, 2011).

A guerra poderia ser considerada como uma ação de força de um estado para contra outro a fim de compelir este a realizar aquilo que se deseja. A guerra teria o objetivo de tornar o inimigo incapaz de resistir contra a vontade imposta a ele. Assim, a guerra poderia ser considerada como o uso da força a fim de impor ao inimigo o cumprimento de nossa vontade (VON CLAUSEWITZ, 1832).

Ao explorar o significado da expressão guerra cibernética, seria possível compreender que a guerra cibernética seria a fusão de diversos conceitos correlato, pois se trata de uma ação no campo cibernético que visa obrigar o inimigo a realizar a sua vontade. A guerra cibernética é capaz de alcancar objetivos estratégicos sem que seja necessário empregar o uso da força física (CZOSSECK; GEERS, 2009).

Nos dias atuais, grande parte dos sistemas de comando e controle são conectados por redes de computadores. E mais ainda, para as forças armadas de forma, diversos sistemas logísticos, armamentos de artilharia, sistemas de defesa anti aérea e aeronaves dependem de uma infraestrutura de rede de computadores para ter seu perfeito funcionamento. Aeronaves e mísseis de defesa aérea são guiados remotamente e recebem e atualizam suas rotas constantemente por meio de comunicação de rede com base em posições GPS (Sistema Global de Posicionamento). Dessa forma, o campo de batalha foi digitalizado e as infraestruturas de redes de computadores tornaram-se o alvo principal de ataques cibernéticos (ANDRESS; WINTERFELD, 2011).

2.5 DOUTRINA MILITAR DE GUERRA CIBERNÉTICA

Após o direcionamento político do Governo Federal estipulando diretrizes para as bases do desenvolvimento da estrutura de defesa do país, o Ministério

da Defesa elaborou a Doutrina Militar de Defesa Cibernética, atribuindo a guerra cibernética ao nível operacional e tático das Forças Armadas, conforme figura 3.

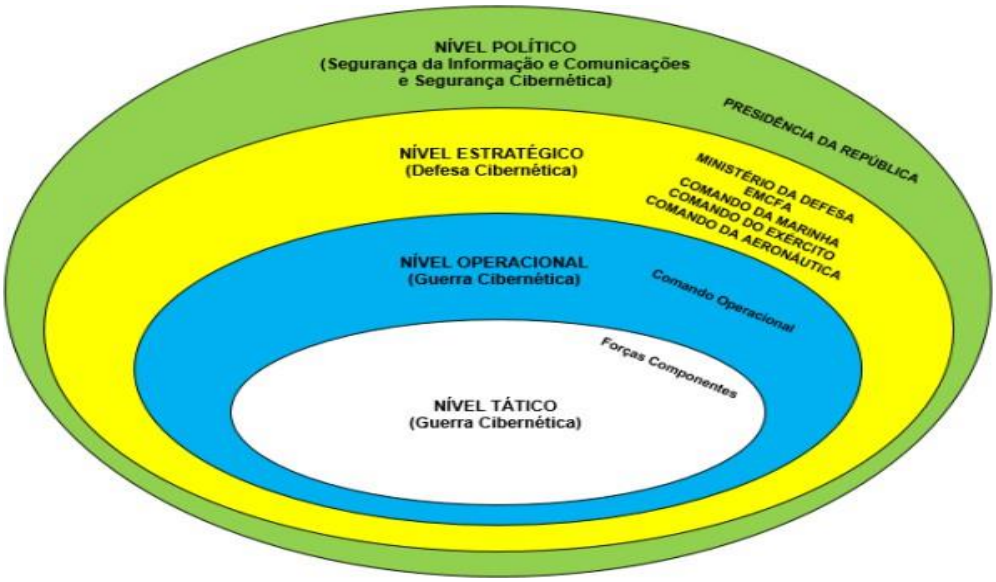

Figura 3 - Níveis de decisão

Fonte: Ministério da Defesa - Doutrina Militar de Defesa Cibernética (2014, p. 17)

Sobre a figura 3 é possível inferir que as ações do nível político abrange as ações de defesa cibernética e guerra cibernética. Dependendo da ação cibernética a ser realizada, é fundamenta a tomada de decisão pelo nível político, tendo em vista que as consequências de uma ação de grande vulto podem tomar proporções nacionais e internacionais.

Assim sendo, o Ministério da Defesa, por meio da Doutrina Militar de Defesa, definiu guerra cibernética da seguinte maneira:

> **Guerra Cibernética** - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2 . Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (BRASIL, 2014, p. 19).

É possível perceber pela Doutrina Militar de Defesa do Ministério da Defesa a especial atenção a respeito das limitações impostas pelo ordenamento jurídico vigente à ações cibernéticas, conforme transcrito a seguir:

> **Limites às Ações Cibernéticas em Operações de Não Guerra**: Por ocasião da execução de Operações de não-guerra, o emprego de ações de ataque cibernético necessita de autorização expressa de autoridade competente, normalmente em nível político. Para as ações de exploração cibernética, deverão ser observados atos normativos do ordenamento jurídico em vigor. Em caso de dúvidas, caberá ao EMCFA consultar o nível político acerca do emprego das ações anteriormente mencionadas (BRASIL, 2014, p. 24).

Assim, a Defesa busca pautar as suas ações com base no princípio constitucional da legalidade, e demonstra o vasto caminho disponível para a pesquisa científica neste ramo.

Tendo em vista a possibilidade de uma ação cibernética alcançar repercussão e consequências regionais, nacionais e internacionais, o Ministério da Defesa determinou que durante as Operações de Guerra somente poderão ser executadas as ações efetivamente necessárias com base na observância de critérios e formas de atuação previamente definidos. Em caso de dúvidas com relação às ações a serem executadas, o EMCFA (Estado-Maior Conjunto das Forças Armadas) deverá consultar o nível político.

2.6 DOUTRINA DE GUERRA CIBERNÉTICA DO EXÉRCITO BRASILEIRO

Na esteira no Ministério da Defesa, o Exército Brasileiro aprovou o manual de campanha de guerra cibernética. Este manual apresentou as linhas gerais do emprego em campanha da guerra cibernética. Pode-se destacar aspectos sobre os fundamentos de guerra cibernética, os princípios de emprego, possibilidades e limitações, bem como a forma que a guerra cibernética irá interagir no domínio cibernético durante as operações combinadas, ofensivas, defensivas, de cooperação e coordenação com agências e de informação.

O manual de campanha de guerra cibernética do Exército Brasileiro aponta a guerra cibernética como sendo o uso ofensivo e defensivo de informação ou sistemas de tecnologia da informação tendo por objetivo impedir o uso do comando e do controle ao adversário, seja destruindo ou corrompendo, no contexto de operações militares no nível operacional.

A doutrina militar do Exército Brasileiro faz uso de princípios de guerra que podem ser utilizados em todos os tipos de operações militares. Entretanto, ocorre que, esses princípios de guerra gerais não se adequam perfeitamente à atividade de guerra cibernética, tendo em vista sua excepcional especificidade.

Por isso, o Exército Brasileiro designou 4 princípios de emprego da guerra cibernética - quais sejam - princípio do efeito, princípio da dissimulação, princípio da rastreabilidade e princípio da adaptabilidade.

O princípio do efeito impõe que as ações cibernéticas devem ser voltadas a produzir vantagens estratégicas, operacionais e táticas. Segundo o princípio do efeito, as ações cibernéticas devem alcançar a vantagem necessária sobre o inimigo, podendo ter um efeito cinético ou não cinético. Para compreender a distinção de efeito cinético ou não cinético, faz-se necessário recorrer ao Manual de Campanha Fogos do Exército Brasileiro que aborda a definição de fogos cinéticos e não cinéticos. O fogo cinético é caracterizado pelo emprego de sistemas de armas que realizam o lançamento de artefato explosivo (granadas, misseis e/ou foguetes), a fim de se alcançar algum objetivo militar, seja para facilitar as operações das tropas amigas, seja para diminuir o poder de combate do inimigo, pela letalidade ou pela destruição de estruturas. Já a ação não cinética é caracterizada pelo emprego de sistemas de ataque de guerra cibernética, eletrônica ou outro meio que não realiza o lançamento físico de artefatos explosivos, mas que, a despeito de não realizar o lançamento de um foguete, pode causar baixas, avarias ou efeitos destrutivos contra estruturas físicas e de comando e controle de interesse do inimigo.

O princípio da dissimulação determina que as ações cibernéticas realizadas pelo Exército Brasileiro devem impedir a rastreabilidade das mesmas, a fim de negar ao inimigo a possibilidade de identificar a autoria e a localização do ponto de partida inicial da ação cibernética realizada.

Em contra partida, o princípio da rastreabilidade determina que o Exército Brasileiro deve envidar esforços para identificar a origem e autoria de ações cibernéticas desencadeadas por forças inimigas contra estruturas de Tecnologia da Informação de tropas amigas.

Por fim, o princípio da adaptabilidade significa que a atuação da guerra cibernética do Exército Brasileiro deve ter a capacidade de se adaptar frente às mudanças súbitas e imprevisíveis da dimensão cibernética das operações.

Para o Exército Brasileiro, a guerra cibernética não possui limitações físicas de sua zona de ação, tendo em vista possuir um alcance global. Ações

de guerra cibernética podem ser desencadeadas de qualquer local do globo terrestre contra qualquer outro ponto do planeta.

2.6.1 SISTEMA DE GUERRA CIBERNÉTICA DO EXÉRCITO BRASILEIRO

O Sistema de Guerra Cibernética do Exército Brasileiro (SGCEx) está inserido no Sistema Militar de Defesa Cibernética. Para as ações no nível tático, caso exista uma situação de conflito bélico militar, será ativada a Estrutura Militar de Defesa (Etta Mi D) e então, a Força Terrestre Componente (FTC) deverá ser apoiada por uma Estrutura de Guerra Cibernética. Essa estrutura de guerra cibernética que dará apoio para a FTC será composta por elementos do 1º Batalhão de Guerra Eletrônica (1º BGE), do Batalhão de Comunicações (B Com), do Batalhão de Comunicações e Guerra Eletrônica (B Com GE), do Batalhão de Inteligência Militar (BIM), da Companhia de Comando e Controle (Cia C2) e das Companhias de Comunicações (Cia Com) conforme a figura 4 abaixo:

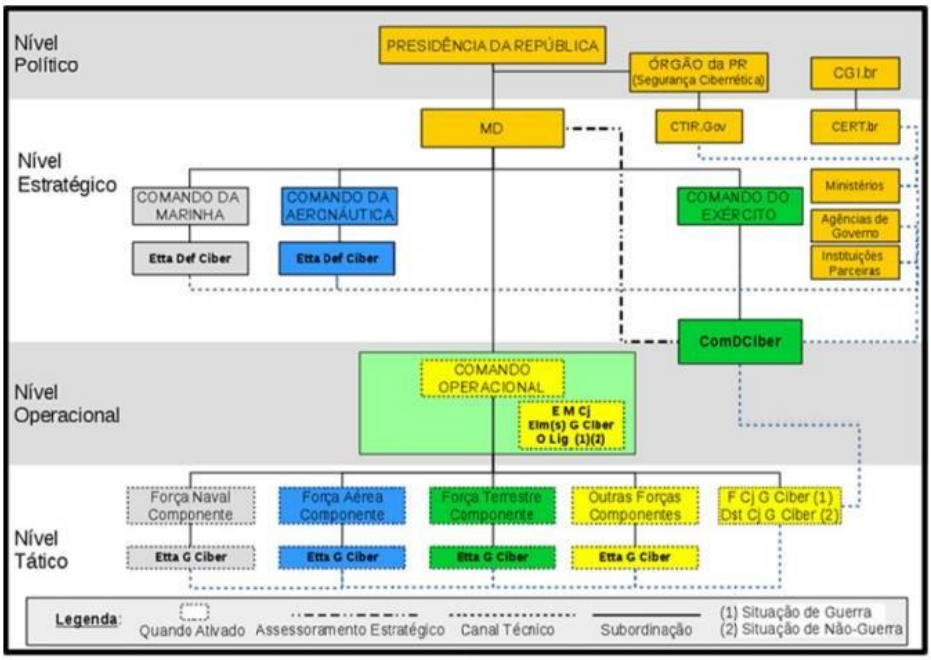

Figura 4 - Sistema Militar de Defesa Cibernética (SMDC)

fonte: Manual de Campanha Guerra Cibernética Exército Brasileiro 2017

2.6.2 TIPOS DE ATIVIDADES DE GUERRA CIBERNÉTICAS DO EXÉRCITO BRASILEIRO

As atividades de guerra cibernética a serem executadas pelo Exército Brasileiro podem ser divididas em 3 tipos - quais sejam - a proteção cibernética, a exploração cibernética e o ataque cibernético.

A proteção cibernética é compreendida como uma atividade de caráter permanente que visa impedir ataques e exploração cibernética inimiga contra dispositivos e redes amigas. Essa atividade é realizada desde os tempos de paz, não possui preocupações jurídicas e tem por finalidade testar as vulnerabilidades existentes nas próprias redes informacionais, bem como realizar medidas de proteção do Sistema de Comando e Controle do Exército (SC²Ex). A proteção cibernética não será abordada no escopo deste trabalho.

O foco do trabalho estará voltado para os outros 2 tipos de ações cibernéticas, que o Manual de Doutrina Militar de Defesa Cibernética do Ministério da Defesa descreve da seguinte forma:

> **Exploração Cibernética** - consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas.
> **Ataque Cibernético** - compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

Para o Exército Brasileiro, a atividade de exploração cibernética consiste em obter informações sobre questões técnicas dos sistemas inimigos, coletar informações sobre o modo que o inimigo opera seus sistemas, bem como buscar vulnerabilidades do sistema de tecnologia da informação. Por compreender que a exploração cibernética poderia ser considerada uma entrada não autorizada nas redes informacionais de outras nações, o Exército ressaltou que esta tarefa deve ser realizada com observação do arcabouço normativo e legal vigente.

Já o ataque cibernético é aquele que consiste em utilizar códigos computacionais realizados em dispositivos de redes de computadores (servidores, hardwares, firewalls, etc) com o intuito de negar o uso, destruir ou corromper informações de sistemas críticos computacionais, gerando dano. As ações de ataque cibernético, assim como a de proteção, devem procurar ao

máximo alcançar o princípio da dissimulação, a fim de ocultar a origem do ataque. Tendo em vista a sensibilidade que as ações de ataque cibernético possuem, estas ações devem estar amparadas perante a legislação vigente.

O Exército Brasileiro apresenta também um quadro com as capacidades operativas (CO) da capacidade militar terrestre cibernética, que se confunde com as 3 atividades de guerra cibernética realizadas pelo Sistema de Guerra Cibernética do Exército Brasileiro. conforme tabela 2 abaixo representada.

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Tabela 2 - Capacidades Operativas

Fonte: Manual de Campanha Guerra Cibernética Exército Brasileiro 2017

As capacidades operativas pode ser traduzida como a habilidade que uma unidade militar ou força possua a fim de cumprir a missão recebida da melhor forma possível. Ocorre que, a fim de realizar um emprego mais eficiente e judicioso dos meios disponíveis, cada organização militar integrante do Sistema de Guerra Cibernética do Exército irá possuir uma ou mais capacidades operativas. Dessa forma, no nível tático, o Batalhão de Guerra Eletrônica é a única estrutura com capacidade operativa suficiente para realizar o ataque, a exploração e a proteção cibernética. A exploração cibernética será realizada pelo Batalhão de Comunicações e Guerra Eletrônica, bem como pelo Batalhão de Inteligência Militar. O manual de campanha guerra cibernética, por meio da tabela 3, pormenoriza a responsabilidade de cada tipo de ação cibernética de cada organização militar integrante do SGCEx.

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (B Com)			X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Tabela 3 - Estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades

Fonte: Manual de Campanha Guerra Cibernética Exército Brasileiro 2017

2.7 DIREITO INTERNACIONAL HUMANITÁRIO

Juntamente com a elaboração da carta das Nações Unidas, os membros da Organização das Nações Unidas entenderam que seria importante a elaboração de uma Declaração Internacional a fim de combater à violação dos direitos humanos. (ACCIOLLY; SILVA, 2019)

Nesse sentido, em 1948 foi assinado em Paris a Declaração Universal dos Direitos Humanos. A despeito de ser uma declaração das Nações Unidas, e

assim não ser de cumprimento obrigatório para os países que a ratificaram, a Declaração Universal dos Direito Humanos teve grande importância pois seus princípios passaram a ser observados como normas de direito internacional consuetudinários. (ACCIOLLY; SILVA, 2019)

A Organização das Nações Unidas (2020) considera que a Declaração Universal dos Direitos Humanos estabeleceu pela primeira vez uma proteção universal dos direitos humanos. Em conjunto com uma série de normas e tratados internacionais, implementados a partir de 1945, a Declaração Universal dos Direitos Humanos expandiu a proteção aos direitos inerentes à condição humana, como direitos civis, políticos e de prevenção e repressão ao genocídio.

Nos artigos da Declaração Universal dos Direitos Humanos são pontuados diversos mandamentos protetivos do ser humano. No artigo 5º, a declaração determina que nenhum ser humano poderá ser torturado ou exposto à tratamentos cruéis, desumanos ou degradantes. Prosseguindo, no artigo 12º declara ainda que, nenhuma pessoa poderá sofrer interferência em sua vida privada, de sua família e de sua correspondência. Continua ainda garantindo que, o direito à propriedade fica salvaguardado e que não o indivíduo não pode ser privado de seus bens arbitrariamente. Por fim, no seu artigo 25º, garante que deve ser garantido ao ser humano uma condição mínima que lhe garanta saúde, bem-estar, alimentação, vestuário e assistência médica. (UNITED NATIONS, 1948)

2.7.1 PRINCÍPIOS DO DIREITO INTERNACIONAL HUMANITÁRIO DOS CONFLITOS ARMADOS

Segundo o Comitê Internacional da Cruz Vermelha, o Direito Internacional Humanitário (DIH) é o conjunto de normas do direito internacional público que visam limitar as consequências dos conflitos armados. Esse conjunto de normas é composto por tratados, normas de base consuetudinária, ou seja, baseado nos costumes internacionais, bem como por princípios gerais do direito (CICV, 2022).

Nesse mesmo sentido, o Ministério da Defesa, por meio do Manual de Emprego do Direito Internacional dos Conflitos Armados nas Forças Armadas definiu o conceito de como sendo:

> O Direito Internacional Humanitário é o conjunto de normas internacionais, de origem convencional ou consuetudinária, especificamente destinado a ser aplicado nos conflitos armados, internacionais ou não-internacionais, e que limita, por razões humanitárias, o direito das Partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege as pessoas e os bens afetados, ou que possam ser afetados pelo conflito.

Ainda segundo o mesmo manual do Ministério da Defesa, a humanidade procurou implementar regras sobre os métodos e meios utilizados nos conflitos. Durante o desenrolar da história, houve a pactuação de acordos internacionais e tratados de paz. Contudo, somente em 1864 que foi estabelecida a Convenção de Genebra, a qual versava sobre a proteção das vítimas de conflitos armados, bem como de feridos e doentes.

2.8 CONVENÇÃO DE GENEBRA DE 1949

O Brasil e diversos países firmaram acordo por meio da convenção internacional de Genebra de 1949 destinado a proteger as vítimas provenientes de guerra, para a melhoria da condições dos feridos e enfermos dos exércitos em campanha, bem como para proteção de civis em tempo de guerra. (BRASIL, 1957)

Durante a convenção de genebra, os países signatários se comprometeram em aplicar as suas disposições em caso de guerra declarada ou perante qualquer outro conflito que pudesse surgir entre dois ou mais países. (BRASIL, 1957)

No artigo 3º da Convenção de Genebra ficou determinado que as pessoas que não participem diretamente das hostilidades deverão ser tratadas com humanidade e sem qualquer tipo de diferença em função de sua raça, credo, sexo ou riqueza. Neste mesmo sentido, tratamento digno também deve ser dado para militares que tenham entregue suas armas e para feridos em combate. Dessa forma, a Convenção de Genebra proibiu atentados contra a vida e a integridade física dessas pessoas, bem como tratamento humilhante, degradante, torturas e homicídios. (BRASIL, 1957).

Proteção especial foi dada ainda pelo artigo 6º e 7º da Convenção de Genebra para feridos, enfermos, membros dos serviços de saúde e religiosos, tendo em vista que estes não poderiam renunciar nem mesmo parcialmente aos direitos conferidos em Genebra. (BRASIL, 1957).

Seguindo nesta proteção, o artigo 19 determina que em nenhuma hipótese podem ocorrer ataques que tenham por objetivo o sistema de atendimento hospitalar, sejam estes móveis ou fixos. (BRASIL, 1957)

Por fim, o capítulo IX, nos artigos 49 e 50, determina que as nações contratantes tem o compromisso de fixar nacionalmente a cominação penal a fim de garantir a responsabilização das pessoas que cometam as seguintes infrações graves: homicídio intencional, tortura, experiências biológicas e tratamento desumano contra pessoas protegidas pela convenção; e destruição e apropriação de bens sem fins militares e realizados em grande escala e de maneira arbitrária. (BRASIL, 1957)

2.9 CARTA DAS NAÇÕES UNIDAS

A carta das Nações Unidas foi promulgada pelo Brasil em 1945 após ter sido ratificada pelo pelo governo brasileiro por ocasião da Conferência Internacional das Nações Unidas.

O propósito da constituição das Nações Unidas baseou-se nos objetivos de garantir a paz e a segurança internacional, tendo como princípio a solução pacífica de controvérsias internacionais, bem como evitar o uso da força entre as nações. (BRASIL, 1945)

A Organização das Nações Unidas é uma associação de países que tem objetivo claro de realizar a manutenção da paz e a segurança internacional, favorecer o desenvolvimento de relações amistosas em prol da cooperação internacional bem como resolver questões internacionais relacionadas ao desenvolvimento econômico, social, cultural e humanitário no mundo (ACCIOLLY; SILVA, 2019).

Constituem órgãos das Nações Unidas o Conselho de Segurança e a Corte Internacional de Justiça. O Conselho de Segurança decide sobre as principais questões relacionadas aos países membros e a Corte seria um órgão com jurisdição sobre os países membros que teria condições de assegurar a solução de controvérsias entre os estados.

O Conselho de Segurança é o orgão no qual devem ser levadas as demandas que digam respeito à violação da paz e da segurança internacional, e este tem competência coercitiva para fazer frente à ameaça, inclusive com o uso de força armada. A despeito da existência dessa capacidade de resposta, a

Carta das Nações Unidas reconhece em seu artigo 51 o direito de legítima defesa, seja esta indivudual ou coletiva. O uso da legítima defesa poderá ser exercido pelo estado que tenha sofrido, ou esteja na eminência de sofrer, agressão armado, até que o Conselho de Segurança tome as medidas necessárias ao reestabelecimento da paz. (ACCIOLLY; SILVA, 2019).

2.9.1 DEFINIÇÃO DE AGRESSÃO ARMADA DA ONU

A Assembleia Geral da Organização das Nações Unidas publicou por meio da Resolução nº 3.314 de 14 de dezembro de 1971 a adoção de uma definição de agressão.

No preâmbulo da Resolução 3.314 ressaltou que o Conselho de Segurança da ONU tem o condão de determinar a existência de ameaça à paz, podendo tomar medidas para restaurar a segurança das nações.

Nesse sentido, a Assembleia Geral da ONU considerou também que a agressão é a forma mais grave e perigosa que uma nação pode realizar o uso ilegal de força contra outro estado. Dessa forma, tornou-se imperioso que a Organização das Nações Unidas adotasse uma definição clara de agressão, a fim de simplificar a identificação de atos de agressão dirigidos de um estado para outro. Dessa forma, no artigo I da Resolução 3.314 foi apresentada a seguinte definição de agressão:

> Agressão é o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou de qualquer outra forma inconsistente com a Carta das Nações Unidas, conforme estabelecido nesta Definição.

Além disso, no artigo 3º, a Resolução nº 3.314 considera também que a invasão e/ou o ataque de uma força armada, a ocupação militar do território, o bombardeio realizado pelas forças armadas ou o uso de qualquer arma de um estado contra o outro também será considerado como agressão.

Por fim, nos artigos 4º e 8º, a Assembleia Geral orienta que a definição apresentada para agressão não é taxativa, sendo a interpretação e a aplicação desta norma realizada em consonância com outros dispositivos, possibilitando ainda que o Conselho de Segurança determine que outros atos não descritos nesta definição sejam considerados como agressão.

2.10 O TRIBUNAL PENAL INTERNACIONAL

O Estatuto de Roma, de 1998, instituiu o primeiro Tribunal Penal Internacional. Este tribunal tem competência jurisdicional para julgar crimes de genocídio, crimes contra a humanidade, crimes de guerra e crimes de agressão. A intensão do Tribunal é complementar e não substituir a atividade jurisdicional dos Estados. Apesar de não ser um órgão das Nações Unidas, o Tribunal Penal Internacional trabalha em cooperação com a ONU a fim de coibir e reprimir crimes desta natureza (INTERNATIONAL CRIMINAL COURT, 2023).

O Congresso Nacional ratificou o texto, e o Presidente da República promulgou o Estatuto de Roma no ano de 2002. Em seu preâmbulo, o Estatuto de Roma considerou que milhares de pessoas tem sido vítimas de crimes em todo o mundo e que a depender da gravidade de tal crime este torna-se verdadeira ameaça à paz e à segurança mundial, não podendo desta forma permanecer sem punição. Determinou também que o tribunal possuirá caráter permanente e com poder jurisdicional para julgar crimes de grande importância perante a comunidade internacional (BRASIL, 2002)

Dentro da competência da corte internacional, o Tratado de de Roma considera como crime de genocídio captulado pelo artigo 6º como sendo qualquer ato de homicídio, ofensa grave à integridade física ou mental, imposição de condições de vida que provoquem sua destruição, impedimento de nascimentos dirigidos contra grupos nacionais, étnicos, raciais e religiosos. (BRASIL, 2002)

Os crimes contra a humanidade são descritos no artigo 7º do Tratado de Roma. As ações de homicídio, extermínio, escravidão, deportação ou transferência forçada de um povo, prisões e restrições de liberdade, tortura, agressão e exploração sexual e perseguição de grupos políticos, raciais e religiosos, quando realizados em uma situação generalizada ou sistemática contra a população civil são considerados crimes contra a humanidade. (BRASIL, 2002)

Além dos crimes citados acima, o Tribunal Penal Internacional também tem competência para julgar os crimes de guerra realizados em desfavor de pessoas e bens protegidos pela Convenção de Genebra (BRASIL, 2002).

2.10.1 CRIMES DE GUERRA

O artigo 8º do Tratado de Roma define os crimes de guerra que serão julgados pela corte. Este artigo determina que as ações tituladas como homicídio doloso (com intenção do agente), tortura e tratamentos desumanos, experiências biológicas e destruição ou apropriação de bens em grande escala sem justificativa militar serão consideradas crimes de guerra e serão sujeitas a cominação penal internacional. Considera também como crime de guerra a realização de ataques intencionais contra bens civis que não possuam objetivos militares, ataques que provoquem a morte ou ferimento em civis, danos a bens civis (BRASIL, 2002).

Segundo o artigo 8º do Tratado de Roma, também é considerado como crime de guerra o fato de realizar ataques dirigidos contra hospitais e unidades hospitalares (BRASIL, 2002).

A responsabilização criminal da corte internacional será aplicada de forma individual, para todo e qualquer agente de um estado que cometer, ordenar, facilitar ou contribuir para a ocorrência dos crimes descritos no Tratado de Roma (BRASIL, 2002).

3. METODOLOGIA

O presente trabalho se propôs a realizar uma pesquisa bibliográfica com base na doutrina jurídica existente acerta do assunto tratado, bem como em artigos e revistas científicas. A pesquisa bibliográfica utilizou a doutrina de referencia para seleção das fontes, com autores renomados em cibernética, direito constitucional, e direito internacional.

Tendo por base as condições técnicas das ações de guerra cibernética, foi feita uma correlação dessas ação à luz do pensamento jurídico nacional e internacional a fim de contribuir para a solução do problema apresentado.

A fim de contribuir e proporcionar maior credibilidade com os dados alcançados, foi realizado um questionário com integrantes do Comando de Defesa Cibernética do Exército Brasileiro, a fim de esclarecer sobre as peculiaridades do emprego da guerra cibernética bem como sobre suas implicações jurídicas.

Foi realizada uma ampla pesquisa bibliográfica a fim de trazer fontes robustas para a pesquisa. Após a abordagem teórica do emprego da guerra

cibernética, bem como dos temas de direito relacionados com a atividade, foram realizados questionários com os militares integrantes do Comando de Defesa Cibernética.

3.1 OBJETO FORMAL DE ESTUDO

O objeto formal do estudo desta pesquisa foi centrado nas limitações legais impostas às ações de guerra cibernéticas. Essas limitações são impostas pela ordem constitucional vigente, pela legislação penal, pelas relações internacionais e pelo direito internacional dos conflitos armados. As limitações cíveis não foram objeto de estudo deste trabalho.

3.2 DELINEAMENTO DA PESQUISA

O presente trabalho tem por característica ser uma pesquisa bibliográfica e documental exploratória. A pesquisa se propôs a realizar o aprofundamento do conhecimento sobre as implicações legais sobre o emprego da guerra cibernética, por meio de uma coleta de dados técnicos a respeito da doutrina militar de emprego da guerra cibernética pelo Exército Brasileiro, bem como jurídica, tendo como referência importantes juristas das mais diversas áreas do direito. Utilizou como fonte referencial para análise do assunto os materiais já publicados (pesquisa bibliográfica), como por exemplo livros, artigos, monografias e doutrina, bem como de fontes primárias (documental), oriundo de leis, tratados, códigos e manuais de emprego militar.

Quanto a forma de abordagem, a pesquisa é qualitativa, tendo em vista que a observação sob o ponto de vista jurídico da doutrina militar de emprego necessita de uma análise crítica, subjetiva, e carece de interpretação e subsunção da norma jurídica ao fato estudado, não sendo possível analisá-la conforme números.

O questionário digital por meio da plataforma google forms proporcionou a coleta de informações e suas percepções junto aos militares integrantes do Comando de Defesa Cibernética a respeito das capacidades e limitações da guerra cibernética, bem como os principais problemas jurídicos enfrentados. A forma digital proporcionou a possibilidade de coletar uma quantidade maior de resposta, no menor tempo possível.

Para a coleta de dados, foram utilizados instrumentos de busca bibliográfica, documental e por meio de questionário, todos de forma digital.

Os acervos digitais possuem grande quantidade de material bibligráfico à disposição do pesquisador, fato que proporciona uma vasta pesquisa sob diferentes abordagens.

O uso de ferramentas digitais proporciona o acesso a grande quantidade de leis, tratados, acordos internacionais, manuais de emprego militar e manuais de doutrina militar.

Quanto à natureza da pesquisa, trata-se de uma pesquisa do tipo aplicada. Os conhecimentos produzidos com esta pesquisa poderão ser empregados pelo Exército Brasileiro no aperfeiçoamento da doutrina militar de emprego e como orientação aos guerreiros cibernéticos sobre as implicações jurídicas da atividade.

3.3 AMOSTRA

A pesquisa utilizou os oficiais e sargentos do Exército Brasileiro integrantes do Comando de Defesa Cibernética, do 1º Batalhão de Guerra Eletrônica do Exército, do 1º Batalhão de Comunicações e Guerra Eletrônica de Selva possuidores do curso de guerra cibernética e oficiais da assessoria jurídica como amostra para coleta de dados por meio de questionário.

Tendo em vista a especificidade da atividade estudada, o público amostra da pesquisa foi de aproximadamente 13 militares.

3.4 PROCEDIMENTOS PARA REVISÃO DA LITERATURA

Para a revisão da literatura, esta pesquisa buscou utilizar os mais recentes manuais de doutrina militar terrestre a respeito do emprego da guerra cibernética pelo Exército Brasileiro e pelo Ministério da Defesa. Foi utilizada ainda como fonte a biblioteca digital do Exército Brasileiro a fim de que as principais pesquisas sobre doutrina militar integrem a revisão da literatura.

No campo da ciência jurídica, as principais fontes do direito constitucional, penal e internacional foram utilizados como referência. Foram utilizadas as plataformas google academy e scielo Brasil a fim de que fossem realizadas

buscas de artigos e pesquisas científicas a respeito de temas jurídicos correlatos com esta pesquisa.

Para consulta da legislação nacional foi utilizado o site do governo federal com as leis vigentes.

Como critérios de inclusão, foram utilizados manuais do Ministério da Defesa, do Exército Brasileiro e bibliografia estrangeira técnica sobre a cibernética e a legislação nacional bem como tratados e acordos internacionais dos quais o Brasil tomou parte e o congresso nacional ratificou. Foram incluídos também trabalhos científicos de instituição reconhecidas no estudo da doutrina militar terrestre, como por exemplo as publicações do Observatório Militar da Praia Vermelha (Escola de Comando e Estado Maior do Exército). Para o estudo das ciências jurídicas foram utilizadas plataformas confiáveis de pesquisa acadêmica, como por exemplo a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

Como critério de exclusão, foram retiradas as legislações nacionais de caráter civil e penal. Foram excluídas também as fontes bibliográficas que não utilizaram referencial robusto e confiável.

3.5 ANÁLISE DOS DADOS

Foi realizada a coleta bibliográfica, documental e por meio do questionário aplicado no grupo citado.

A coleta bibliográfica buscou os aspectos técnicos sobre as possibilidades do emprego da guerra cibernética e as considerações jurídicas dos principais teóricos do direito nacional e internacional. A pesquisa tratou também sobre as considerações técnicas de experientes integrantes do Comando de Defesa Cibernética a respeito das possibilidades e limitações e jurídicas da guerra cibernética.

Após a coleta das fontes bibliográficas e dos questionários realizados, foi procedida uma análise qualitativa a fim de proporcionar uma resposta ao problema discutido. Essa análise levou em consideração aspectos técnicos tanto do emprego militar quanto das ciências jurídicas.

Por fim, realizou-se uma analise qualitativa de todos os dados obtidos, por meio de métodos indutivos e subjetivos, a fim de alcançar a demonstração das principais limitações jurídicas impostas à guerra cibernética.

4. RESULTADOS

A presente pesquisa buscou detalhar as possibilidades e limitações das ações de guerra cibernética e compreender se ações cibernéticas poderiam ser consideradas agressões armadas entre nações e ensejar dessa forma a responsabilização penal internacional pelo Tribunal Penal Internacional. O questionário apresentou perguntas com respostas objetivas do tipo sim e não e foram destinadas ao público alvo abordado na metodologia. O questionário foi enviado para o público alvo no período de 27 de abril de 2023 e esteve disponível para receber respostas até 14 de maio de 2024.

A atividade de cibernética dentro das forças armadas se trata de uma atividade bem específica e desta forma o grupo amostral para o qual se destinou a pesquisa é bem reduzido. Em função dessa peculiaridade, o questionário foi respondido por um total de 13 militares, tendo em vista que foi destinado para Oficiais e Sargentos possuidores do curso de guerra cibernética, integrantes de Organizações militares que exercem atividades cibernéticas e assessores jurídicos de unidades militares que realizam atividades desta área.

Foram feitas um total de 16 perguntas de caráter qualitativo com respostas objetivas do tipo sim e não.

A primeira pergunta questionou se o público amostral possui conhecimento sobre a norma de direito internacional dos conflitos armados (convenção de Genebra de 1949 e seus protocolos adicionais). Um total de 10 militares (76,9%) responderam que possuem conhecimento, enquanto 3 militares (23,1%) responderam que não possuem conhecimento. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 4 a seguir:

Tabela 4 - Conhecimento sobre DICA(convenção de Genebra e seus protocolos adicionais)

A segunda pergunta questionou se o público amostral possui conhecimento sobre a norma de direito internacional que instituiu o Tribunal Penal Internacional. Um total de 9 militares (69,2%) responderam que possuem conhecimento, enquanto 4 militares (30,8%) responderam que não possuem conhecimento. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 5 a seguir:

Tabela 5 - conhecimento sobre a norma que instituiu o Tribunal Penal Internacional

A terceira pergunta questionou se o público amostral possui conhecimento sobre as limitações legais impostas pelo direito internacional à atividade de guerra cibernética. Um total de 7 militares (53,8%) responderam que não possuem conhecimento, enquanto 6 militares (46,2%) responderam que

possuem conhecimento. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 6 a seguir:

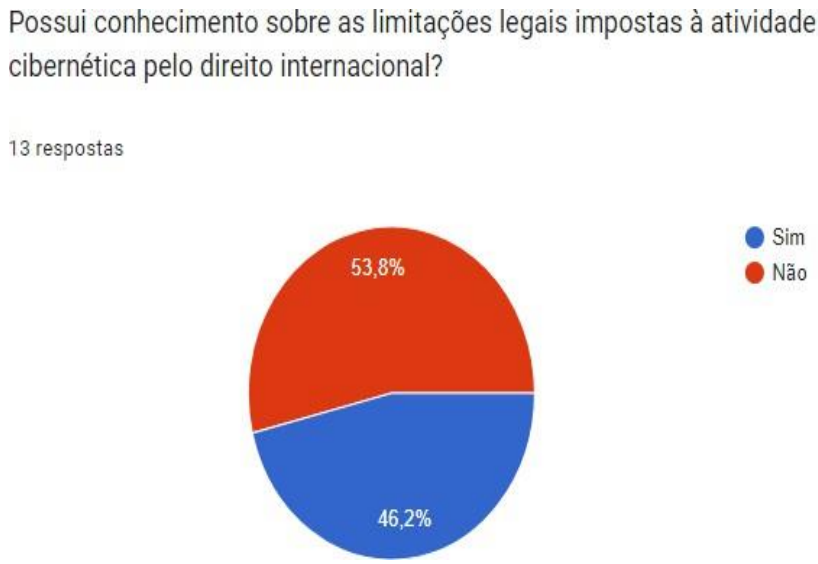

Tabela 6 - conhecimento sobre limitações legais impostas à atividade de guerra cibernética pelo direito internacional

A quarta pergunta questionou se o público amostral possui conhecimento sobre a definição de agressão armada da Organização das Nações Unidas. Um total de 08 militares (61,5%) responderam que possuem conhecimento, enquanto 5 militares (38,5%) responderam que não possuem conhecimento. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 7 a seguir:

Tabela 7 - conhecimento sobre a definição de agressão armada da Organização das Nações Unidas

A quinta pergunta questionou o público amostral se ações cibernéticas de caráter exploratório (busca e coleta) dirigidas de um país para outro teriam condições de gerar dano à direitos civis, políticos, sociais, econômicos e culturais em outros povos. Um total de 09 militares (69,2%) responderam que as ações cibernéticas de caráter exploratório teriam condições de causar danos aos direitos citados, enquanto 4 militares (30,8%) responderam que não teriam. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 8 a seguir:

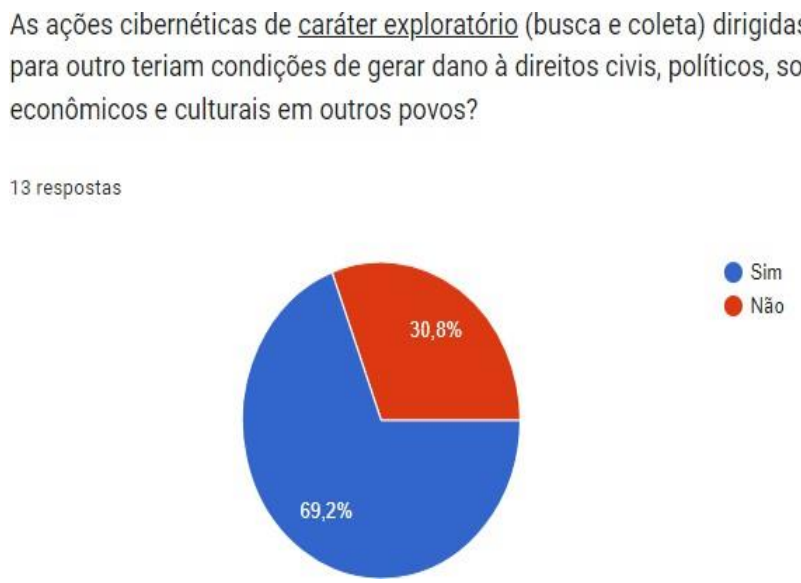

Tabela 8 - ações cibernéticas de caráter exploratório teriam condições de gerar dano à direitos civis, políticos, sociais, econômicos e culturais em outros povos

A sexta pergunta questionou o público amostral se ações cibernéticas de caráter exploratório (busca e coleta) dirigidas de um país para outro teriam condições de ferir a soberania, integridade territorial ou independência política de outro Estado. Um total de 09 militares (69,2%) responderam que as ações cibernéticas de caráter exploratório teriam condições de causar danos aos direitos citados, enquanto 4 militares (30,8%) responderam que não teriam. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 9 a seguir:

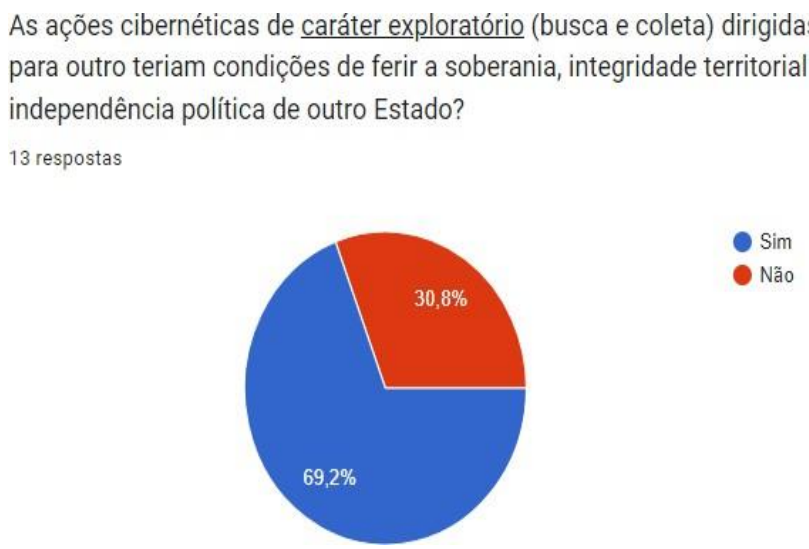

Tabela 9 - ações cibernéticas de caráter exploratório (busca e coleta) dirigidas de um país para outro teriam condições de ferir a soberania, integridade territorial ou independência política de outro Estado

A sétima pergunta questionou o público amostral se ações cibernéticas ofensivas de ransomware dirigidas inicialmente contra um alvo militar teriam condições de acidentalmente ocasionar a criptografia de todos os dados de um hospital instalado na área do Teatro de Operações ou em áreas de retaguarda. Um total de 12 militares (92,3%) responderam que sim, enquanto 1 militar (7,7%) respondeu que não teria. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 10 a seguir:

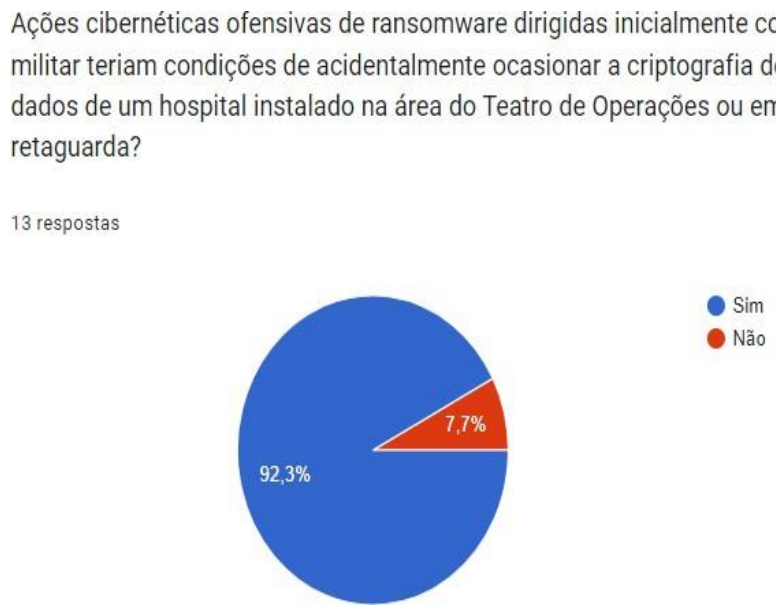

Tabela 10 - ações cibernéticas ofensivas de ransomware dirigidas inicialmente contra um alvo militar teriam condições de acidentalmente ocasionar a criptografia de todos os dados de um hospital instalado na área do Teatro de Operações ou em áreas de retaguarda

A oitava pergunta questionou o público amostral se ações cibernéticas ofensivas teriam condições de gerar danos aos sistemas de uma estação de produção/distribuição de energia elétrica vindo a interromper o seu fornecimento. Um total de 12 militares (92,3%) responderam que sim, enquanto 1 militar (7,7%) respondeu que não teria. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 11 a seguir:

Tabela 11 - ações cibernéticas ofensivas teriam condições de gerar danos aos sistemas de uma estação de produção/distribuição de energia elétrica vindo a interromper o seu fornecimento

A nona pergunta questionou o público amostral se ações cibernéticas ofensivas teriam condições de gerar alteração no comportamento de equipamentos de uma usina nuclear causando um dano físico em sua estrutura e consequente vazamento de material nuclear. Todos os 13 militares (100%) responderam que sim. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 12 a seguir:

Tabela 12 - ações cibernéticas ofensivas teriam condições de gerar alteração no comportamento de equipamentos de uma usina nuclear causando um dano físico em sua estrutura e consequente vazamento de material nuclear

A décima pergunta questionou o público amostral se ações cibernéticas ofensivas teriam condições de realizar a subtração de valores financeiros de contas bancárias de civis, incluindo criptomoedas. Todos os 13 militares (100%) responderam que sim. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 13 a seguir:

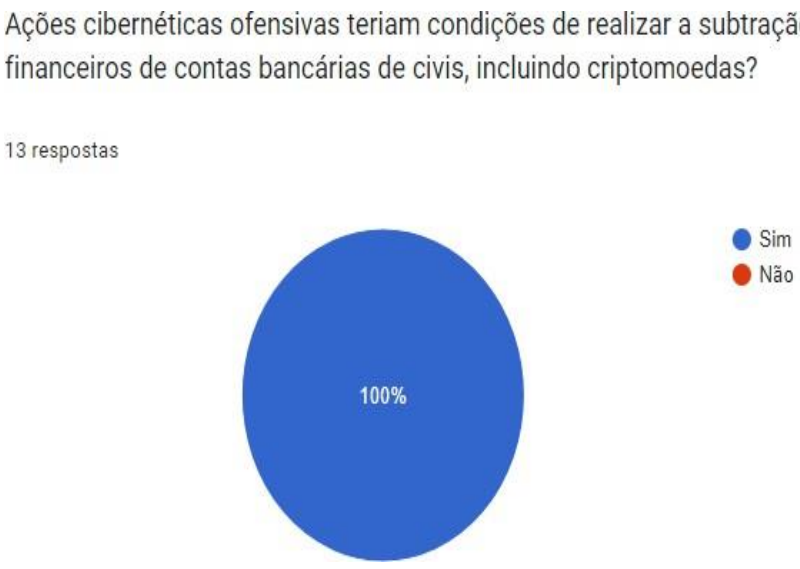

Tabela 13 - ações cibernéticas ofensivas teriam condições de realizar a subtração de valores financeiros de contas bancárias de civis, incluindo criptomoedas

A décima primeira pergunta questionou o público amostral se ações cibernéticas ofensivas teriam condições de negar acesso à sites do Sistema Financeiro Nacional de outro Estado. Todos os 13 militares (100%) responderam que sim. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 14 a seguir:

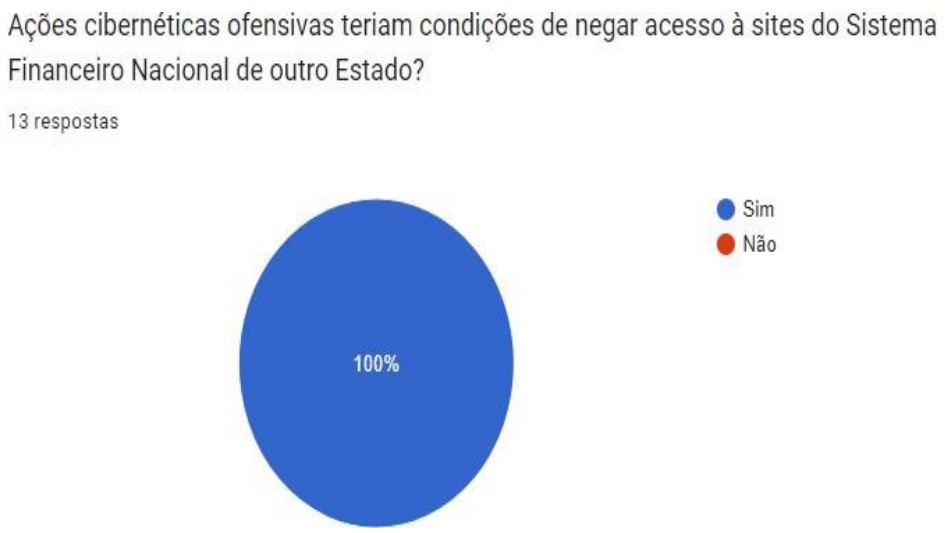

Tabela 14 - ações cibernéticas ofensivas teriam condições de negar acesso à sites do Sistema Financeiro Nacional de outro Estado

A décima segunda pergunta questionou o público amostral se ação ofensiva conhecida como "troll de rede social", dirigido de um país contra outro, teria condições de mudar a opinião pública de determinado grupo, e assim afetar a independência política de um Estado. Um total de 9 militares (69,2%) responderam que sim, enquanto 4 militares (30,8%) respondeu que não teria. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 15 a seguir:

Tabela 15 - ação ofensiva conhecida como "troll de rede social", dirigido de um país contra outro, teria condições de mudar a opinião pública de determinado grupo, e assim afetar a independência política de um Estado

A décima terceira pergunta questionou o público amostral se ações cibernéticas de caráter ofensivo dirigidas de um país contra outro teriam condições de gerar dano à vida, à direitos civis, políticos, sociais e culturais em outros povos. Um total de 12 militares (92,3%) responderam que sim, enquanto 1 militar (7,7%) respondeu que não teria. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 16 a seguir:

Tabela 16 - ações cibernéticas de caráter ofensivo dirigidas de um país contra outro teriam condições de gerar dano à vida, à direitos civis, políticos, sociais e culturais em outros povos

A décima quarta pergunta questionou o público amostral se ações cibernéticas de caráter ofensivo, dirigidas de um país para outro, teriam condições de ferir a soberania, integridade territorial ou a independência política de outro Estado. Um total de 10 militares (90,9%) responderam que sim, enquanto 1 militar (9,1%) respondeu que não teria. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 17 a seguir:

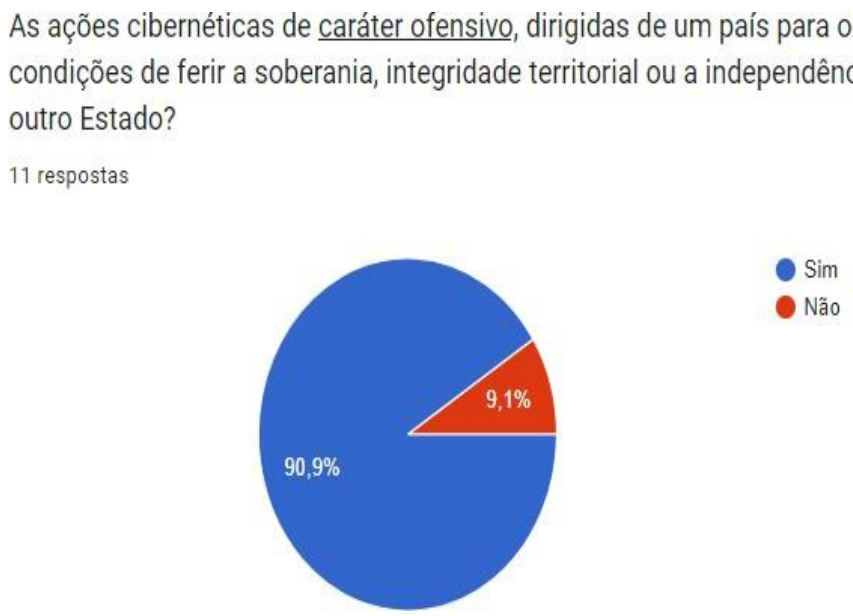

Tabela 17 - ações cibernéticas de caráter ofensivo, dirigidas de um país para outro, teriam condições de ferir a soberania, integridade territorial ou a independência política de outro Estado

A décima quinta pergunta questionou o público amostral se uma ação cibernética ofensiva dirigida de um país para outro poderia ser considerada uma agressão armada entre nações. Todos os 13 militares (100%) responderam que sim. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 18 a seguir:

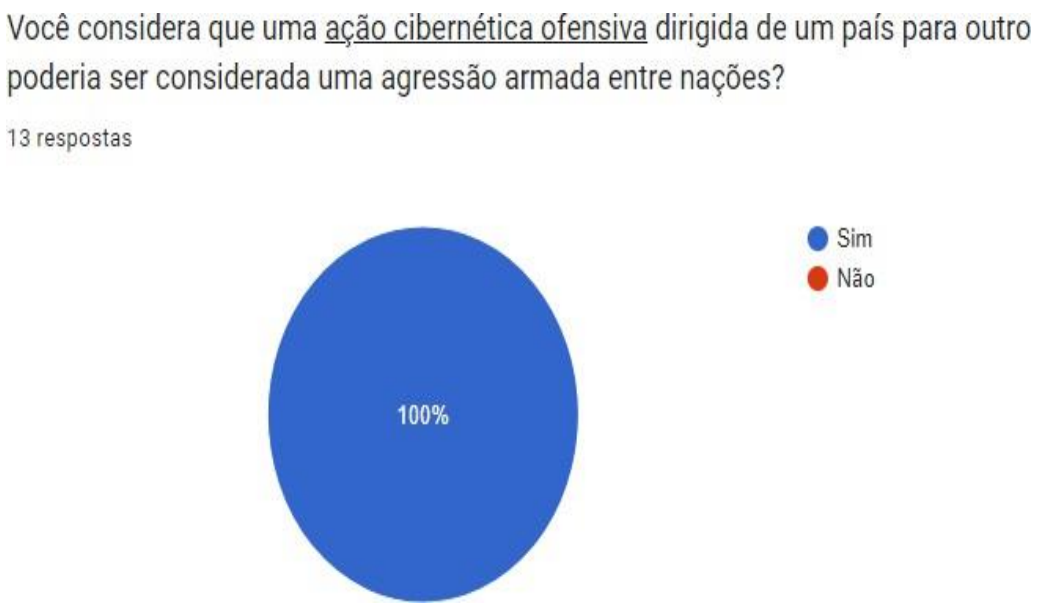

Tabela 18 - ação cibernética ofensiva dirigida de um país para outro poderia ser considerada uma agressão armada entre nações

A décima sexta e última pergunta questionou o público amostral se uma ação cibernética exploratória dirigida de um país para outro poderia ser considerada uma agressão armada entre nações. Um total de 7 militares (53,8%) responderam que não, enquanto 6 militares (46,2%) que sim. A resposta segue da seguinte forma estatística, conforme ilustra a tabela nº 19 a seguir:

Tabela 19 - uma ação cibernética exploratória dirigida de um país para outro poderia ser considerada uma agressão armada entre nações

5. DISCUSSÃO DOS RESULTADOS

A análise e a discussão dos resultados objetos da presente pesquisa científica foram baseados em métodos qualitativos, tendo em vista que a temática diz respeito à conceitos e interpretações jurídicas a respeito da doutrina de emprego da guerra cibernética.

5.1 ASPECTOS JURÍDICOS NACIONAIS E INTERNACIONAIS

As Forças Armadas devem seguir os princípios constitucionais previstos na Carta Magna Brasileira de 1988 no que diz respeito à preservação dos direitos humanos, a não-intervenção em outros países, a proteção da paz e principalmente pela busca da solução pacífica de controvérsias internacionais, caso ocorram.

Dado a conjuntura nacional e internacional, a nação Brasileira entendeu que seria fundamental para a defesa nacional a implementação de ações voltadas para o espaço cibernético, cabendo ao Exército o desenvolvimento deste setor estratégico. Dessa forma, o amparo legal para a atividade de guerra cibernética desenvolvida pelo Exército Brasileiro encontra seu alicerce pautado sobre a Política Nacional de Defesa, o qual designou para o Exército Brasileiro a missão de desenvolver o setor estratégico da cibernética.

No ambiente internacional, após o término da 2ª Guerra Mundial, a comunidade de países entendeu que a criação da Organização das Nações Unidas seria fundamental para contribuir com a manutenção da paz e da segurança internacional, bem como favoreceria a cooperação entre as nações na solução de problemas internacionais. Com isso, diversas medidas foram sendo tomadas e órgãos e organismos internacionais foram sendo criados ao longo do século XX com o objetivo de garantir a paz e garantir a solução pacífica de controvérsias entre estados nacionais.

Ainda por ocasião da criação da ONU, ficou assegurado o respeito ao uso da legítima defesa contra uma injusta agressão sofrida por outro país. Entretanto, para garantir segurança jurídica na fruição do uso do direito de legítima defesa seria importante o perfeito entendimento sobre a definição de agressão.

Prosseguindo na trilha da proteção aos direitos humanos, a ONU publicou a Declaração dos Direito Humanos em 1948. Esta declaração estabeleceu pela primeira vez as orientações a serem seguidas a fim de se garantir a proteção

dos direito básicos do homem, como a proteção de direitos civis, políticos e de dignidade humana.

Somente no ano seguinte, em 1949 que, um acordo internacional foi firmado por meio da Convenção de Genebra, com a finalidade de proporcionar certo ordenamento jurídico em meio ao caos da guerra. A Convenção de Genebra buscou proteger os direitos humanos de todos os envolvidos em um conflito armado, sejam estes combatentes ou civis.

A Assembleia Geral da ONU considerou que a agressão é a forma ilegal que um estado pode fazer uso da força contra outra nação. Dessa forma, a agressão é ó uso de força armada sobre outro estado que afete sua soberania, integridade territorial ou sua independência política. Além disso, o entendimento sobre agressão é extensivo a mais interpretações, podendo ser considerado também como o avanço de uma força armada sobre a soberania ou território de um outro estado e também como o uso de qualquer tipo de armamento sobre outra nação.

Com a criação do Tribunal Penal Internacional houve de fato uma sistematização a respeito da responsabilização penal do indivíduo que vai além das fronteiras nacionais. Dessa forma, passou-se a investigar, julgar e condenar crimes de genocídio, crimes contra a humanidade, crimes de guerra e crimes de agressão de grande importância mundial.

Com o Estatudo de Roma de 1998 foi possível definir internacionalmente que ações de homicídio doloso, tratamento desumano, desapropriação e destruição de bens civis em larga escala, ataques contra unidades de tratamento de saúde podem ser consideradas como ações criminosas perante a comunidade internacional e assim sujeitar os agentes à condenações penais.

5.2 A GUERRA CIBERNÉTICA

O Brasil avançou no domínio do espaço cibernético a partir do início do século XXI, principalmente por meio da Política Nacional de Defesa, com a criação do Comando de Defesa Cibernética e com a inserção do Objetivo Estratégico do Exército de atuar com liberdade no espaço cibernético.

Por ser uma atividade sensível e capaz de causar danos extensos, os níveis de decisão sobre quais ações realizar e quando realizá-las perpassa por

toda a cadeia de comando, extrapolando o nível tático e chegando até o nível político.

As ações de cibernéticas devem ser observadas como um sistema de combate de fogos, que tem condições de atuar por meio de redes de computadores causando baixas, danos materiais, físicos e econômicos. Corroborando com isso, o público amostral considerou que ações cibernéticas, principalmente as de ataque, teriam condições de gerar danos a direitos civis, políticos, sociais e econômicos. As ações cibernéticas teriam condições também de ferir a soberania, a integridade territorial e a independência política de uma nação.

A respeito das técnicas de ações cibernéticas, ações ofensivas de ransomware poderiam causar a criptografia de dados em um hospital instalado no teatro de operações em uma situação de guerra. Tal fato poderia vir a atrasar ou até mesmo interromper diversos serviços médicos, trazendo consequência graves como a morte e o agravamento do quadro clínicos de feridos em combate. Além do mais, a própria instalação hospitalar é protegida internacionalmente por força de tratados e convenções contra ataques militares.

Ações cibernéticas ofensivas poderiam também gerar dano ao sistema de produção e distribuição de energia de um país. A interrupção de energia elétrica da população civil de forma ampla, extensa e sem objetivos militares claros poderia vir a trazer sofrimento desnecessário à população civil na medida que atualmente a energia elétrica é vital ao funcionamento de diversas estruturas ligadas à condição básica de existência do homem, como por exemplo o funcionamento de equipamentos hospitalares e a conservação e preparação de alimentos.

As ações cibernéticas ofensivas seriam capazes de gerar grave dano à estruturas críticas de produção de energia nuclear. O dano nessas estruturas poderia causar o vazamento de material radioativo e este seria capaz de causar mortes em larga e escala e sofrimento desnecessário à população civil.

A respeito de bens e propriedades civis, as ações cibernéticas ofensivas teriam condições de realizar a subtração de valores de contas bancárias civis e ainda a possibilidade de negar acesso ao sistema financeiro de um outro estado.

5.3 AÇÕES CIBERNÉTICAS E O DIREITO

Ao realizar a correlação das bases legais existentes em tratados e convenções internacionais que o Brasil participou com as ações cibernéticas podemos realizar uma análise qualitativa sobre as doutrina militar de guerra cibernética e a doutrina jurídica.

Com relação as possibilidades de guerra cibernética, percebe-se que as capacidades militares no espaço cibernético vão desde de atividades de defesa e proteção cibernética, passando por medidas de exploração cibernética e terminando com ações ofensivas. As ações ofensivas possuem capacidade de realizar a criptografia de dados de redes de computadores, impedir o acesso de diversos sistemas tecnológicos e ainda tem condições de gerar danos físicos em infraestruturas críticas de produção e distribuição de energia elétrica.

No âmbito nacional, o amparo legal para a atividade militar de cibernética encontra repouso no âmbito da Política Nacional de Defesa, entretanto, carece de um arcabouço jurídico mais robusto a fim de proporcionar maior segurança jurídica aos operadores de guerra cibernética.

Na esfera internacional, as atividades de guerra cibernética podem ser limitadas por uma série de acordos e tratados internacionais dos quais o Brasil é parte.

Considerando as capacidades e possibilidades cibernéticas levantadas durante esta pesquisa, e confrontando-as com o arcabouço jurídico internacional, seria possível que ações cibernéticas ofensivas produzissem danos físicos e sofrimento desnecessário na população civil. Teria condições também de paralisar o atendimento médico em hospitais em uma situação de combate. Poderiam também realizar a apropriação de bens civis e subtração de valores financeiros do sistema bancário. Poderiam também levar ao vazamento de material radioativo oriundo de usinas de produção de energia nuclear, provocando a contaminação e morte de milhares de pessoas. Todas essas ações, ao analisar a legislação internacional da qual o Brasil faz parte, poderiam ser considerado uma agressão internacional. Essas ações ciberneticas poderiam também ser consideradas como crimes de guerra e dessa forma sujeitar seus agentes à cominação penal pelo tribunal penal internacional.

5.4 APERFEIÇOAMENTO DOS OPERADORES CIBERNÉTICOS

Com relação ao conhecimento técnico dos operadores de guerra cibernética, é possível considerar que o Exército Brasileiro necessita dedicar atenção especial à instruções sobre a legislação internacional que podem ter relação com a atividade cibernética. Aproximadamente 23% da amostra não tinha conhecimento sobre a Convenção de Genebra (Direito Internacional dos Conflitos Armados), 30% da amostra não tinha conhecimento sobre a legislação do Tribunal Penal Internacional e 53% da amostra não teria conhecimento sobre as limitações legais impostas à atividade de guerra cibernética pelo direito internacional.

6. CONCLUSÕES

A presente pesquisa buscou realizar uma pesquisa bibliográfica ampla, relacionando questões técnicas e doutrinárias do emprego militar da guerra cibernética com aspectos jurídicas, principalmente ao que concerne ao Direito Internacional dos Conflitos armados e crimes de guerra.

Após a coleta de dados realizada juntamente com uma análise qualitativa dos dados com a pesquisa bibliográfica realizada, foi possível concluir sobre as limitações jurídicas impostas à atividade de guerra cibernética, bem como se uma ação cibernética pode ser considerada uma agressão e se é possível uma responsabilização por crime de guerra pelas ações cibernéticas realizadas.

Para o emprego da guerra cibernética em um contexto de guerra, o espaço cibernético dever ser utilizado buscando atender às diretrizes existentes na Declaração Universal dos Direitos Humanos, na convenção de Genebra e no Tratado de Roma.

As ações de guerra cibernética são não devem ser dirigidas contra hospitais, não devem realizar a apropriação de bens civis sem objetivos militares, não podem trazer sofrimento desnecessário e de forma indiscriminada para a população civil, deve ser pautada pela proteção da população civil e da manutenção de condições mínimas para a existência humana durante as hostilidades. Dessa forma, as ações cibernéticas estarão legalmente amparadas perante a comunidade internacional.

Como sugestão para a doutrina militar, o Exército Brasileiro deve criar uma espécie de “regra de engajamento” para as ações ofensivas de guerra

cibernética, a fim de orientar os chefes militares e operadores cibernéticos em todos os níveis sobre a limitação das ações cibernéticas. Além disso, deve ser criado um “Plano de fogos não-cinéticos” a ser incluído na documentação da Ordem de Operações de um escalão considerado.

Além disso, o legislador Brasileiro deve buscar o aperfeiçoamento do arcabouço jurídico nacional a fim de proporcionar segurança jurídica para a atuação no espaço cibernético.

REFERÊNCIAS

ACCIOLLY, Hildebrando; SILVA, G. E. do Nascimento e. **Manual de Direito Internacional Público**. 24. ed. São Paulo: Saraiva, 2019. Atualizado por Paulo Borba Casella.

ANDRESS, Jason; WINTERFELD, Steve. **Cyber Warfare: techniques, tactics and tools for security practitioners**. Waltham: Elsevier, 2011. 321 p.

BRASIL. **Decreto nº 19.841**, de 22 de outubro de 1945. Disponível em <https://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm>. Acessado em 10 julho 2023.

BRASIL. **Decreto nº 42.121**, de 21 de agosto de 1957. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D42121.htm>. Acessado em 10 julho 2023.

BRASIL. Constituição (1988) **Constituição da República Federativa do Brasil.** Disponível em: <https://www.planalto.gov.br/c/constituicao/constituicao.htm>. Acessado em 11 novembro 2022.

BRASIL. **Decreto nº 4.388**, de 25 de setembro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm. Acesso em: 04 maio 2023

BRASIL. **Decreto nº 5.484**, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm>. Acessado em 09 novembro 2022.

BRASIL. **Decreto nº 6.703**, de 18 de dezembro de 2008. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm>. Acessado em 09 novembro 2022.

BRASIL. Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014. **Doutrina Militar de Defesa Cibernética**. Brasília, DF, 19 nov. 2014.

BRASIL. Portaria nº 003/EME, de 05 de janeiro de 2015. **Manual de Campanha Eb20-Mc-10.206 Fogos**. 1. ed. Brasília, DF, 09 jan. 2015.

BRASIL. Portaria nº 42/COTER, de 08 de junho de 2017. **Manual de Campanha Eb70-Mc-10.232 Guerra Cibernética**. 1. ed. Brasília, DF, 23 jun. 2017.

BRASIL. CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (Brasil) **Apresentação**. 2023. disponível em: <https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao>. Acesso em: 10 março 2023.

BRASIL. CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (Brasil) **Números**. 2023. disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral. Acesso em: 10 março 2023.

CLARKW, Richard; KNAKE, Robert. **Cyber War: the next threat to national security and what to do about it**. New York: Harper Collins Publishers Inc, 2010. 191 p.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Direito Internacional Humanitário**. 2022. Disponível em: https://www.icrc.org/pt/document/o-que-e-o-direito-internacional-humanitario. Acesso em: 18 jun. 2023.

CZOSSECK, Christian; GEERS, Kenneth (ed.). **The Virtual Battlefield: perspectives on cyber warfare**. Amsterdam: Ios Press, 2009. 328 p.

INTERNATIONAL CRIMINAL COURT. **How the Court works**. Disponível em: https://www.icc-cpi.int/about/how-the-court-works. Acesso em: 08 ago. 2023

SANTOS, Daniel Mendes Aguiar; MALTEZ, Marcelo Monteiro; GOMES, Túlio Endres da Silva; FREITAS, Gerson de Moura. “A arte da guerra no século XXI: avançando à Multi-Domain Battle”. Coleção Meira Mattos, v. 13, n. 46, janeiro/abril 2019, pp. 83-105. Disponível em: <http://ebrevistas.eb.mil.br/index.php/RMM/article/download/1644/1761>. acessado em 08 novembro 2022.

UNITED NATIONS. **Universal Declaration of Human Rights**. 1948. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/english. Acesso em: 10 jul. 2023

UNITED NATIONS. Resolution nº 3314, de 14 de dezembro de 1974. **Definition Of Aggression**. Disponível em: https://iilj.org/wp-content/uploads/2016/08/General-Assembly-Resolution-3314.pdf. Acesso em: 10 abr. 2023.